Dell™ OpenManage™ Server Administrator Version 6.2- Installationshandbuch

Anmerkungen und Vorsichtshinweise

ANMERKUNG: Eine ANMERKUNG macht auf wichtige Informationen aufmerksam, mit denen Sie das System besser einsetzen können.

VORSICHTSHINWEIS: Durch VORSICHTSHINWEISE werden Sie auf potenzielle Gefahrenquellen hingewiesen, die Hardwareschäden oder Datenverlust zur Folge haben könnten, wenn die Anweisungen nicht befolgt werden.

Oktober 2009

Zurück zum Inhaltsverzeichnis

Bereitstellungsszenarien für Server Administrator

Dell™ OpenManage™ Server Administrator Version 6.2- Installationshandbuch

- Server Administrator-Komponenten auf Managed System

Sie können Dell™ OpenManage™ Server Administrator auf die folgenden Arten installieren:

- Server Administrator Web Server auf einem beliebigen System (Dell PowerEdge-System, Laptop oder Desktop) und Server Instrumentation auf einem anderen unterstützten Dell PowerEdge™-System installieren.

  Bei dieser Methode führt der Server Administrator Webserver die Funktion eines zentralen Webservers aus und Sie können ihn zur Überwachung einer Reihe von verwalteten Systemen verwenden. Mit dieser Methode wird die Beanspruchung der verwalteten Systeme durch den Server Administrator reduziert.

- Fahren Sie fort, um Server Administrator Web Server und Server Instrumentation auf dem gleichen System zu installieren.

Tabelle 4-1 listet die Bereitstellungsszenarien für Installation und Verwendung von Server Administrator und bietet Hilfe, damit Sie beim Auswählen der verschiedenen Installationsoptionen die richtige Wahl treffen können:

Tabelle 4-1. Bereitstellungsszenarien

Sie möchten:	Auswahl
Ihr gesamtes Netzwerk verwalteter Systeme von Ihrem System (kann ein Laptop, Desktop oder Server sein) aus remote verwalten.	**Server Administrator Web Server**. Sie müssen Server Instrumentation auf den verwalteten Systemen installieren.
Ihr derzeitiges System verwalten und überwachen.	**Server Administrator Web Server** + **Server Instrumentation**.
Ihr derzeitiges System unter Verwendung eines anderen Remote-Systems verwalten und überwachen.	**Remoteaktivierung** Für Systeme, die unter Microsoft Windows ausgeführt werden, befindet sich **Remoteaktivierung** unter der Option **Server Instrumentation**. Sie müssen dann Server Administrator Web Server auf dem Remote-System installieren.
Zeigen Sie den Zustand von lokalem Speicher und Remote-Speicher, der an ein verwaltetes System angeschlossen ist, an und rufen Sie Speicherverwaltungsinformationen in einer integrierten grafischen Ansicht ab.	**Storage Management**.
Remote auf ein betriebsunfähiges System zugreifen, Warnbenachrichtigungen erhalten, wenn ein System außer Betrieb ist, und ein System remote neu starten.	**Remote Access Controller**.

ANMERKUNG: Installieren Sie mithilfe Ihres Betriebssystem-Datenträgers den SNMP-Agenten auf Ihrem verwalteten System, bevor Sie die Managed System Software installieren.

Server Administrator-Komponenten auf Managed System

Das Setup-Programm enthält sowohl eine Option **Benutzerdefiniertes Setup** als auch eine Option **Typisches Setup.**

Mit der Option "Benutzerdefiniertes Setup" können Sie die Softwarekomponenten auswählen, die Sie installieren möchten. Tabelle 4-2 enthält eine Liste der verschiedenen Managed System-Softwarekomponenten, die Sie während einer benutzerdefinierten Installation installieren können. Einzelheiten über die benutzerdefinierte Setup-Option finden Sie unter "Benutzerdefinierte Installation".

Tabelle 4-2. Managed System-Softwarekomponenten

Komponente	Was installiert ist	Bereitstellungsszenario	Systeme, auf denen die I
Server Administrator Web Server	Webbasierte Systemverwaltungsfunktionalität, mit der Sie Systeme lokal oder remote verwalten können.	Installieren Sie nur Server Administrator Web Server, falls Sie das verwaltete System remote von Ihrem System aus überwachen möchten. Sie benötigen keinen direkten Zugang zum verwalteten System.	Beliebiges System. Zum B System.
ANMERKUNG: Wenn Sie mehrere Systeme, die sowohl Windows- als auch Linux-Betriebssysteme ausführen, remote verwalten möchten, sollten Sie Server Adm Betriebssystem installieren.			
Server Instrumentation	Server Administrator CLI + Instrumentation Service	Installieren Sie Server Instrumentation, um Ihr System als das verwaltete System zu verwenden. Bei der Installation von Server Instrumentation und Server Administrator Web Server wird Server Administrator installiert. Sie können Server Administrator verwenden, um Ihr System zu überwachen, zu konfigurieren und zu verwalten. **Hinweis:** Falls Sie nur Server Instrumentation (ohne Auswahl von Remoteaktivierung) installieren, müssen Sie auch Server Administrator Web Server installieren.	Unterstützte Dell PowerEd PowerEdge-Systeme finde *Systemen* auf der Support **http://support.dell.com/**
Storage Management	Server Administrator Storage Management	Installieren Sie die Speicherverwaltung, um Hardware-RAID-Lösungen zu implementieren und die an Ihrem System angeschlossenen Speicherkomponenten zu konfigurieren. Weitere Informationen über die Speicherverwaltung finden Sie im *Dell OpenManage Server Administrator Storage Management-Benutzerhandbuch* in dem Verzeichnis **docs** oder auf der Support-Website von Dell unter	Nur jene Systeme, auf den Remoteaktivierung installie

		http://support.dell.com/support/edocs/software/omswrels/index.htm.	
Remoteaktivierung	Server Administrator CLI + Instrumentation Service + CIM Provider	Installieren Sie Remoteaktivierung, um Remote-Systemverwaltungsaufgaben durchzuführen. Sie können Remoteaktivierung auf Ihrem System installieren und lediglich Server Administrator Web Server auf einem anderen System (z. B. System X) installieren. Sie können dann System X verwenden, um Ihr System im Remotezustand zu überwachen und zu verwalten. Sie können System X verwenden, um beliebig viele Systeme zu verwalten, auf denen Remoteaktivierung installiert ist.	Unterstützte Dell PowerEd Dell PowerEdge-Systeme f *Systemen* auf der Support **http://support.dell.com/**
Remote-Access-Controller	Server Administrator CLI + Instrumentation Service + iDRAC oder DRAC 5 oder DRAC 4 (abhängig vom Typ des Dell PowerEdge Systems)	Installieren Sie Remote Access Service, um E-Mail-Warnungen zu erhalten, wenn Warn- oder Fehlerereignisse hinsichtlich Spannung, Temperatur und Lüftergeschwindigkeit auftreten. Weiterhin protokolliert Remote Access Service auch Ereignisdaten und den neuesten Absturzbildschirm (nur auf Systemen mit Microsoft Windows-Betriebssystem), um Ihnen zu helfen, die wahrscheinliche Ursache eines Systemausfalls zu diagnostizieren.	Nur jene Systeme, auf den Remoteaktivierung installie
Intel SNMP-Agent	Intel SNMP-Agent	Installieren Sie diesen SNMP-Agenten, um Server Administrator zu aktivieren und Informationen über Netzwerkschnittstellenkarten (NICs) abzurufen. Dieser SNMP-Agent hilft beim Identifizieren der NICs.	Nur auf Dell PowerEdge Sy installiert ist und das Micr
Broadcom SNMP-Agent	Broadcom SNMP-Agent	Installieren Sie diesen SNMP-Agenten, um Server Administrator zu aktivieren und Informationen über NICs abzurufen. Dieser SNMP-Agent hilft beim Identifizieren der NICs.	Nur auf Dell PowerEdge Sy installiert ist und das Micr

---

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Häufig gestellte Fragen

Dell™ OpenManage™ Server Administrator Version 6.2- Installationshandbuch

---

Allgemein

Wie installiert man Dell OpenManage Server Administrator nur mit den CLI-Funktionen?

Indem Sie wählen den Server Administrator Web Server nicht zu installieren, erhalten Sie nur CLI-Funktionen.

Welche Schnittstellen verwenden Dell OpenManage-Anwendungen?

Der von Server Administrator verwendete Standardanschluss-Server lautet 1311. Die Standardschnittstellen, die von Dell OpenManage™ IT Assistant verwendet werden, lauten 2607 (für den Verbindungsdienst) und 2606 (für den Netzwerküberwachungsdienst). Diese Schnittstellen sind konfigurierbar. Schnittstelleninformationen einer bestimmten Komponente finden Sie im Benutzerhandbuch zur jeweiligen Komponente.

Wenn ich virtuelle Datenträger auf dem DRAC Controller über ein WAN (Wide Area Network) mit niedriger Bandbreite und Latenz ausführe, schlägt das Starten der Installationsdatei von OpenManage direkt auf dem virtuellen Datenträger fehl. Was soll ich tun?

Im Fehlerfall kopieren Sie das Web-Installationspaket (erhältlich unter **support.dell.com**) zuerst direkt auf das lokale System und starten die Installationsdatei von Dell OpenManage direkt vom lokalen System.

Muss ich die Anwendung "Adaptec Fast Console" auf dem System vor der Installation des Server Administrator Storage Management-Dienst deinstallieren?

Ja, falls Adaptec Fast Console bereits auf dem System installiert ist, müssen Sie diese Anwendung deinstallieren, bevor Sie den Server Administrator Storage Management-Dienst installieren.

Microsoft® Windows®

Wie behebe ich eine fehlerhafte Installation von Server Administrator?

Sie können eine fehlerhafte Installation beheben, indem Sie eine Neuinstallation erzwingen und anschließend Server Administrator deinstallieren. So erzwingen Sie eine Neuinstallation:

- Bringen Sie in Erfahrung, welche Version von Server Administrator zuvor installiert wurde.
- Laden Sie das Installationspaket für diese Version von der Dell Support-Internetseite unter **support.dell.com** herunter.
- Gehen Sie zu **SysMgmt.msi** im Verzeichnis **SYSMGMT\srvadmin\windows\SystemsManagement** und geben Sie folgenden Befehl als Eingabeaufforderung zum Erzwingen einer Neuinstallation ein:

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

- Wählen Sie **Benutzerdefiniertes Setup** und alle Funktionen, die ursprünglich installiert wurden. Wenn Sie nicht sicher sind, welche Funktionen installiert waren, wählen Sie sie alle aus und führen Sie die Installation aus.

  ANMERKUNG: Wenn Sie Server Administrator nicht in einem Standardverzeichnis installiert haben, achten Sie darauf, dies auch beim **benutzerdefinierten Setup** zu ändern.

Nachdem die Anwendung installiert ist, kann sie über **Software** deinstalliert werden.

Was muss ich tun, wenn die Erstellung von WinRM Listener mit der folgenden Meldung fehlschlägt: *Die Eigenschaft "CertificateThumbprint" muss leer ein, wenn die SSL-Konfiguration für einen anderen Dienst freigegeben wird*?

Wenn der Internet Information Server (IIS) bereits installiert und für HTTPS-Kommunikation konfiguriert ist, tritt der obige Fehlercode auf. Einzelheiten über die Koexistenz von IIS und WinRM sind verfügbar unter: **http://technet.microsoft.com/en-us/library/cc782312.aspx**.

In diesem Fall verwenden Sie den nachstehenden Befehl, um einen HTTPS Listener mit leerer **CertificateThumbprint** zu erstellen.

Beispiel: `winrm create winrm/config/Listener?Address=*+Transport=HTTPS @{Hostname="<host_name>";CertificateThumbprint=""}`

Was sind die auf die Firewall bezogenen Konfigurationsänderungen, die für WinRM vorgenommen werden müssen?

Bei eingeschalteter Firewall muss WinRM zur Firewall-Ausschlussliste hinzugefügt werden, damit TCP-Port 443 für HTTPS-Verkehr zulässig ist.

Beim Starten des Installationsprogramms von Dell OpenManage kann eine Fehlermeldung auftreten, die einen Fehler beim Laden einer bestimmten Bibliothek, eine Verweigerung des Zugriffs oder einen Initialisierungsfehler anzeigt. Ein Beispiel für einen Installationsfehler bei der Ausführung des Installationsprogramms von Dell OpenManage ist: "Fehler beim Laden von OMIL32.DLL ." Was soll ich tun?

Der Grund dafür sind wahrscheinlich ungenügende COM-Berechtigungen auf dem System. Zur Behebung dieser Situation lesen Sie bitte den folgenden Artikel: **http://support.installshield.com/kb/view.asp?articleid=Q104986**

Das Installationsprogramm von Dell OpenManage schlägt möglicherweise auch fehl, wenn eine vorherige Installation von Dell OpenManage Systems

Management-Software oder anderer Softwareprodukte nicht erfolgreich war. Eine temporäre Windows Installer-Registry kann gelöscht werden, was möglicherweise den Dell OpenManage-Installationsfehler behebt. Entfernen Sie ggf. den folgenden Schlüssel:

`HKLM\Software\Microsoft\Windows\CurrentVersion\Installer\InProgress`

Ich erhalte eine irreführende Warn-/Fehlermeldung während der Installation von Dell OpenManage.

Wenn auf dem Windows-Systemlaufwerk nicht genügend Speicher vorhanden ist, kann eine irreführende Warn-/Fehlermeldung auftreten, wenn Sie das Installationsprogramm von Dell OpenManage ausführen. Das Windows-Installationsprogramm benötigt zusätzlichen Speicherplatz, um das Installationspaket vorübergehend in den Ordner `%TEMP%` zu extrahieren. Stellen Sie sicher, dass auf dem Systemlaufwerk ausreichend Speicherplatz (mindestens 100 MB) vorhanden ist, bevor Sie das Installationsprogramm von Dell OpenManage ausführen.

Beim Starten des Installationsprogramms von Dell OpenManage erhalte ich die Fehlermeldung "Auf diesem System wurde eine frühere Version der Server Administrator-Software festgestellt. Bevor Sie diese Version installieren können, müssen Sie alle vorhergehenden Versionen von Server Administrator-Anwendungen deinstallieren."

Wenn diese Meldung angezeigt wird, wenn Sie das Installationsprogramm von Dell OpenManage starten, sollten Sie das Programm **OMClean.exe** im Verzeichnis **SYSMGMT\srvadmin\support\OMClean** ausführen, um eine frühere Version von Server Administrator auf dem System zu entfernen.

Muss ich vor der Installation von Citrix Metaframe frühere Versionen von Server Administrator deinstallieren?

Ja. Deinstallieren Sie frühere Versionen von Server Administrator, bevor Sie Citrix Metaframe installieren (alle Versionen). Da nach der Installation von Citrix Metaframe Fehler in der Registry vorliegen können, müssen Sie Server Administrator neu installieren.

Wenn ich das Installationsprogramm von Dell OpenManage ausführe, werden auf dem Bildschirm "Voraussetzungsprüfungsinformationen" unlesbare Zeichen angezeigt.

Wenn Sie das Installationsprogramm von Dell OpenManage in Englisch, Deutsch, Französisch oder Spanisch ausführen und auf dem Bildschirm **Voraussetzungsprüfungsinformationen** unlesbare Zeichen angezeigt werden, stellen Sie sicher, dass Ihre Browser-Kodierung den Standardzeichensatz verwendet. Ein Zurücksetzen der Browser-Kodierung auf den Standardzeichensatz löst das Problem.

Ich habe Server Administrator und Dell Online Diagnostics im selben Verzeichnis installiert und Dell Online Diagnostics funktioniert nicht. Was soll ich tun?

Wenn Sie Server Administrator und Dell Online Diagnostics im selben Verzeichnis installiert haben, funktioniert Online Diagnostics möglicherweise nicht. Später bei Deinstallation von Server Administrator gehen möglicherweise alle Online Diagnostics-Dateien verloren. Um dieses Problem zu vermeiden, installieren Sie Server Administrator und Online Diagnostics in verschiedenen Verzeichnissen. Im Allgemeinen wird empfohlen, nicht mehr als eine Anwendung im gleichen Verzeichnis zu installieren.

Ich habe Server Administrator mit Remote Server Administrator-Bereitstellung unter Windows Server 2008 installiert. Ich kann das Server Administrator-Symbol nicht auf dem Desktop finden.

Bei einer erstmaligen Server Administrator-Installation mit Remote Server Administrator-Bereitstellung (OMSA Push) auf einem Server unter Windows 2008 ist das Server Administrator-Symbol nicht sichtbar, bis der Desktop manuell aktualisiert wird. Zum Beispiel durch Drücken der Taste *<F5>*.

Ich sehe eine Warnmeldung beim Deinstallieren von Server Administrator unter Microsoft Windows Server 2008, wenn das Installationsprogramm versucht, die Verknüpfung zu entfernen.

Beim Deinstallieren von Server Administrator unter Microsoft Windows Server 2008 wird möglicherweise eine Warnmeldung angezeigt, wenn das Installationsprogramm versucht, die Verknüpfung zu entfernen. Klicken Sie bei der Warnmeldung auf OK, um die Deinstallation fortzusetzen.

Wo kann ich die MSI-Protokolldateien finden?

Die MSI-Protokolldateien sind standardmäßig in dem von der Umgebungsvariablen **%TEMP%** definierten Pfad gespeichert.

Ich habe die Server Administrator-Dateien für Windows von der Support-Website von Dell heruntergeladen und sie auf mein eigenes Speichermedium kopiert. Der Versuch, die SysMgmt.msi-Datei zu starten, schlug fehl. Was stimmt nicht?

MSI erfordert, dass alle Installationsprogramme die Eigenschaft **MEDIAPACKAGEPATH** angeben, wenn sich die MSI-Datei nicht im Stammverzeichnis der DVD befindet.

Diese Eigenschaft ist für das Managed System Software-MSI -Paket auf **SYSMGMT\srvadmin\windows\SystemsManagement** eingestellt. Wenn Sie beschließen, Ihre eigene DVD herzustellen, müssen Sie sicherstellen, dass das DVD-Layout gleich bleibt. Die Datei **SysMgmt.msi** muss sich im Verzeichnis **SYSMGMT\srvadmin\windows\SystemsManagement** befinden. Weitere Informationen finden Sie unter **http://msdn.microsoft.com**. Suchen Sie nach Eigenschaft MEDIAPACKAGEPATH.

Unterstützt das Installationsprogramm von Dell OpenManage Installer Windows Advertised-Installation?

Nein. Das Installationsprogramm von Dell OpenManage unterstützt "Windows Advertised-Installation" nicht - Windows Advertised-Installation ist das Verfahren der automatischen Verteilung eines Programms an Client-Computer für nachträgliche Installation über die Windows-Gruppenrichtlinien.

Wie prüfe ich die Verfügbarkeit von Festplattenspeicher während einer benutzerdefinierten Installation?

Sie müssen auf dem Bildschirm **Benutzerdefiniertes Setup** auf eine aktive Funktion klicken, um die Verfügbarkeit von Festplattenspeicher anzuzeigen bzw. das Installationsverzeichnis zu ändern. Wenn beispielsweise die Funktion A zur Installation ausgewählt ist (aktiv) und die Funktion B ist nicht aktiv, sind die Schaltflächen **Ändern** und **Speicher** deaktiviert, wenn Sie auf die Funktion B klicken. Klicken Sie auf die Funktion A, um die Speicherplatzverfügbarkeit anzuzeigen oder das Installationsverzeichnis zu ändern.

Was muss ich tun, wenn ich die Meldung erhalte, dass die aktuelle Version bereits installiert ist?

Wenn Sie mit MSP von Version "X" auf Version "Y" erweitern und dann versuchen, die Version "Y"-DVD (vollständige Installation) zu installieren, meldet die Voraussetzungsprüfung der Version "Y"-DVD an, dass die aktuelle Version bereits installiert ist. Wenn Sie fortfahren, wird die Installation nicht im "Wartungsmodus" ausgeführt und die Optionen "Bearbeiten", "Reparieren" oder "Entfernen" werden nicht angezeigt. Durch Fortsetzung der Installation wird die MSP-Datei entfernt und es wird ein Cache der im Version "Y"- Paket vorhandenen MSI-Datei erstellt. Wenn Sie sie ein zweites Mal ausführen, wird das Installationsprogramm im "Wartungsmodus" ausgeführt.

Wie kann man die Voraussetzungsprüfungsinformationen am besten verwenden?

Die Voraussetzungsprüfung ist für Windows erhältlich. Detaillierte Informationen zur Verwendung der Voraussetzungsprüfung finden Sie in der Infodatei **SYSMGMT\srvadmin\windows\PreReqChecker\readme.txt** auf der DVD *Dell Systems Management Tools and Documentation*.

Im Voraussetzungsprüfungsbildschirm erhalte ich die Meldung "Beim Versuch, ein Visual Basic-Skript auszuführen, ist ein Fehler aufgetreten. Bitte bestätigen Sie, dass die Visual Basic-Dateien korrekt installiert sind". Wie kann dieses Problem behoben werden?

Dieser Fehler tritt auf, wenn die Voraussetzungsprüfung das Dell OpenManage-Skript **vbstest.vbs** (ein Visual Basic-Skript) aufruft, um die Installationsumgebung zu bestätigen, und dieses Skript fehlschlägt.

Mögliche Ursachen sind:

- Falsche Internet Explorer-Sicherheitseinstellungen.

  Stellen Sie sicher, dass **Extras→ Internetoptionen→ Sicherheit→ Benutzerdefinierte Stufe→ Scripting→ Active Scripting** auf **Aktivieren** eingestellt ist.

  Stellen Sie sicher, dass **Extras→ Internetoptionen→ Sicherheit→ Benutzerdefinierte Stufe→ Scripting→ Scripting von Java-Applets** auf **Aktivieren** eingestellt ist.

- Windows Scripting Host (WSH) hat die Ausführung von VBS-Skripts deaktiviert. WSH ist während der Betriebssysteminstallation standardmäßig installiert. WSH kann konfiguriert werden, um die Ausführung von Skripts mit einer **.VBS-**Erweiterung zu vermeiden.

  c. Klicken Sie mit der rechten Maustaste auf **Arbeitsplatz** auf Ihrem Desktop und klicken Sie auf **Öffnen→ Hilfsprogramme→ Ordneroptionen→ Dateitypen**.

  d. Suchen Sie nach der **VBS-**Dateierweiterung und stellen Sie sicher, dass **Dateitypen** auf **VBScript Script File** eingestellt ist.

  e. Ist dies nicht der Fall, klicken Sie auf **Ändern** und wählen **Microsoft Windows Based Script Host** als diejenige Anwendung, die aufgerufen wird, um das Skript auszuführen.

- WSH ist die falsche Version, beschädigt oder nicht installiert. WSH wird während der Betriebssysteminstallation standardmäßig installiert. Laden Sie WSH von **msdn.microsoft.com** herunter**.**

Sind die durch Windows-Installationsdienste während einer Installation/Deinstallation angezeigten Zeitangaben genau?

Nein. Der Windows-Installationsdienst zeigt während einer Installation/Deinstallation möglicherweise die restliche Laufzeit der aktuell ausgeführten Aufgabe an. Dies ist lediglich eine auf verschiedenen Faktoren basierende Schätzung der Windows Installer Engine.

Kann ich meine Installation starten, ohne die Voraussetzungsprüfung auszuführen? Wie mache ich dies?

Ja, das können Sie. Sie können beispielsweise MSI der Managed System-Software direkt über **SYSMGMT\srvadmin\Windows\SystemsManagement** ausführen. Im Allgemeinen ist es nicht zu empfehlen, die Voraussetzungsinformationen zu umgehen, da diese wichtige Informationen enthalten.

Wie bringe ich in Erfahrung, welche Version der Systems Management-Software auf dem System installiert ist?

Gehen Sie zu **Start→ Einstellungen→ Systemsteuerung→ Software** und wählen Sie **Dell OpenManage Server Administrator**. Wählen Sie den Link für **Support-Informationen**.

Muss ich das System nach einem Upgrade von Dell OpenManage neustarten?

Die Aktualisierung kann einen Neustart erfordern, wenn die zur Aktualisierung bestimmten Dateien verwendet werden. Dies ist für Windows-Installationsprogramme typisch. Es wird empfohlen, den System-Neustart bei Aufforderung durchzuführen.

Wo kann ich in Erfahrung bringen, welche Server Administrator-Funktionen derzeit auf meinem System installiert sind?

Mit der **Windows-Option "Software"** erfahren Sie, welche Server Administrator-Funktionen derzeit installiert sind.

Wie heißen alle Dell OpenManage-Funktionen unter Windows?

Die folgende Tabelle enthält die Namen aller Dell OpenManage-Funktionen und ihre entsprechenden Namen in Windows.

Tabelle 11-1. Dell OpenManage-Funktionen unter Windows

Funktion	**Name in Windows**
Managed System Services	
Server Administrator Instrumentation Service	DSM SA Data Manager DSM SA Event Manager
Server Administrator	DSM SA-Verbindungsdienst DSM SA-Freigabedienste
Server Administrator Storage Management Service	Mr2kserv
Remote Access Controller-Konsole (DRAC 4)	Remote Access Controller 4 (DRAC 4)

Red Hat® Enterprise Linux® oder SUSE® Linux Enterprise Server

Ich kann mich nach dem Installieren von Server Administrator nicht anmelden.

Melden Sie sich nach dem Installieren von Service Administrator ab und dann wieder an, um auf die Server Administrator Befehlszeilenschnittstelle (CLI) zuzugreifen.

Beim Versuch, Server Administrator auf einem Linux Gast-Betriebssystem zu installieren, wird die folgende Meldung angezeigt: ./srvadmin-install.sh:

line 2295 : [: ==: unärer Operator erwartet

Beim Installieren der Dell OpenManage-Komponenten auf einem Linux Gast-Betriebssystem wird die Warnmeldung möglicherweise angezeigt. Die Installation wird jedoch fortgesetzt und ohne Funktionalitätsverluste fertiggestellt.

Ich habe das Betriebssystem Red Hat Enterprise Linux 4 - x86_64 manuell installiert und bekomme bei dem Versuch, Server Administrator zu installieren, RPM-Abhängigkeiten angezeigt. Wo kann ich diese abhängigen RPM-Dateien finden?

Für Red Hat Enterprise Linux befinden die abhängigen RPM-Dateien auf der Installations-CD zu Red Hat Enterprise Linux. Alle anderen RPMs sind im Verzeichnis **/SYSMGMT/srvadmin/linux/RPMS/supportRPMS\opensource-components** zu finden.

Führen Sie folgenden Befehl aus, um alle abhängigen RPM-Dateien zu aktualisieren:

```
rpm –ivh /SYSMGMT/srvadmin/linux/RPMS/
supportRPMS/opensource-components
```

Anschließend können Sie mit der Server Administrator-Installation fortfahren.

Ich habe eine nicht-standardmäßige Installation des Linux-Betriebssystems unter Verwendung des gelieferten Linux-Betriebssystem-Mediums durchgeführt und erhalte während der Installation von Server Administrator fehlende RPM-Dateiabhängigkeiten.

Server Administrator ist eine 32-Bit-Anwendung. Bei Installation auf einem System unter einer 64-Bit-Version des Red Hat Enterprise Linux-Betriebssystems bleibt der Server Administrator eine 32-Bit-Anwendung, wogegen die durch Server Administrator installierten Gerätetreiber 64-Bit-Programme sind. Wenn Sie versuchen, Server Administrator auf einem System unter Red Hat Enterprise Linux (Versionen 4 und 5) für Intel EM64T zu installieren, stellen Sie sicher, dass Sie die entsprechenden 32-Bit-Versionen der fehlenden RPM-Dateiabhängigkeiten installieren. Die 32-Bit-RPM-Versionen haben stets **i386** in der Dateinamenerweiterung. Sie erhalten möglicherweise auch Abhängigkeiten freigegebener Objektdateien (Dateien mit **so** in der Dateinamenserweiterung). In diesem Fall können Sie bestimmen, welche RPM zur Installation des freigegebenen Objekts benötigt wird, indem Sie den RPM-Schalter `--whatprovides` verwenden. Beispiel:

```
rpm -q --whatprovides libpam.so.0
```

Es kann ein RPM-Name wie **pam-0.75-64** zurückgegeben werden. Beschaffen Sie dementsprechend die **pam-0.75-64.i386.rpm** und installieren Sie sie. Wenn Server Administrator auf einem System unter einer 64-Bit-Version eines Linux-Betriebssystems installiert wird, stellen Sie sicher, dass das RPM-Paket **compat-libstdc++-<version>.i386.rpm** installiert ist. Sie müssen die Abhängigkeiten manuell auflösen, indem Sie die fehlenden RPM-Dateien vom Linux-Betriebssystem-Medium installieren.

ANMERKUNG: Wenn Sie spätere Versionen unterstützter Linux-Betriebssysteme verwenden und die im Verzeichnis `SYSMGMT/srvadmin/linux/RPMS/supportRPMS` auf der DVD verfügbaren RPM-Dateien inkompatibel sind, verwenden Sie die neuesten RPMs Ihres Betriebssystem-Mediums.

Wo finde ich die Quellpakete für Open Source RPMs?

Quellpakete für Open Source RPMs sind auf einem bestellbaren DVD-Image verfügbar.

Was muss ich tun, wenn die Management Station-RAC-Dienstprogramm-Installation wegen einer fehlenden RPM-Datei fehlschlägt?

Die Installation des Management Station-RAC-Dienstprogramms (RPM `mgmtst-racadm` im Verzeichnis `/SYSMGMT/ManagementStation/linux/rac` auf der DVD *Dell Systems Management Tools and Documentation*) kann wegen fehlender RPM-Dateiabhängigkeiten von libstdc++.so-Bibliotheken fehlschlagen. Installieren Sie die im selben Verzeichnis enthaltene RPM **compat-libstdc++**, um die Abhängigkeit aufzulösen, und versuchen Sie die Installation nochmals.

Bei Verwendung des Befehls `rpm -e 'rpm -qa | grep srvadmin'` **zur Entfernung von Dell OpenManage Systems Management-Software legen bestimmte RPM-Dienstprogrammversionen möglicherweise eine Deinstallation in einer falschen Reihenfolge fest, was dazu führt, dass Benutzer irreführende Warn- oder Fehlermeldungen erhalten. Was ist die Lösung?**

Die Lösung besteht darin, das auf der DVD enthaltene Dell OpenManage-Deinstallationsskript `srvadmin-uninstall.sh` zu verwenden.

Was soll ich tun, wenn ich aufgefordert werde, mich mit dem Stammbenutzerkonto zu authentifizieren?

Dell Systems Build and Update Utility fügt ein Skript zur **.bash_profile**-Datei des Stammbenutzers hinzu. Dieses Skript fordert zur Installation von Dell OpenManage Systems Management-Software auf. Das Skript kann Remote-Client-Anwendungen beeinträchtigen, die sich mit dem Stammbenutzerkonto beim System authentifizieren, jedoch keine Möglichkeit haben, Benutzeraufforderungen zu handhaben. Zum Beheben dieser Einschränkung bearbeiten Sie die **.bash_profile**-Datei und verwandeln die folgende Zeile in einem Kommentar: `[ ${SHLVL}....`

Bei Deinstallation wird die Fehlermeldung *Fehler: %preun(srvadmin-NAME-X.Y.Z-N.i386) Scriptlet fehlgeschlagen, Exit-Status 1* **angezeigt.**

Nach einem nicht erfolgreichen Upgrade während eines manuellen RPM-Upgrades treten möglicherweise Probleme bei der Deinstallation von Server Administrator auf. Die folgende Fehlermeldung wird angezeigt:

```
Fehler: %preun(srvadmin-NAME-X.Y.Z-N.i386) Scriptlet fehlgeschlagen, Exit-Status 1
```

In diesem Fall ist `NAME` eine Funktion, z. B. `omacore`. `X.Y.Z-N` ist die Version und Build-Nummer der Funktion. Mögliche Lösungen zur Behebung dieses Problems:

1. Versuchen Sie erneut zu deinstallieren. Verwenden Sie zum Beispiel den folgenden Befehl:

```
rpm -e srvadmin-NAME-X.Y.Z-N.i386
```

2. Löschen Sie die Zeile "upgrade.relocation=bad", wenn sie in der Datei `/etc/omreg.cfg` vorhanden ist, und versuchen Sie erneut zu deinstallieren.

Warum erhalte ich während der Installation eine Warnung im Hinblick auf den RPM-Paketschlüssel?

Die RPM-Dateien sind mit einer Digitalsignatur versehen. Damit diese Warnung vermieden wird, sollten Sie die CD oder das Paket laden und den Schlüssel mithilfe eines Befehls wie beispielsweise folgendem importieren:

```
rpm --import /mnt/dvdrom/SYSMGMT/srvadmin/linux/RPM-GPG-KEY
```

Wie lauten die Namen aller Funktionen von Dell OpenManage unter Red Hat Enterprise Linux oder SUSE Linux Enterprise Server?

Die folgende Tabelle enthält alle Namen der Dell OpenManage-Funktionen und ihren entsprechenden init Skript-Namen unter Red Hat Enterprise Linux- und SUSE Linux Enterprise Server-Betriebssystemen:

Tabelle 11-2. Dell OpenManage-Funktionen unter Red Hat Enterprise Linux und SUSE Linux Enterprise Server

Funktion	Name in VMware ESX, Red Hat Enterprise Linux und SUSE Linux Enterprise Server
Dienstfunktion von Managed System	Funktion init Skript-Name
DSM SA-Gerätetreiber DSM SA Data Engine-Dienst	instsvcdrv dataeng
DSM SA-Freigabedienst DSM SA-Verbindungsdienst	dsm_om_shrsvc dsm_om_connsvc
DSM SM LSI-Manager	mptctl
Integrierter Dell Remote Access Controller (iDRAC)	Keine
Remote Access Controller (DRAC 4)	racsvc
Remote Access Controller (DRAC 5)	Keine

Was enthalten die Verzeichnisse unter srvadmin/linux/custom/<Betriebssystem>?

Die folgende Tabelle enthält die Namen der Verzeichnisse im Verzeichnis **SYSMGMT/srvadmin/linux/custom/<Betriebssystem>**.

Tabelle 11-3. Namen der Verzeichnisse unter dem srvadmin/linux/custom/<Betriebssystem>-Verzeichnis

Name von RPM	Beschreibung	Andere Server Administrator-RPMs erforderlich
Server-Instrumentation – Dies ist der Kerncode für Server Administrator. Er gibt Hauptplatinenwarnungen aus und enthält die Befehlszeilenschnittstellenbefehle, die eine Überwachung und Steuerung von Server Administrator ermöglichen, zum Beispiel: `omconfig`, `omdiag` und `omreport`. Für alle Peripheriepakete außer dem DRAC-Support müssen alle oder die meisten RPM in diesem Verzeichnis installiert werden. **ANMERKUNG:** Zur Gewährleistung einer ordnungsgemäßen Funktionalität kann die Installation von IPMI-Treibern erforderlich sein.		
srvadmin-cm	Server Administrator-Bestandsaufnahmensammler - Systems Management: Bestandsaufnahmensammler-Änderungsverwaltung.	srvadmin-omilcore, srvadmin-deng und srvadmin-omacore.
srvadmin-deng	Server Administrator Data Engine - Systems Management enthält ein Datenverwaltungs-Framework für Systems Management-Software.	srvadmin-omilcore
- srvadmin-hapi	Hardware-Anwendungsprogrammierschnittstelle von Server Administrator - Dieses Systems Management-Paket enthält die Gerätetreiber und Bibliotheken, die von der Systems Management-Software zum Zugreifen auf Hardwareinformationen von unterstützten Systemen erforderlich ist.	srvadmin-omilcore
srvadmin-isvc	Server Administrator Instrumentation Service - Server Administrator enthält Systemverwaltungsinformationen, damit im Netzwerk unterstützte Systeme fehlerfrei funktionieren. Server Administrator Instrumentation Service enthält Fehlerverwaltungsinformationen, Vorfehlerinformationen sowie Bestands- and Bestandsaufnahmeinformationen für Verwaltungsanwendungen. Der Instrumentation Service überwacht den Systemzustand und sorgt für einen schnellen Zugriff auf ausführliche Fehler- und Leistungsinformationen zu unterstützter Systemhardware. Für den Instrumentation Service ist die Installation von Systems Management-Gerätetreibern erforderlich.	srvadmin-omilcore, srvadmin-deng und srvadmin-hapi
srvadmin-omacore	Server Administrator - Systems Management-Verwaltungsmodus: Kern und CLI.	srvadmin-omilcore und srvadmin-deng
srvadmin-omhip	Server Administrator Instrumentation Service Integration Layer - Enthält Instrumentation-CLI.	srvadmin-omilcore, srvadmin-deng, srvadmin-hapi, srvadmin-isvc und srvadmin-omacore
srvadmin-omilcore	Server Administrator-Installationskern - Dies ist das Kerninstallationspaket, welches die erforderlichen Tools für die restlichen Installationspakete von Systems Management enthält. Alle Server Administrator-RPMs benötigen diesen RPM.	
srvadmin-syscheck	Paket, das den Grad der OpenManage-Unterstützung prüft.	srvadmin-omilcore
add-iDRAC – Software für die Remote-Verwaltung von Remote Access Controllern der dritten Generation. Beispiel: iDRAC.		
srvadmin-idrac-components	Integrierte Remote Access Controller-Komponenten für die Datenbestückung der Remote-Zugriffskarte.	srvadmin-omilcore, srvadmin-deng, srvadmin-hapi und srvadmin-racser
srvadmin-idracadm	iDRAC-Befehlsschnittstelle - Die Befehlszeilen-Benutzerschnittstelle zum integrierten Dell Remote Access Controller (RAC).	srvadmin-omilcore
srvadmin-idracdrsc	iDRAC Integration Layer - integrierte Dell Remote-Access-CLI und Internet-Plugin für Server Administrator.	srvadmin-omilcore, srvadmin-deng, srvadmin-rac4-Komponenten und srvadmin-omacore

add-RAC4 - Software für die Remote-Verwaltung von Remote Access Controllern der vierten Generation. Beispiel: DRAC 4.		
srvadmin-rac4-Komponenten	Datenbestückung der Remote-Zugriffskarte - Remote Access Controller-Komponenten.	srvadmin-omilcore, srvadmin-deng, srvadmin-hapi und srvadmin-racsvc
srvadmin-racadm4	RAC-Befehlsschnittstelle - Die Befehlszeilen-Benutzerschnittstelle zum Remote Access Controller (RAC).	srvadmin-omilcore
srvadmin-racdrsc4	DRAC 4 Integration Layer - Remote-Zugriff-CLI und Internet-Plugin für Server Administrator.	srvadmin-omilcore, srvadmin-deng, srvadmin-rac4-Komponenten und srvadmin-omacore
srvadmin-racsvc	Verwalteter Knoten der Remote-Zugriffskarte - RAC-Dienste (Remote Access Controller), die die zentrale Verwaltung der Server-Cluster und die Remote-Verwaltung der verteilten Quellen unterstützt.	srvadmin-omilcore
add-RAC5 - Software für die Remote-Verwaltung von Remote Access Controllern der fünften Generation. Beispiel: DRAC 5.		
srvadmin-rac5-Komponenten	Daten der Remote-Zugriffskarte, DRAC 5 und Remote Access Controller-Komponenten, DRAC 5.	srvadmin-omilcore, srvadmin-deng und srvadmin-hapi
srvadmin-racadm5	RAC-Befehlsschnittstelle - Die Befehlszeilen-Benutzerschnittstelle zum Remote Access Controller (RAC).	srvadmin-omilcore und srvadmin-hapi
srvadmin-racdrsc5	DRAC 5 Integration Layer - Remote-Zugriff-CLI und Internet-Plugin für Server Administrator	srvadmin-omilcore, srvadmin-deng, srvadmin-omacore und srvadmin-rac5-Komponenten
add-StorageManagement — RAID-Konfigurationsdienstprogramm von Storage Management und Storage-Warnsoftware		
Srvadmin-storage	Storage Management - Enthält Storage Services von Systems Management.	srvadmin-omilcore, srvadmin-deng, srvadmin-omacore und srvadmin-odf
SA-WebServer – Ermöglicht den Internetzugang zur Verwaltung des Servers.		
- srvadmin-hapi	Hardware-Anwendungsprogrammierschnittstelle von Server Administrator - Dieses Systems Management-Paket enthält die Gerätetreiber und Bibliotheken, die von der Systems Management-Software für den Zugriff auf Hardwareinformationen von unterstützten Systemen erforderlich ist.	srvadmin-omilcore
srvadmin-iws	Sicherer Schnittstellenserver - Webserverpaket zum verwalteten Knoten von Systems Management.	srvadmin-omilcore, srvadmin-deng, srvadmin-omacore und srvadmin-jre
srvadmin-jre	Sun Java-Laufzeitumgebung von Server Administrator - verwalteter Knoten zur Java-Laufzeit von Systems Management.	srvadmin-omilcore, srvadmin-deng und srvadmin-omacore
srvadmin-omauth	Liefert die Authentifizierungsdateien.	srvadmin-omilcore
srvadmin-omcommon	Liefert das von Server Administrator benötigte Common Framework.	srvdamin-omilcore
srvadmin-omilcore	Server Administrator Web Server Install Core — Dies ist das Kerninstallationspaket. Alle Server Administrator Web Server-RPMs benötigen diesen RPM.	
srvadmin-wsmanclient	Betriebssystemspezifisches WSMan-Client-Paket.	srvadmin-omcommon und srvadmin-omauth
Remote-Enablement — Verwaltung und Überwachung Ihres aktuellen Systems mithilfe eines anderen Remote-Systems		
srvadmin-cm	Server Administrator-Bestandsaufnahmensammler - Systems Management: Bestandsaufnahmensammler-Änderungsverwaltung.	srvadmin-omilcore, srvadmin-deng und srvadmin-omacore.
srvadmin-deng	Server Administrator Data Engine - Systems Management enthält ein Datenverwaltungs-Framework für Systems Management-Software.	srvadmin-omilcore
- srvadmin-hapi	Hardware-Anwendungsprogrammierschnittstelle von Server Administrator - Dieses Systems Management-Paket enthält die Gerätetreiber und Bibliotheken, die von der Systems Management-Software zum Zugreifen auf Hardwareinformationen von unterstützten Systemen erforderlich ist.	srvadmin-omilcore
srvadmin-isvc	Server Administrator Instrumentation Service - Server Administrator enthält Systemverwaltungsinformationen, so dass im Netzwerk unterstützte Systeme fehlerfrei funktionieren. Server Administrator Instrumentation Service enthält Fehlerverwaltungsinformationen, Vorfehlerinformationen sowie Bestands- and Bestandsaufnahmeinformationen für Verwaltungsanwendungen. Der Instrumentation Service überwacht den Systemzustand und sorgt für einen schnellen Zugriff auf ausführliche Fehler- und Leistungsinformationen zu unterstützter Systemhardware. Für den Instrumentation Service ist die Installation von Systems Management-Gerätetreibern erforderlich.	srvadmin-omilcore, srvadmin-deng und srvadmin-hapi
srvadmin-omacore	Server Administrator - Systems Management-Verwaltungsmodus: Kern und CLI.	srvadmin-omilcore und srvadmin-deng
srvadmin-omcommon	Liefert Common Framework, benötigt von Server Administrator.	srvadmin-omilcore
srvadmin-omhip	Server Administrator Instrumentation Service Integration Layer - Enthält Instrumentation-CLI.	srvadmin-omilcore, srvadmin-deng, srvadmin-hapi, srvadmin-isvc und srvadmin-omacore
srvadmin-omilcore	Server Administrator Install Core - Dies ist das Kerninstallationspaket, welches die erforderlichen Hilfsprogramme für die restlichen Installationspakete von Systems Management enthält. Alle Server Administrator-RPMs benötigen diesen RPM.	

srvadmin-ssa	Ermöglicht die Verwaltung des Systems über WS-Man-Schnittstellen von einem Remote-System aus, auf dem Server Administrator Web Server installiert ist.	srvadmin-omacore, srvadmin-omhip und srvadmin-isvc.
srvadmin-syscheck	Paket, das den Grad der OpenManage-Unterstützung prüft.	srvadmin-omilcore

Welches sind die zusätzlichen Komponenten, die auf einem System installiert werden können, auf dem Server Administrator bereits installiert ist?

Es gibt einige zusätzliche Komponenten, die auf einem System installiert werden können, auf dem Server Administrator bereits installiert ist. So können Sie beispielsweise Online Diagnostics auf einem System installieren, auf dem sich die Managed System-Software bereits befindet. Auf einem solchen System werden bei einer Deinstallation von Server Administrator nur die RPM-Pakete deinstalliert, die nicht von einer der neu installierten Komponenten benötigt werden. Im obigen Beispiel benötigt

Online Diagnostics Pakete wie -

srvadmin-omilcore-X.Y.Z-N und **srvadmin-hapi-X.Y.Z-N**. Diese Pakete werden bei einer Deinstallation von Server Administrator nicht deinstalliert.

Wenn Sie in diesem Fall versuchen, Server Administrator
durch Ausführen des Befehls sh `srvadmin-install.sh` zu einem späteren Zeitpunkt zu installieren, wird die folgende Meldung angezeigt:

Server Administrator Version X.Y.Z ist derzeit installiert.

Installierte Komponenten:

- srvadmin-omilcore-X.Y.Z-N
- srvadmin-hapi-X.Y.Z-N

Möchten Sie Server Administrator auf X.Y.Z erweitern? Drücken Sie (**y** für ja | **Eingabe**, um zu beenden):

Nach Drücken von **y** werden im obigen Beispiel nur die Server Administrator-Pakete **srvadmin-omilcore-X.Y.Z-N** und **srvadmin-hapi-X.Y.Z-N**, die sich auf dem System befinden, erweitert.

Wenn Sie weitere Dell OpenManage-Komponenten installieren müssen, müssen Sie den folgenden Befehl nochmals ausführen:

```
sh srvadmin-install.sh
```

Was geschieht, wenn ich das RPM-Paket auf einem nicht unterstützten System oder unter einem nicht unterstützten Betriebssystem installiere?

Wenn Sie RPM-Pakete auf einem nicht unterstützten System oder unter einem nicht unterstützten Betriebssystem installieren, kommt es möglicherweise zu unvorhersehbarem Verhalten während der Installation oder Nutzung des RPM-Pakets. Die meisten RPM-Pakete wurden für Dell PowerEdge™ Systeme und die in dieser Infodatei aufgeführten Linux-Versionen entwickelt und getestet.

Welche Daemons werden auf den Red Hat Enterprise Linux- und SUSE Linux Enterprise Server-Betriebssystemen ausgeführt, nachdem Server Administrator gestartet wurde?

Welche Daemons auf den Red Hat Enterprise Linux- und SUSE Linux Enterprise Server-Betriebssystemen ausgeführt werden, hängt davon ab, was installiert und aktiviert wurde. Die folgende Tabelle bietet Aufschluss über die Daemons, die normalerweise nach einer vollständigen Installation ausgeführt werden:

Tabelle 11-4. Daemons, die auf Red Hat Enterprise Linux und SUSE Linux Enterprise Server ausgeführt werden, sobald Server Administrator gestartet wurde

Daemon-Name	Name in Red Hat Enterprise Linux und SUSE Linux Enterprise Server
Für RPMs im Srvadmin-Basisverzeichnis	
dsm_sa_datamgr32d	DSM SA Data Manager - Der Data Manager-Daemon von Server Administrator wurde vom DSM SA Data Engine-Dienst gestartet.
dsm_sa_eventmgr32d	DSM SA Event Manager - Der Ereignis- und Anmelde-Daemon von Server Administrator wurde vom DSM SA Data Engine-Dienst gestartet.
dsm_sa_snmp32d	DSM SA Data Manager-Daemon- Der Data Manager-Daemon von Server Administrator wurde vom DSM SA Data Engine-Dienst gestartet.
dsm_om_shrsvc32d	DSM SA-Freigabedienste - Server Administrator Core-Daemon.
Für RPMs im SA-WebServer-Verzeichnis	
dsm_om_connsvc32d	DSM SA-Verbindungsdienste - Server Administrator Web Server-Daemon.
Für Systeme, die DRAC 4: add-RAC4 unterstützen	
racsvc	DRAC 4 Administrator-Daemon

Welche Kernel-Module werden beim Start von Server Administrator geladen?

Dies hängt vom System-Instrumentationstyp ab. In der folgende Tabelle sind die Kernel-Module aufgeführt, die beim Start von Server Administrator geladen werden.

Tabelle 11-5. Nach dem Start der Server Administrator Services geladene Kernel-Module

Treibername	Beschreibung
Für ein System mit IPMI	
dell_rbu	Dell BIOS-Aktualisierungstreiber
ipmi_devintf	IPMI-Gerätetreiber

ipmi_msghandler	IPMI-Gerätetreiber
ipmi_si	IPMI-Gerätetreiber - Für Systeme, auf denen Red Hat Enterprise Linux (Version 4) oder SUSE Linux Enterprise Server (Version 10) ausgeführt wird
Für ein TVM-System	
dcdbas	Dell Systems Management-Basistreiber
dell_rbu	Dell BIOS-Aktualisierungstreiber
Für ein ESM-System	
dcdbas	Dell Systems Management-Basistreiber
dell_rbu	Dell BIOS-Aktualisierungstreiber
Für den Support von Server Administrator-Speichersystemen	
mptctl	Gerätetreiber für LSI RAID

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Glossar

Dell™ OpenManage™ Server Administrator Version 6.2- Installationshandbuch

In der folgenden Liste werden technische Begriffe, Abkürzungen und Akronyme definiert, die in den Systemdokumenten verwendet werden.

Anbieter

Ein Anbieter ist eine Erweiterung eines CIM-Schemas, die mit verwalteten Objekten kommuniziert und Daten und Ereignisbenachrichtigungen von einer Vielzahl von Quellen aufruft. Anbieter leiten diese Informationen für Integration und Interpretation an den CIM-Objektmanager weiter.

Attribut

In Bezug auf DMI ist ein Attribut ein Teil der Informationen zu einer Komponente. Attribute können zu Gruppen zusammengeschlossen werden. Wenn es sich um ein Lese-Schreib-Attribut handelt, kann es durch eine Verwaltungsanwendung definiert sein.

Bedienfeld

Der Teil des Systems, der die Anzeigen und Bedienelemente enthält, z. B. den Netzschalter, die Festplattenlaufwerk-Zugriffsanzeige und die Betriebsanzeige.

Bildschirmadapter

Siehe Videoadapter.

Bildwiederholfrequenz

Die Rate, mit der der Monitor das Bild auf den Bildschirm projiziert. Die Bildwiederholfrequenz ist die Frequenz in Hz, mit der die waagerechten Zeilen des Bildschirms neu gezeichnet werden (manchmal auch als Vertikalfrequenz bezeichnet). Je höher die Bildwiederholfrequenz ist, desto weniger Flimmern kann vom menschlichen Auge wahrgenommen werden. Die höheren Bildwiederholfrequenzen sind auch zeilensprungfrei.

BIOS

Akronym für Basic Input/Output System (Grundlegendes Eingabe-/Ausgabesystem). Das BIOS des Systems enthält Programme, die in einem Flash-Speicherchip gespeichert sind. Das BIOS steuert die folgenden Funktionen:

- Kommunikation zwischen dem Mikroprozessor und den Peripheriegeräten wie z. B. Tastatur und Videoadapter
- Verschiedene Hilfsfunktionen wie z. B. Systemmeldungen

BMC

Abkürzung für Baseboard-Verwaltungs-Controller, bei dem es sich um den Controller handelt, der die Intelligenz in der IPMI-Struktur bereitstellt.

Bus

Ein Leitungssystem zur Informationsübertragung zwischen den Komponenten eines Systems. Das System besitzt einen Erweiterungsbus, mit dessen Hilfe der Mikroprozessor mit den Controllern der verschiedenen an das System angeschlossenen Peripheriegeräte Daten austauschen kann. Zusätzlich enthält das System einen Adressbus und einen Datenbus für die Kommunikation zwischen Mikroprozessor und RAM.

CA

Abkürzung für Certification Authority (Zertifizierungsstelle).

CIM

Akronym für Common Information Model (Allgemeines Informationsmodell), ein Modell zur Beschreibung von Verwaltungsinformationen von der DMTF. CIM ist implementierungsunabhängig und ermöglicht es verschiedenen Verwaltungsanwendungen, die erforderlichen Daten aus einer Vielzahl von Quellen zu erfassen. CIM enthält Schemata für Systeme, Netzwerke, Anwendungen und Geräte; zudem werden neue Schemata hinzugefügt. Es enthält Zuweisungstechniken für den Austausch von CIM-Daten mit MIB-Daten von SNMP-Agenten.

CI/O

Abkürzung für Comprehensive Input/Output (Umfassende Eingabe/Ausgabe).

CLI

Abkürzung für Befehlszeilenoberfläche.

cm

Abkürzung für Zentimeter.

ConsoleOne

Novell® ConsoleOne® ist eine Java-basierte Oberfläche für Grafikdienstprogramme, die Netzwerkressourcen von verschiedenen Standorten und Plattformen aus steuern und verwalten. ConsoleOne enthält einen einzelnen Steuerungspunkt für alle Novell- und externen Produkte.

Controller

Ein Chip zur Steuerung der Datenübertragung zwischen Mikroprozessor und Speicher bzw. Mikroprozessor und Peripheriegerät (wie z. B. einem Festplattenlaufwerk oder einer Tastatur).

DHCP

Abkürzung für Dynamic Host Configuration Protocol (Dynamisches Host-Konfigurationsprotokoll), ein Protokoll zur dynamischen Zuweisung von IP-Adressen an Computer in einem LAN.

Dienstprogramm

Ein Programm zum Verwalten von Systemressourcen, z. B. Speicher, Festplattenlaufwerke oder Drucker.

Dienstprogramm-Partition

Ein startbare Partition auf der Festplatte, die Dienstprogramme und Diagnoseprogramme für die Hardware und Software enthält. Wenn sie aktiviert wird, startet die Partition und stellt eine ausführbare Umgebung für die Dienstprogramme auf der Partition bereit.

DIN

Akronym für Deutsche Industrie-Norm, die Organisation, die in Deutschland für die Bestimmung von Normen verantwortlich ist. Ein DIN-Anschluss ist ein Anschluss, der einem der vielen DIN-definierten Standards entspricht. DIN-Anschlüsse sind in Personalcomputern weit verbreitet. So stellt beispielsweise der Tastaturanschluss für Personalcomputer einen DIN-Anschluss dar.

DKS

Abkürzung für Dynamic Kernel Support (Dynamische Kernel-Unterstützung).

DNS

Abkürzung für den Domänennamensdienst.

DRAC 4

Akronym für Dell™ Remote Access Controller 4.

DRAM

Akronym für Dynamic Random-Access Memory (Dynamischer Speicher mit wahlfreiem Zugriff). Der RAM eines Systems besteht normalerweise nur aus DRAM-Chips. Da DRAM-Chips elektrische Ladung nicht auf unbegrenzte Zeit speichern können, wird jeder DRAM-Chip fortwährend aktualisiert.

E/A

Abkürzung für Eingabe/Ausgabe. Die Tastatur ist ein Eingabegerät und ein Drucker ein Ausgabegerät. Technisch wird zwischen E/A-Operationen und Rechenoperationen unterschieden. Wenn beispielsweise ein Programm ein Dokument an den Drucker sendet, erfolgt eine Ausgabeaktivität; wenn ein Programm eine Liste mit Begriffen sortiert, erfolgt eine Rechneraktivität.

Einstellungen

Einstellungen sind Bedingungen eines verwaltbaren Objekts, mit deren Hilfe definiert werden kann, was geschieht, wenn in einer Komponente ein bestimmter Wert festgestellt wird. Ein Benutzer kann z. B. den oberen kritischen Schwellenwert einer Temperatursonde auf 75 °C einstellen. Wenn die Sonde diese Temperatur erreicht, wird durch die Einstellung das Senden einer Warnungsnachricht an die Verwaltungskonsole veranlasst, so dass der Benutzer eingreifen kann. Manche Einstellungen können bei Erreichung das Herunterfahren des Systems oder andere Reaktionen auslösen, die Schäden am System verhindern können.

ERA

Abkürzung für Embedded Remote Access (Integrierter Remote-Zugriff).

ERA/MC

Abkürzung für Embedded Remote Access Modular Computer (Integrierter Remote-Zugriff/modularer Computer). Siehe Modulares System.

ERA/O

Abkürzung für Embedded Remote Access Option (Integrierte Remote-Zugriffsoption).

Erweiterungskartensteckplatz

Ein Steckplatz auf der Systemplatine des Systems, in dem die Erweiterungskarte installiert wird.

Erweiterungsspeicher

RAM oberhalb der 1 MB-Grenze. Die meisten Softwareprogramme, die diesen Speicher benutzen können (z. B. das Microsoft® Windows®-Betriebssystem), erfordern, dass sich ein Erweiterungsspeicher unter der Kontrolle eines XMM befindet.

Externer Cache-Speicher

Ein RAM-Cache, der SRAM-Chips verwendet. Da SRAM-Chips wesentlich schneller als DRAM-Chips sind, kann der Mikroprozessor Daten und Anweisungen schneller aus dem externen Cache-Speicher als dem RAM einlesen.

F

Abkürzung für Fahrenheit.

FAT

Akronym für File Allocation Table (Dateizuordnungstabelle). FAT und FAT32 sind Dateisysteme, die wie folgt definiert werden:

- **FAT** - Das Betriebssystem verwaltet eine Tabelle zur Beobachtung des Status verschiedener Segmente der Festplatte, die zum Speichern von Dateien verwendet werden.
- **FAT32** - Abgeleitet vom FAT-Dateisystem. FAT32 unterstützt kleinere Cluster-Formate als FAT und sorgt dadurch für effizientere Kapazitätsausnutzung auf FAT32-Laufwerken.

Fibre-Channel

Eine Datenübertragungs-Schnittstellentechnik, die Hochgeschwindigkeits-E/A- und Netzwerkfunktionen in einer Anschlusstechnologie vereint. Der Fibre Channel-Standard unterstützt mehrere Topologien, einschließlich Fibre Channel-Point-to-Point, Fibre Channel-Architektur (generische Schalttopologie) und willkürliche Fibre Channel-Schleife (FC_AL).

Firmware

Software (Programme oder Daten), die in den Nur-Lese-Speicher (ROM) geschrieben wurde. Die Firmware kann ein Gerät starten und betreiben. Jeder Controller enthält Firmware, die hilft, seine Funktionalität bereitzustellen.

Formatieren

Der Vorgang, mit dem ein Festplattenlaufwerk oder eine Diskette auf die Dateispeicherung vorbereitet wird. Ein uneingeschränkter Formatierungsbefehl löscht alle gespeicherten Daten vom Datenträger.

FSMO

Abkürzung für Flexible Single Master Operation (Flexibler Einzelbetriebsmaster).

FTP

Abkürzung für File Transfer Protocol (Dateiübertragungsprotokoll).

GB

Abkürzung für Gigabyte. Ein Gigabyte entspricht 1.024 Megabyte oder 1.073.741.824 Byte.

gcc

Abkürzung für GNU-C-Compiler.

Gerätetreiber

Ein Programm, mit dem das Betriebssystem oder ein anderes Programm mit einem Peripheriegerät wie z. B. einem Drucker korrekt kommunizieren kann. Einige Gerätetreiber wie z. B. Netzwerktreiber müssen von der Startdatei config.sys (mit der Aussage device=) oder als speicherresidente Programme (normalerweise über die autoexec.bat-Datei) geladen werden. Andere, wie z. B. Videotreiber, müssen jeweils bei Aufruf des Programms, für das sie zu verwenden sind, geladen werden.

GNU

Akronym für GNU's Not Unix® (Nicht-Unix® [-Software] von GNU). GNU-Software ist unter der GPL-Open-Source-Lizenz veröffentlicht.

GPG

Abkürzung für GNU Privacy Guard (GNU-Datenschutz).

GUI

Akronym für Graphical User Interface (Graphische Benutzeroberfläche).

GUID

Akronym für Globally Unique Identifier (Globaler eindeutiger Kennzeichner).

h

Abkürzung für hexadezimal. Bezeichnung für eine Zahl aus dem 16er-System, mit der beim Programmieren oft die Adressen im RAM des Systems und die E/A-Adressen der Peripheriegeräte identifiziert werden. Die Folge von dezimalen Zahlen von 0 bis 16 wird z. B. in der Hexadezimal-Notation ausgedrückt als: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F, 10. In einem Text folgt auf Hexadezimalzahlen häufig ein h.

HBA

Abkürzung für Host Bus Adapter (Host-Bus-Adapter). Eine PCI-Adapterkarte, die sich in dem System befindet, dessen einzige Funktion es ist, Datenbefehle vom PCI-Busformat zum Speicherverbindungsformat (Beispiele: SCSI, Fibre Channel) zu konvertieren und direkt mit Festplattenlaufwerken, Bandlaufwerken, CD-Laufwerken und anderen Speichergeräten zu kommunizieren.

HTTP

Abkürzung für Hypertext Transfer Protocol (Hypertextübertragungsprotokoll). HTTP ist das Client-Server TCP/IP-Protokoll, das auf dem World Wide Web für den Austausch von HTML-Dokumenten verwendet wird.

HTTPS

Abkürzung für HyperText Transmission Protocol, Secure. Bei HTTPS handelt es sich um eine Variante von HTTP, die von Web Browsern zum Abwickeln sicherer Transaktionen verwendet wird. HTTPS ist ein eindeutiges Protokoll, bei dem SSL unter HTTP eingesetzt wird. Für HTTP-URLs mit SSL verwenden Sie "https://", während für HTTP-URLs ohne SSL weiterhin "http://" verwendet wird.

ICES

Abkürzung für Interface-Causing Equipment Standard (in Canada) (Standard zur Frequenzstörfreiheit von Geräten, in Kanada).

ICMP

Abkürzung für Internet Control Message Protocol (Internet-Steuerungsmeldungsprotokoll). ICMP ist ein TCP/IP-Protokoll, das zum Senden von Fehler- und Steuerungsmeldungen verwendet wird.

ICU

Abkürzung für ISA Configuration Utility (ISA-Konfigurationsdienstprogramm).

ID

Abkürzung für Identifikation, Kennung.

IDE

Abkürzung für Integrated Drive Electronics (Integrierte Laufwerkelektronik). IDE ist eine Computersystem-Schnittstelle, die in der Hauptsache für Festplattenlaufwerke und CDs verwendet wird.

iDRAC

Akronym für Integrated Dell Remote Access Controller.

IHV

Abkürzung für Independent Hardware Vendor (Unabhängiger Hardwareanbieter). IHV entwickeln oft ihre eigenen MIBs für Komponenten, die sie selbst herstellen.

Infodatei

Eine der Software oder Hardware beigefügte Textdatei mit ergänzenden oder aktualisierenden Informationen zur gelieferten Software- oder Hardwaredokumentation. Normalerweise enthalten Infodateien Installationsinformationen und Beschreibungen zu neuen Produktverbesserungen oder -veränderungen, die in der Dokumentation noch nicht berücksichtigt wurden, und zeigen bekannte Probleme oder andere Informationen auf, die für die Verwendung der Hardware oder Software bekannt sein müssen.

Interlacing

Verfahren zur Erhöhung der Videoauflösung, indem die horizontalen Zeilen auf dem Bildschirm nur abwechselnd aktualisiert werden. Da Interlacing zu sichtbarem Bildschirmflimmern führen kann, bevorzugen die meisten Benutzer zeilensprungfreie Bildschirmauflösungen.

IP address (IP-Adresse)

Abkürzung für Internet Protocol Address (Internet-Protokolladresse). Siehe TCP/IP.

IPMI

Abkürzung für Intelligent Platform Management Interface, ein Industriestandard für die Verwaltung von Peripheriegeräten in Unternehmen, die mit einer Intel®-Architektur arbeiten. Das Hauptmerkmal von IPMI ist, dass die Steuerungsfunktionen für Bestandsaufnahme, Überwachung, Protokollierung und Wiederherstellung unabhängig von den Hauptprozessoren, dem BIOS und dem Betriebssystem verfügbar sind.

IRQ

Abkürzung für Interrupt Request (Interrupt-Anforderungen). Ein Signal, dass Daten in Kürze an ein Peripheriegerät ausgegeben oder von einem Peripheriegerät empfangen werden, wird über eine IRQ-Leitung zum Mikroprozessor geleitet. Jeder Peripherieverbindung muss eine eigene IRQ-Nummer zugewiesen werden. Beispiel: Die erste serielle Schnittstelle des Systems (COM1) ist standardmäßig IRQ4 zugewiesen. Zwei Geräte können sich dieselbe IRQ-Zuweisung teilen, diese kann dann aber nicht gleichzeitig verwendet werden.

ISV

Abkürzung für Independent Software Vendor (Unabhängiger Softwareanbieter).

ITE

Abkürzung für Information Technology Equipment (Informationstechnische Geräte).

Java

Eine plattformübergreifende Programmiersprache, die von Sun Microsystems entwickelt wurde.

JSSE

Abkürzung für Java Secure Socket Extension (Sichere JAVA-Sockelerweiterung).

K

Abkürzung für Kilo- (gibt 1000 an).

Kerberos

Ein Netzwerk-Authentifizierungsprotokoll. Es wurde entwickelt, um starke Authentifizierung für Client/Server-Anwendungen durch die Verwendung der Secret-Key-Kryptographie zu bieten.

LAN

Akronym für Local Area Network (Lokales Netzwerk). Ein LAN-System ist normalerweise auf ein und dasselbe oder einige benachbarte Gebäude beschränkt, wobei alle Geräte in einem Netzwerk durch Verkabelung fest miteinander verbunden sind.

LDAP

Abkürzung für Lightweight Directory Access Protocol (Lightweight-Verzeichniszugriffsprotokoll).

LDIF

Abkürzung für Lightweight Directory Interchange Format (ein Verzeichnisaustauschformat)

Local Bus

Für ein System mit Local Bus-Expansionsfähigkeit können bestimmte Peripheriegeräte (z. B. Videoadapter) so entwickelt werden, dass sie wesentlich schneller arbeiten als mit einem herkömmlichen Expansionsbus. Einige Local Bus-Konstruktionen erlauben Peripheriegeräten, mit derselben Taktrate und Datenpfadbreite wie der Mikroprozessor des Systems zu arbeiten.

LRA

Abkürzung für Local Response Agent (Lokaler Antwortagent).

Management Station

Ein System, mit dem ein oder mehrere Managed Systems von einem zentralen Standort aus entfernt verwaltet werden.

Mathematischer Coprozessor

Siehe Coprozessor.

Maus

Ein Zeigegerät, das die Cursor-Bewegungen auf dem Bildschirm steuert. Mit mausorientierter Software können Befehle aufgerufen werden, indem der Zeiger auf das dargestellte Objekt bewegt und mit einer Maustaste geklickt wird.

Mb

Abkürzung für Megabit.

MB

Abkürzung für Megabyte. Der Begriff Megabyte bedeutet 1.048.576 Byte; bei der Bezeichnung der Festplattenkapazität wird der Begriff häufig als Synonym für 1.000.000 Byte verwendet.

MIB

Akronym für Management Information Base (Verwaltungsinformationsbasis). MIB wird zum Senden detaillierter Status- bzw. Befehlsinformationen von einer oder an eine SNMP-verwaltete Komponente verwendet.

Mikroprozessor

Der primäre Rechnerchip im Innern des Systems, der die Auswertung und Ausführung von arithmetischen und logischen Funktionen steuert. Wenn Software für einen bestimmten Mikroprozessortyp geschrieben wurde, muss sie normalerweise für einen anderen Mikroprozessor umgeschrieben werden. CPU ist ein Synonym für Mikroprozessor.

mm

Abkürzung für Millimeter.

MMC

Abkürzung für Microsoft Management Console.

Modulares System

Ein System, das mehrere Servermodule enthalten kann. Jedes Servermodul arbeitet als eigenständiges System. Um als System arbeiten zu können, wird ein Servermodul in ein Gehäuse mit Netzteilen, Lüftern, einem Systemverwaltungsmodul und mindestens einem Netzwerkschaltermodul eingesetzt. Die Netzteile, Lüfter, das Systemverwaltungsmodul und das Netzwerkschaltermodul stellen gemeinsam genutzte Ressourcen der Servermodule im Gehäuse dar. Siehe Servermodul.

MOF

Akronym für Managed Object Format (Verwaltetes Objektformat), eine ASCII-Datei mit der formalen Definition eines CIM-Schemas.

MPEG

Akronym für Motion Picture Experts Group (wörtl.: Expertengruppe für bewegte Bilder). MPEG ist ein digitales Videodateiformat.

ms

Abkürzung für Millisekunden.

Name

Der Name eines Objekts oder einer Variablen entspricht genau der Zeichenkette, die es/sie in einer SNMP-Managementinformationsbank-Datei (MIB) oder in einer CIM-Verwaltungsobjektdatei (MOF) kenntlich macht.

NDS

Abkürzung für NovellDirectory Service.

Netzteil

Ein elektrisches System, das Wechselstrom von der Netzsteckdose in den von den Systemschaltkreisen erforderten Gleichstrom umwandelt. Das Netzteil in einem Personalcomputer erzeugt normalerweise mehrere Spannungen.

NIC

Akronym für Network Interface Karte (Netzwerkschnittstellenkarte).

NIS

Abkürzung für Netzwerk-Informations-Dienstleistungen. NIS ist ein Netzwerkverzeichnis- und Verwaltungssystem für kleinere Netzwerke. Ein Benutzer an einem beliebigen Host kann mit einer Benutzeridentifikation und einem Kennwort auf Dateien oder Anwendungen auf einem beliebigen Host im Netzwerk zugreifen.

Non-Interlaced

Eine Technik, um Bildschirmflimmern zu vermindern, indem jede horizontale Zeile auf dem Bildschirm aktualisiert wird.

ns

Abkürzung für Nanosekunde, ein Milliardstel einer Sekunde.

NTFS

Abkürzung für die Microsoft Windows NT®-Dateisystem-Option (NT-Dateisystem) des Betriebssystems Windows NT. NTFS ist ein erweitertes Dateisystem speziell zur Verwendung im Windows NT-Betriebssystem. Es unterstützt Dateisystemwiederherstellung, extrem umfangreiche Speicherkapazitäten und lange Dateinamen. Es unterstützt auch objektorientierte Anwendungen durch die Behandlung aller Dateien als Objekte mit benutzerdefinierten und systemdefinierten Attributen. Siehe auch FAT und FAT32.

NTLM

Abkürzung für Windows NT LAN Manager. NTLM ist das Sicherheitsprotokoll für das Windows NT-Betriebssystem. NTLM ist jetzt als Integrierte Windows-Authentifizierung bekannt.

Nur-Lese-Datei

Eine Nur-Lese-Datei kann weder bearbeitet noch gelöscht werden. Eine Datei kann Nur-Lese-Status haben, wenn folgendes zutrifft:

- Das Nur-Lese-Attribut ist aktiviert.
- Es befindet sich auf einer physisch schreibgeschützten Diskette oder auf einer Diskette in einem schreibgeschützten Laufwerk.
- Die Datei befindet sich in einem Netzwerkverzeichnis, für das Ihnen der Systemadministrator ausschließlich Leserechte zugewiesen hat.

Oberer Speicherbereich

Speicher im RAM-Bereich zwischen 640 KByte und 1 MByte. Wenn sich im System ein Intel386er oder höherer Mikroprozessor befindet, kann ein Speicherverwalter-Dienstprogramm UMBs im oberen Speicherbereich bereitstellen, in denen Gerätetreiber und speicherresidente Programme geladen werden.

OID

Abkürzung für Object Identifier (Objektbezeichner). Ein einsatzspezifischer Integer oder Zeiger, der ein Objekt eindeutig kenntlich macht.

Online-Zugriffsdienst

Ein Dienst, der gewöhnlich den Zugang zu Internet, E-Mail, Bulletin-Boards, Chat-Räumen und Dateibibliotheken anbietet.

PAM

Akronym für Pluggable Authentication Modules (Steckbare Authentifizierungsmodule). PAM ermöglicht es Systemadministratoren, eine Authentifizierungsregelung zu erstellen, ohne Authentifizierungsprogramme erneut kompilieren zu müssen.

Parallele Schnittstelle

Eine E/A-Schnittstelle, über die ein Paralleldrucker am System angeschlossen werden kann. Der parallele Anschluss des Systems ist an seiner 25-poligen Steckbuchse zu erkennen.

Parameter

Ein Wert oder eine Option, die von einem Programm gefordert wird. Ein Parameter wird manchmal auch als Schalter oder Argument bezeichnet.

Partition

Ein Festplattenlaufwerk kann mit dem Befehl fdisk in mehrere physikalische Abschnitte, so genannte Partitionen, unterteilt werden. Jede Partition kann über mehrere logische Laufwerke verfügen. Nach dem Partitionieren des Festplattenlaufwerks muss jedes logische Laufwerk mit dem Befehl "format" formatiert werden.

PC-Karte

Ein kreditkartengroßes, herausnehmbares Modul für portable Computer, standardisiert durch PCMCIA. PC-Karten (auch als PCMCIA-Karten bezeichnet) sind 16-Bit- Geräte zum Anschließen von Modems, Netzwerkadaptern, Soundkarten, Funkempfängern, Festkörperplatten und Festplattenlaufwerken an einen tragbaren Computer. Die PC-Karte ist ein "Plug-and-Play"-Gerät, das automatisch von der Kartendienstsoftware konfiguriert wird.

PCI

Abkürzung für Peripheral Component Interconnect (Verbindung peripherer Komponenten). Der vorherrschende, von Intel Corporation entwickelte 32-Bit- oder 64-Bit-Lokalbusstandard.

PERC

Akronym für Erweiterbarer RAID-Controller.

Peripheriegerät

Ein mit dem System verbundenes internes oder externes Gerät, z. B. ein Drucker, ein Festplattenlaufwerk oder eine Tastatur.

Physikalisches Speicher-Array

Das physikalische Speicher-Array ist der gesamte physikalische Speicher eines Systems. Variablen für den physikalischen Speicher sind Höchstumfang, Gesamtanzahl an Speichersteckplätzen auf der Hauptplatine und Gesamtanzahl der belegten Steckplätze.

Pixel

Ein einzelner Punkt auf einem Bildschirm. Pixel werden in Zeilen und Spalten zu ganzen Bildern zusammengestellt. Die Grafikauflösung wie z. B. 640 × 480 wird durch die Anzahl der horizontalen und vertikalen Bildpunkte ausgedrückt.

Plug-and-Play

Ein Industriestandard, mit dem Hardware-Geräte leichter an Personalcomputer angeschlossen werden können. Plug-and-Play bietet automatische Installation

und Konfiguration, ist kompatibel mit bereits vorhandener Hardware und unterstützt mobile Computerumgebungen.

ppm

Abkürzung für Pages Per Minute (Seiten pro Minute).

PPP

Abkürzung für Point-to-Point Protocol (Punkt-zu-Punkt-Protokoll).

Programmdiskettensatz

Der Diskettensatz, mit dem die vollständige Installation eines Betriebssystems oder eines Anwendungsprogramms durchgeführt werden kann. Beim erneuten Konfigurieren eines Programms wird oft dessen Diskettensatz benötigt.

RAC

Akronym für Remote Access Controller (Remote Access Controller).

RAID

Akronym für Redundant Array of Independent Drives (Redundantes Array unabhängiger Laufwerke).

RAM

Akronym für Random Access Memory (Speicher mit wahlfreiem Zugriff). Der primäre und temporäre Speicherbereich des Systems für Programminstruktionen und Daten. Jeder Bereich im RAM ist durch eine Zahl gekennzeichnet, die so genannte Speicheradresse. Beim Ausschalten des Systems gehen alle im RAM abgelegten Daten und Befehle verloren.

RBAC

Abkürzung für Role-Based Access Control (Funktionsbasierte Zugriffskontrolle).

Realmodus

Ein Betriebsmodus, der von 80286er oder höheren Mikroprozessortypen unterstützt wird und die Architektur eines 8086er Mikroprozessors emuliert.

Remote-Verwaltungssystem

Ein Remote-Verwaltungssystem ist ein beliebiges System, das von einem entfernten Standort aus mithilfe eines unterstützten Web-Browsers auf die Server Administrator-Startseite auf einem verwalteten System zugreift. Siehe Managed System.

ROM

Akronym für Read-Only Memory (Nur-Lese-Speicher). Einige der für den Einsatz des Systems wesentlichen Programme befinden sich im ROM. Im Gegensatz zum RAM geht der Inhalt des ROM-Chips beim Ausschalten des Systems nicht verloren. Ein Beispiel für Code im ROM ist das Programm, das die Startroutine des Systems und den POST einleitet.

RPM

Abkürzung für Red Hat® Package Manager (Red Hat-Paketverwaltung).

SAN

Akronym für Storage Area Network (Speicherbereichsnetzwerk).

SAS

Das Akronym für seriell verbundene SCSI-Schnittstelle.

SCA

Abkürzung für Single Connector Attachment (Einzelanschlussanlage).

Schema

Eine Zusammenstellung von Klassendefinitionen, die verwaltete Objekte in einer bestimmten Umgebung beschreibt. Ein CIM-Schema ist eine Zusammenstellung von Klassendefinitionen, mit denen verwaltete Objekte dargestellt werden, die in jeder Verwaltungsumgebung vorkommen - daher die Bezeichnung allgemeines Informationsmodell (CIM).

Schreibgeschützt

Dateien, auf die nur ein Lesezugriff möglich ist, sind schreibgeschützt. Eine 3,5-Zoll-Diskette kann durch Verschieben der Schreibschutzkerbe in die offene Position oder durch Einstellen der Schreibschutzfunktion im System-Setup-Programm schreibgeschützt werden.

Schutzmodus

Ein Betriebsmodus, der von 80286er oder höheren Mikroprozessortypen unterstützt wird und dem Betriebssystem folgende Funktionen ermöglicht:

- Ein Speicheradressbereich von 16 MB (80286 Mikroprozessor) bis 4 GB (Intel386 oder höherer Mikroprozessor)
- Multitasking
- Virtueller Speicher, ein Verfahren, um den adressierbaren Speicherbereich durch Verwendung des Festplattenlaufwerks zu vergrößern.

Schwellenwerte

Systeme sind üblicherweise mit verschiedenen Sensoren ausgerüstet, die Temperatur, Spannung, Strom und Lüfterdrehzahl überwachen. Die Sensorschwellenwerte legen die Bereiche (minimale und maximale Werte) fest, um zu bestimmen, ob der Sensor unter normalen, nicht kritischen, kritischen oder schwerwiegenden Bedingungen arbeitet. Server Administrator-unterstützte Schwellenwerte sind

- UpperThresholdFatal
- UpperThresholdCritical
- UpperThresholdNon-critical
- Normal
- LowerThresholdNon-critical
- LowerThresholdCritical
- LowerThresholdFatal

SCSI

Akronym für Small Computer System Interface (Schnittstelle für kleine Computersysteme). Eine E/A-Busschnittstelle mit höheren Datenübertragungsraten als herkömmliche Schnittstellen. Es können bis zu sieben Geräte an eine SCSI-Schnittstelle angeschlossen werden (15 bei bestimmten neueren SCSI-Typen).

Secure Port-Server

Eine Anwendung, mit der Webseiten verfügbar sind zur Anzeige über Web-Browsern unter Verwendung des HTTPS-Protokolls. Siehe Web-Server.

SEL

Akronym für System Event Log (Systemereignisprotokoll).

Sek.

Abkürzung für Sekunde.

Serielle Schnittstelle

Eine E/A-Schnittstelle, die meistens dazu verwendet wird, ein Modem an ein System anzuschließen. Die serielle Schnittstelle ist normalerweise an ihrer 9-poligen Buchse zu erkennen.

Servermodul

Eine modulare Systemkomponente, die als eigenständiges System arbeitet. Um als System arbeiten zu können, wird ein Servermodul in ein Gehäuse mit Netzteilen, Lüftern, einem Systemverwaltungsmodul und mindestens einem Netzwerkschaltermodul eingesetzt. Die Netzteile, Lüfter, das Systemverwaltungsmodul und das Netzwerkschaltermodul sind freigegebene Ressourcen der Servermodule im Gehäuse. Siehe Modulares System.

Service-Tag-Nummer

Ein Strichcode-Etikett, anhand dessen jedes System identifiziert werden kann, wenn man sich an den Kundendienst oder den technischen Support wenden muss.

Signaltoncode

Eine diagnostische Meldung in Form einer Serie von Signaltonmustern, die über den Lautsprecher des Systems ausgegeben wird. Ein Signalton, gefolgt von einem zweiten Signalton und anschließend einer Folge von drei Signaltönen stellt den Signaltoncode 1-1-3 dar.

SIMM

Akronym für Single In-line Memory Module (Speichermodul mit einer Kontaktanschlussreihe). Eine kleine Platine mit DRAM-Chips, die an die Systemplatine angeschlossen ist.

SMTP

Abkürzung für Simple Mail Transfer Protocol (Einfaches Mail-Übertragungsprotokoll).

SNMP

Abkürzung für Simple Network Management Protocol (Einfaches Netzwerkverwaltungsprotokoll). SNMP, ein beliebtes Netzwerksteuerungs- und Überwachungsprotokoll, ist Teil der ursprünglichen TCP/IP-Protokollgruppe. SNMP enthält das Format, in dem wichtige Informationen über verschiedene Netzwerkgeräte, z. B. Netzwerkserver oder -router, an die Verwaltungsanwendung gesendet werden können.

Speicher

Ein System kann verschiedene Speichertypen besitzen, wie RAM, ROM und Videospeicher. Das Wort Speicher wird oft als Synonym für RAM verwendet. Zum Beispiel bedeutet die Aussage "ein System mit 16-MB-Speicher", dass es sich um ein System mit 16 MB RAM handelt.

Speicheradresse

Eine bestimmte Adresse im RAM des Systems, die als hexadezimale Zahl angegeben wird.

Spiegeln

Der System- und Video-BIOS-Code eines Computers wird normalerweise auf ROM-Chips gespeichert. Spiegeln (Shadowing) bezieht sich auf eine leistungssteigernde Technik, bei der der BIOS-Code während der Startroutine in schnelleren RAM-Chips im oberen Speicherbereich (oberhalb von 640 KB) abgelegt wird.

SRAM

Abkürzung für Static Random-Access Memory (Statischer Speicher mit wahlfreiem Zugriff). Da SRAM-Chips nicht fortwährend aktualisiert werden müssen, sind sie wesentlich schneller als DRAM-Chips.

SSL

Abkürzung für Secure Socket Layer (Sichere Sockelschicht).

Startfähige Diskette

Sie können das System von einer Diskette aus starten. Zum Erstellen einer startfähigen Diskette legen Sie eine Diskette in das Diskettenlaufwerk ein, geben

sys a: in die Befehlszeile ein und drücken die<Eingabetaste>. Verwenden Sie diese startfähige Diskette, wenn Ihr System nicht von der Festplatte startet.

Startroutine

Sie löscht beim Systemstart den gesamten Speicher, initialisiert die Geräte und lädt das Betriebssystem. Sofern das Betriebssystem nicht versagt, kann das System mit der Tastenkombination <Strg><Alt><Entf>; neu gestartet werden (auch Warmstart genannt); ansonsten muss durch Drücken der Reset-Taste oder durch Aus- und wieder Einschalten des Systems ein Kaltstart durchgeführt werden.

Status

Bezieht sich auf die Funktionsbereitschaft eines Objekts. Eine Temperatursonde kann z. B. den Status normal haben, wenn die Sonde akzeptable Temperaturen misst. Wenn die Sonde Temperaturen zu registrieren beginnt, welche die vom Benutzer eingestellten Schwellenwerte überschreiten, zeigt sie einen kritischen Status an.

Stromeinheit

Eine Gruppe von Netzteilen in einem Systemgehäuse.

SVGA

Abkürzung für Super Video Graphics Array (Super-Video-Grafikanordnung). VGA und SVGA sind Standards für Grafikkarten, die sich im Vergleich zu früheren Standards durch höhere Auflösungen und größere Farbtiefe auszeichnen.

Um ein Programm mit einer bestimmten Auflösung wiederzugeben, müssen die entsprechenden Videotreiber installiert sein und der Monitor muss die gewünschte Auflösung unterstützen. Die Anzahl der Farben, die ein Programm anzeigen kann, hängt von der Leistungsfähigkeit des Monitors, dem Videotreiber und der Größe des im System installierten Videospeichers ab.

Switch

Schalter (Switches) kontrollieren verschiedene Schaltkreise auf der Systemplatine bzw. steuern verschiedene Funktionen im Computersystem. Diese Schalter sind als DIP-Schalter bekannt; sie sind normalerweise in Gruppen von zwei oder mehr Schaltern in einem Plastikgehäuse untergebracht. Zwei allgemeine DIP-Schalter werden auf Systemplatinen verwendet: Schiebeschalter und Kippschalter. Die Namen der Schalter basieren darauf, wie die Einstellungen (ein und aus) der Schalter geändert werden.

Syntax

Die Regeln, die bei der Eingabe einer Instruktion oder eines Befehls zu befolgen sind, damit das System die Eingabe ordnungsgemäß verarbeiten kann. Die Syntax einer Variablen zeigt ihren Datentyp an.

Systemkonfigurationsdaten

Im Speicher abgelegte Daten, die dem System mitteilen, welche Hardware installiert ist und wie das System für den Betrieb konfiguriert sein sollte.

Systemdiskette

Systemdiskette ist ein Synonym für Startfähige Diskette.

Systemplatine

Auf der Hauptplatine des Systems befinden sich normalerweise die folgenden integrierten Systemkomponenten:

- Mikroprozessor
- RAM
- Controller für standardmäßige Peripheriegeräte wie z. B. die Tastatur
- Verschiedene ROM-Chips

Häufig verwendete Synonyme für Systemplatine sind Hauptplatine und Logikplatine.

Systemspeicher

Systemspeicher ist ein Synonym für RAM.

System-Setup-Programm

Mit diesem im BIOS abgespeicherten Programm kann die Hardware des Systems konfiguriert und die Arbeitsweise des Systems durch das Einrichten von Funktionen wie Kennwortschutz und Stromverwaltung angepasst werden. Bei einigen Optionen des System-Setup-Programms muss das System neu gestartet werden (oder das System startet automatisch neu), damit eine Änderung in der Hardwarekonfiguration wirksam wird. Da das System-Setup-Programm im NVRAM gespeichert ist, bleiben alle Einstellungen unverändert, bis sie erneut geändert werden.

system.ini-Datei

Eine Startdatei für das Betriebssystem Windows. Bei Aufruf des Windows-Betriebssystems wird zuerst die **system.ini**-Datei gelesen, um die verschiedenen Optionen für die Windows-Betriebsumgebung zu bestimmen. Unter anderem wird in der Datei **system.ini** festgehalten, welche Video-, Maus- und Tastaturtreiber für Windows installiert sind.

Durch Änderung der Einstellungen in der Systemsteuerung oder durch Aufruf des Windows-Setup-Programms könnten Optionen der Datei **system.ini** geändert werden. In anderen Fällen müssen eventuell mit einem Texteditor (z. B. Notepad) Optionen für die Datei **system.ini** manuell geändert oder hinzugefügt werden.

Tabelle

In SNMP-MIBs ist eine Tabelle ein zweidimensionales Array, das die Variablen beschreibt, aus denen sich ein verwaltetes Objekt zusammensetzt.

Tastenkombination

Ein Befehl, für den ein gleichzeitiges Drücken von mehreren Tasten erforderlich ist. Beispielsweise kann das System durch Drücken der Tastenkombination <Strg><Alt><Entf> neu gestartet werden.

TCP/IP

Abkürzung für Transmission Control Protocol/Internet Protocol (Übertragungssteuerungsprotokoll/Internetprotokoll). Ein System zur Übertragung von Informationen über ein Computernetzwerk mit unterschiedlichen Systemen, z. B. Systeme, die unter Windows und UNIX laufen.

Terminierung

Bestimmte Geräte (wie z. B. das letzte Gerät an jedem Ende eines SCSI-Kabels) müssen mit einem Abschlusswiderstand versehen werden, so dass Reflexionen und Störsignale im Kabel verhindert werden. Wenn solche Geräte in Reihe geschaltet werden, muss die Terminierung an diesen Geräten möglicherweise aktiviert bzw. deaktiviert werden, indem Jumper oder Schalterstellungen an den Geräten bzw. die Einstellungen in der Konfigurationssoftware der Geräte geändert werden.

Texteditor

Ein Anwendungsprogramm zum Bearbeiten von Textdateien, die ausschließlich aus ASCII-Zeichen bestehen. Windows Notepad ist z. B. ein Texteditor. Die meisten Textverarbeitungsprogramme verwenden programmspezifische Dateiformate mit Binärzeichen, obwohl einige auch Textdateien lesen und schreiben können.

Textmodus

Ein Videomodus kann als x Spalten mal y Reihen mit Zeichen definiert werden.

TFTP

Abkürzung für Trivial File Transfer Protocol (Trivial-Dateiübertragungsprotokoll). TFTP ist eine Version des TCP/IP-FTP-Protokolls, das keine Verzeichnis- und Kennwortfunktionen umfasst.

tpi

Abkürzung für Tracks per Inch (Spuren pro Zoll).

TSR

Akronym für Terminate-and-Stay-Resident (Beenden und im Speicher verbleiben). Ein TSR-Programm wird "im Hintergrund" ausgeführt. Die meisten TSR-Programme implementieren eine vordefinierte Tastenkombination (manchmal als Kurztaste bezeichnet), mit der Sie die Oberfläche des TSR-Programms während der Ausführung eines anderen Programms aktivieren können. Nach Ablauf des TSR-Programms kann zum anderen Anwendungsprogramm zurückgekehrt werden und das TSR-Programm verbleibt im Speicher für spätere Einsätze. Manchmal können TSR-Programme Speicherkonflikte verursachen. Bei der Fehlersuche kann diese Möglichkeit ausgeschlossen werden, indem das System ohne das Abrufen von TSR-Programmen neu gestartet wird.

TSOP

Abkürzung für Thin Small Outline Package (Schmalprofilpaket). Ein sehr dünnes, rechteckiges, oberflächenmontiertes Chippaket aus Kunststoff mit Flügelstiften an beiden kurzen Seiten.

UDP

Abkürzung für User Datagram Protocol (Protokoll für Benutzerdatagramme).

UMB

Abkürzung für Upper Memory Blocks (Obere Speicherblöcke).

Unicode

Eine weltweite 16-Bit-Zeichenverschlüsselung mit fester Breite, die vom Unicode Consortium entwickelt wurde und gepflegt wird.

URL

Abkürzung für Uniform Resource Locator (Einheitliche Ressourcenadresse), (früher: Universal Resource Locator=Uniformer Ressourcencode).

USB

Akronym für Universal Serial Bus (Universeller serieller Bus). Ein USB-Anschluss stellt einen einzelnen Anschlusspunkt für mehrere USB-kompatible Geräte wie z. B. Mausgeräte, Tastaturen, Drucker und Computerlautsprecher. USB-Geräte können auch angeschlossen und getrennt werden, während das System ausgeführt wird.

VarBind

Ein Algorithmus, der zur Zuweisung eines Objektkennzeichners (OID) verwendet wird. Der varbind-Algorithmus stellt Regeln zum Erhalten des Dezimalpräfixes auf, das ein Unternehmen eindeutig kennzeichnet, sowie die Formel zur Festlegung einer eindeutigen Kennung von Objekten, die im MIB des Unternehmens definiert sind.

Variable

Eine Komponente eines verwalteten Objekts. Eine Temperatursonde verfügt beispielsweise über eine Variable, die ihre Fähigkeiten, ihren Zustand oder Status und verschiedene Indizes beschreibt, die bei der Suche nach der korrekten Temperatursonde behilflich sein können.

Verwaltetes System

Ein Managed System ist ein System, das nithilfe von Dell OpenManage™ Server Administrator überwacht und verwaltet wird. Systeme, auf denen Server Administrator ausgeführt wird, können lokal oder entfernt über einen unterstützten Web-Browser verwaltet werden. Siehe Remote-Verwaltungssystem.

Verzeichnis

Mithilfe von Verzeichnissen können Dateien auf einer Festplatte in einer hierarchischen Struktur (ähnlich der eines umgekehrten Baumes) organisiert werden. Jede Festplatte hat ein "Stamm"-Verzeichnis; so zeigt beispielsweise eine **C:\>**- Eingabeaufforderung normalerweise an, dass Sie sich beim Stammverzeichnis des Festplattenlaufwerks C befinden. Weitere Verzeichnisse, die vom Stammverzeichnis abzweigen, werden Unterverzeichnisse genannt. Von Unterverzeichnissen können zusätzliche Verzeichnisse abzweigen.

VGA

Abkürzung für Video Graphics Array (Videografikanordnung). VGA und SVGA sind Standards für Grafikkarten, die sich im Vergleich zu früheren Standards durch höhere Auflösungen und größere Farbtiefe auszeichnen. Zur Wiedergabe eines Programms mit einer bestimmten Auflösung müssen die entsprechenden Videotreiber installiert sein und der Monitor muss die gewünschte Auflösung unterstützen. Die Anzahl der von einem Programm wiedergegebenen Farben hängt von den Fähigkeiten des Bildschirms, des Videotreibers und der Größe des für den Videoadapter installierten Videospeichers ab.

VGA-Funktionsanschluss

In einigen Systemen mit einem integrierten VGA-Videoadapter ermöglicht ein VGA-Funktionsanschluss das Hinzufügen eines Erweiterungsadapters (z. B. ein Videobeschleuniger). Ein VGA-Funktionsanschluss wird auch VGA-Pass-Through-Anschluss genannt.

Videoadapter

Die Schaltkreise, die gemeinsam mit dem Monitor die Videomöglichkeiten des Systems realisieren. Ein Videoadapter kann mehr oder weniger Funktionen unterstützen als ein bestimmter Monitor. Zum Videoadapter gehören Videotreiber, mit denen populäre Anwendungsprogramme und Betriebssysteme in einer Vielfalt von Videomodi arbeiten können.

Bei einigen Systemen ist der Videoadapter in die Systemplatine integriert. Es sind auch viele Videoadapterkarten erhältich, die an einen Erweiterungskartenstecker angeschlossen werden können.

Videoadapter können zusätzlich zum RAM-Speicher auf der Systemplatine separaten Speicher aufweisen. Die Größe des Videospeichers kann außerdem zusammen mit den Videotreibern des Adapters die Anzahl der gleichzeitig darstellbaren Farben beeinflussen. Einige Videoadapter besitzen zudem ihren eigenen Coprozessorchip zur schnelleren Grafikverarbeitung.

Videoauflösung

Videoauflösung wie z. B. 800 × 600 wird durch die Anzahl der horizontalen und vertikalen Bildpunkte ausgedrückt. Damit ein Programm mit einer bestimmten Videoauflösung arbeitet, müssen die entsprechenden Videotreiber geladen sein und der Monitor muss die gewünschte Auflösung unterstützen.

Videomodus

Videoadapter unterstützen normalerweise mehrere Text- und Grafikmodi. Zeichenbasierte Software wird im Textmodus angezeigt, der durch *x* Spalten mal *y* Zeilen mit Zeichen definiert ist. Grafikbasierte Software wird im Grafikmodus ausgeführt, der durch *x* horizontale mal *y* vertikale Bildpunkte mal *z* Farben definiert ist.

Videospeicher

Die meisten VGA- und SVGA-Videoadapter enthalten zusätzlich zum RAM des Systems eigene Speicherchips. Die Größe des installierten Videospeichers beeinflusst die Anzahl der Farben, die ein Programm anzeigen kann (mit den entsprechenden Videotreibern und den Fähigkeiten des Monitors).

Videotreiber

Ein Programm, mit dem Grafikmodus-Anwendungsprogramme und Betriebssysteme mit einer bestimmten Auflösung und der gewünschten Anzahl Farben dargestellt werden können. Ein Softwarepaket kann "generische" Videotreiber enthalten. Zusätzliche Videotreiber müssen in der Regel auf den im System installierten Videoadapter zugeschnitten sein.

Virtueller Speicher

Ein Verfahren, um den adressierbaren RAM-Speicher mithilfe des Festplattenlaufwerks zu vergrößern. Beispiel: In einem System mit 16 MB RAM und 16 MB virtuellem Speicher auf der Festplatte würde das Betriebssystem das System so verwalten, als hätte es tatsächlich einen physikalischen RAM mit 32 MB.

Virus

Ein selbststartendes Programm, dessen Funktion darin besteht, Probleme zu bereiten. Virusprogramme sind dafür bekannt, dass sie die auf dem Festplattenlaufwerk abgespeicherten Dateien beschädigen oder sich selber so lange duplizieren, bis auf einem Computersystem oder Netzwerk kein Speicherbereich mehr zur Verfügung steht. Virusprogramme gelangen in der Regel durch infizierte Disketten von einem System zum anderen und kopieren sich dann selbstständig auf das Festplattenlaufwerk. Sie können vorbeugend folgende Schritte durchführen:

- Führen Sie in regelmäßigen Abständen ein Dienstprogramm aus, das das Festplattenlaufwerk auf Viren überprüft.
- Führen Sie für alle Disketten vor deren Anwendung (einschließlich der im Handel erworbenen Software) stets eine Virus-Überprüfung durch.

VMS

Akronym für Virtual Media Server.

VNC

Akronym für Virtual Network Computing. In einem VNC-System stellen Server Anwendungen, Daten und die Desktopumgebung bereit, auf die über das Internet zugegriffen werden kann.

VRAM

Akronym für Video Random-Access Memory (Video-RAM). Einige Videoadapter verwenden VRAM-Chips (oder eine Kombination von VRAM- und DRAM-Chips), um die Videoleistung zu steigern. VRAM-Speicher sind zweikanalig, so dass der Videoadapter gleichzeitig den Bildschirm aktualisieren und neue Anzeigedaten empfangen kann.

W

Abkürzung für Watt.

Wake Up On LAN

Die Fähigkeit, die Stromversorgung in einer Client-Station vom Netzwerk einschalten zu lassen. Die Remote-Aktivierungsfunktion ermöglicht die Ausführung von Software-Upgrades und anderen Verwaltungsaufgaben auf Rechnern von Benutzern nach Ende der Geschäftszeiten. Außerdem können Remote-Benutzer Zugang zu ausgeschalteten Maschinen erhalten. Intel nennt die Remote-Aktivierung "Wake-on-LAN".

Web-Server

Eine Anwendung, mit der Webseiten mithilfe von Web-Browsern unter Verwendung des HTTP-Protokolls angezeigt werden können.

Winbind

Ein Programm, das es Benutzern in einem heterogenen Netzwerk ermöglicht, sich über Arbeitsstationen anzumelden, die unter UNIX oder Windows laufen. Das Programm bewirkt, dass unter UNIX laufende Arbeitsstationen in Windows-Domänen funktionieren, indem jeder UNIX-Arbeitsstation Windows als UNIX präsentiert wird.

win.ini-Datei

Eine Startdatei für das Betriebssystem Windows. Beim Start von Windows konsultiert das Programm die **win.ini**-Datei, um verschiedene Optionen für die Windows-Betriebsumgebung festzulegen. Unter anderem wird in der **win.ini**-Datei festgehalten, welche Drucker und Schriftarten für Windows installiert wurden. Die **win.ini**-Datei enthält normalerweise auch Abschnitte, die optionale Einstellungen für auf dem Festplattenlaufwerk installierte Windows-Anwendungsprogramme enthält. Durch Ändern der Einstellungen in der Systemsteuerung oder durch Aufrufen des Windows-Setup-Programms können Optionen in der Datei **win.ini** geändert werden. In anderen Fällen müssen Optionen für die **win.ini**-Datei eventuell mit einem Texteditor (z. B. Notepad) manuell geändert oder hinzugefügt werden.

Windows NT

Leistungsstarke von Microsoft entwickelte Server- und Workstation-Betriebssystem-Software für technische, Entwicklungs- und Kalkulationsanwendungen.

WinRM

WinRM (Windows Remote Management) ist die Microsoft Implementierung des in das Betriebssystem integrierten WS-Management-Protokolls.

WMI

Akronym für Windows Management Instrumentation. WMI bietet CIM-Objektverwaltungsdienste.

X.509-Zertifikat

Ein X.509-Zertifikat bindet einen öffentlichen Verschlüsselungscode an die Identität oder ein anderes Attribut seines Eigners. Eigner können Menschen, Anwendungscode (z. B. ein signiertes Applet) oder jede andere eindeutig identifizierte Instanz sein (z. B. ein Secure Port-Server oder ein Web Server).

XMM

Abkürzung für Extended Memory Manager (Erweiterungsspeicherverwalter), ein Dienstprogramm zur Speicherverwaltung, das es Anwendungsprogrammen und Betriebssystemen ermöglicht, Erweiterungsspeicher gemäß XMS zu nutzen.

XMS

Abkürzung für Extended Memory Specification (Erweiterungsspeicher-Spezifikation).

X Window-System

Die grafische Benutzeroberfläche, die in Red Hat® Enterprise Linux® und SUSE® Linux Enterprise Server-Umgebungen verwendet wird.

Zeitüberschreitung

Eine bestimmte Dauer von Systeminaktivität, die eintreten muss, bevor die Stromsparfunktion aktiviert wird.

ZIF

Akronym für Zero Insertion Force (Einbau ohne Belastung). Einige Systeme besitzen ZIF-Sockel und Anschlüsse, mit denen Bauteile wie der Mikroprozessor ohne Belastung ein- und ausgebaut werden können.

Zugewiesenes physikalisches Speicher-Array

Das zugewiesene physikalische Speicher-Array bezieht sich auf die Art und Weise der Unterteilung des physikalischen Speichers.

Ein zugewiesener Bereich kann beispielsweise 640 KB und der andere zugewiesene Bereich zwischen 1 und 127 MB aufweisen.

Zustand

Der Zustand eines Objekts, das mehrere Zustände aufweisen kann. Beispiel: Ein Objekt kann sich im Zustand "nicht bereit" befinden.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Dell OpenManage auf VMware ESXi Software

Dell™ OpenManage™ Server Administrator Version 6.2- Installationshandbuch

VMware ESXi ist auf einigen Dell™-Systemen werkseitig installiert. Eine Liste dieser Systeme finden Sie in der neuesten *Dell Systems Software Support Matrix* auf der Support-Website von Dell unter **http://support.dell.com/support/edocs/software/omswrels/index.htm**. Sie können Server Administrator Web Server Version 6.2 verwenden, um auf VMware ESXi 3.5 Update 5 und VMware ESXi 4.0 Update 1-Systeme zuzugreifen.

Dell OpenManage auf VMware ESXi 3.5 Update 5

Sie können Server Administrator verwenden, um ein System mit VMware® ESXi-Virtualisierungssoftware zu verwalten. VMware ESXi und der Instrumentations-Agent sind auf bestimmten Dell™-Systemen werkseitig installiert. Eine Liste dieser Systeme finden Sie in der neuesten *Dell Systems Software Support Matrix* auf der Support-Website von Dell unter **http://support.dell.com/support/edocs/software/omswrels/index.htm**.

Sie können den Server Administrator Web Server auf einer Management Station installieren und auf ein verwaltetes System, auf dem VMware ESXi und der Instrumentations-Agent vorinstalliert sind, protokollieren, um Systemverwaltungsaufgaben durchzuführen.

Informationen über die VMware ESXi-Virtualisierungssoftware finden Sie auf der VMware Support-Website unter **www.vmware.com/support**.

Informationen zur Installation des Server Administrator Web Server auf einer Management Station finden Sie unter "Installieren von Managed System-Software auf Microsoft Windows-Betriebssystemen".

Dell OpenManage auf VMware ESXi 4.0 Update 1

Dell OpenManage Server Administrator ist als **.zip**-Datei (**oem-dell-openmanage-esxi_6.2-A00.zip**) verfügbar und kann auf Systemen installiert werden, die VMware ESXi 4.0 ausführen. Die Datei **oem-dell-openmanage-esxi_6.2-A00.zip** kann von der Dell Support-Website unter **support.dell.com** heruntergeladen werden.

Laden Sie die VMware vSphere-Befehlszeilenschnittstelle (vSphere CLI) von **http://www.vmware.com** herunter und installieren Sie sie auf Ihrem Microsoft Windows- oder Linux-System. Sie haben auch die Möglichkeit, VMware vSphere Management Assistant (vMA) in den ESXi 4-Host zu importieren.

vSphere-CLI verwenden

1. Kopieren Sie die Datei **oem-dell-openmanage-esxi_6.2-A00.zip** in ein Verzeichnis auf Ihrem System.
2. Wenn Sie Microsoft Windows verwenden, navigieren Sie zum Ordner, in dem die vSphere-CLI-Dienstprogramme installiert sind, um den in Schritt 4 erwähnten Befehl auszuführen. Bei Verwendung von Linux wird der Befehl dann installiert, wenn Sie den vSphere-CLI-RPM installieren.
3. Fahren Sie sämtliche Gast-Betriebssysteme auf dem ESXi 4.0-Host herunter und setzen Sie den ESXi 4.0-Host in den Wartungsmodus.
4. Führen Sie den folgenden Befehl aus:

   ```
   vihostupdate --server <IP-Adresse des ESXi 4-Hosts> -i -b <Pfad zur Dell OpenManage-Datei>
   ```

5. Geben Sie den Stammbenutzernamen und das Kennwort des ESXi 4.0- Hosts ein, wenn Sie dazu aufgefordert werden.

   Die Befehlsausgabe zeigt eine erfolgreiche oder eine fehlgeschlagene Aktualisierung an.

6. Starten Sie das ESXi 4.0-Hostsystem neu.

Verwenden von VMware vSphere Management Assistant

Der vSphere Management Assistant (vMA) ermöglicht Administratoren und Entwicklern, Skripts und Agenten zum Verwalten von ESX/ESXi-Systemen auszuführen. Weitere Informationen zum vMA finden Sie unter **http://www.vmware.com/support/developer/vima/**.

1. Melden Sie sich am vMA als Stammbenutzer an und geben Sie das Kennwort ein, wenn Sie dazu aufgefordert werden.
2. Kopieren Sie die Datei **oem-dell-openmanage-esxi_6.2-A00.zip** in ein Verzeichnis auf dem vMA.
3. Führen Sie im vMA den folgenden Befehl aus:

```
vihostupdate --server <IP-Adresse des ESXi 4-Hosts> -i -b <Pfad zur Dell OpenManage-Datei>
```

Wenn Sie den Befehl ausführen, werden die folgenden Komponenten auf dem System installiert:

- Server Administrator Instrumentation Service
- Remoteaktivierung
- Server Administrator Storage Management
- Remote Access Controller

Sie müssen den Server Administrator Web Server auf einer Management Station separat installieren. Informationen zum Installieren des Server Administrator Web Servers finden Sie unter "Installieren von Managed System-Software auf Microsoft Windows-Betriebssystemen."

ANMERKUNG: Stellen Sie sicher, dass Sie ausschließlich Server Administrator Web Server Version 6.1 oder höher installieren. Server Administrator Web Server Version 6.0.3 wird auf VMware ESXi 4.0 nicht unterstützt.

Nach der Installation von Server Administrator ist es erforderlich, die Server Administrator-Dienste zu aktivieren. Informationen zum Aktivieren dieser Dienste finden Sie unter "Aktivieren der Server Administrator-Dienste auf dem Managed System".

Fehlerbehebung

Beim Versuch, den Befehl vihostupdate zu verwenden, wird möglicherweise der folgende Fehler angezeigt:

c:\oem-dell-openmanage-esxi_6.2-A00.zip wird entpackt

metadata.zip.sig ist nicht vorhanden

Signatur-Übereinstimmungsfehler: metadata.zip

Das Update Package kann nicht entpackt werden.

Dieser Fehler wird angezeigt, wenn Sie eine frühere Version der Remote-CLI verwenden. Laden Sie die vSphere-Version der CLI herunter und installieren Sie sie.

Aktivieren der Server Administrator-Dienste auf dem Managed System

Der Server Administrator Web Server kommuniziert mit den VMware ESXi 3.5 System über den Server Administrator-CIM-Provider (Common Interface Model). Der Server Administrator CIM-Provider ist ein OEM-Provider auf dem VMware ESXi 3.5 System. CIM-OEM-Provider sind auf VMware ESXi 3.5 standardmäßig deaktiviert. Sie müssen die CIM-OEM-Provider auf dem VMware ESXi 3.5/ESXi 4.0-System aktivieren, bevor Sie unter Verwendung des Server Administrator Web Servers darauf zugreifen können.

Aktivieren der CIM-OEM-Provider mit VMware Infrastructure Client (für VMware ESXi 3.5)

Um die CIM-OEM-Provider mit dem VMware Infrastructure (VI) Client zu aktivieren, müssen Sie das VI-Client-Hilfsprogramm installieren. Sie können unter **http://<IP-Adresse>** auf das Hilfsprogramm zugreifen, wobei *<IP-Adresse>* die IP-Adresse des VMware ESXi-Systems ist.

So aktivieren Sie die CIM-OEM-Provider auf dem VMware ESXi-System unter Verwendung von VI-Client:

1. Melden Sie sich am VMware ESXi-System mit dem VI-Client an.
2. Wählen Sie das Register **Konfiguration** aus.
3. Klicken Sie auf der linken Seite im Abschnitt **Software** auf **Erweiterte Einstellungen**.
4. Klicken Sie im Dialogfeld **Erweiterte Einstellungen** auf der linken Seite auf **Verschiedenes**.
5. Ändern Sie den Wert des Feldes **OEM-Provider aktivieren** auf **1**.
6. Klicken Sie auf **OK**.
7. Um die Änderung ohne einen Neustart in Kraft zu setzen, verwenden Sie die Funktion **Verwaltungsagenten neustarten** der Direct Console User Interface (DCUI) auf der lokalen Konsole des VMware ESXi-Systems.
8. Starten Sie das System neu, um die Änderung in Kraft zu setzen. Das System kann im VI-Client auf dem Register **Zusammenfassung** neu gestartet werden.

Aktivieren der CIM-OEM-Provider mit VMware Infrastructure Remote CLI (für VMware ESXi 3.5)

Um die CIM-OEM-Provider mit der VI Remote CLI zu aktivieren, müssen Sie das VI Remote CLI-Hilfsprogramm installieren. Sie können das Hilfsprogramm von der VMware-Website unter **http://www.vmware.com/go/remotecli/** herunterladen und installieren.

So aktivieren Sie die CIM-OEM-Provider mit der VI Remote CLI unter Windows:

1. Öffnen Sie eine Befehlszeile.
2. Navigieren Sie zum Verzeichnis, in dem die Remote-CLIs installiert sind. Der Standard-Speicherort ist **C:\Program Files\VMware\VMware VI Remote CLI\bin**.
3. Führen Sie den folgenden Befehl aus:

   ```
   vicfg-advcfg --server <ip_address> --username <user_name> --password <password> --set 1 Misc.CimOemProvidersEnabled
   ```

   ANMERKUNG: Wenn Sie keinen Benutzernamen und kein Kennwort angeben, werden Sie dazu aufgefordert.

4. Um die Änderung ohne einen Neustart zu aktivieren, verwenden Sie die Funktion **Verwaltungsagenten neustarten** der Direct Console User Interface (DCUI) auf der lokalen Konsole des VMware ESXi-Systems.
5. Starten Sie das VMware ESXi-System neu, um die Änderung in Kraft zu setzen.

Weitere Informationen über die Verwendung von VI-Client und VI Remote CLI finden Sie auf der VMware Support-Website unter **www.vmware.com/support**.

vSphere Client zum Aktivieren der CIM OEM-Provider verwenden (für VMware ESXi 4.0)

Um die CIM-OEM-Provider mit dem VMware vSphere Client zu aktivieren, muss das vSphere Client-Hilfsprogramm installiert sein. Sie können das Hilfsprogramm von **https://<IP-Adresse des ESXi 4-Hosts>** herunterladen und installieren, wobei *<IP-Adresse>* die IP-Adresse des VMware ESXi 4-Systems ist.

So aktivieren Sie CIM-OEM-Provider auf dem VMware ESXi 4-System unter Verwendung von vSphere Client:

1. Melden Sie sich unter Verwendung des vSphere Client am VMware ESXi 4-Hostsystem an.
2. Klicken Sie auf das Register **Konfiguration**.
3. Klicken Sie auf der linken Seite im Abschnitt **Software** auf **Erweiterte Einstellungen**.
4. Klicken Sie im Dialogfeld **Erweiterte Einstellungen** auf der linken Seite auf **UserVars**.
5. Ändern Sie den Wert des Feldes **CIMOEMProvidersEnabled** zu **1**.
6. Klicken Sie auf **OK**.
7. Starten Sie das VMware ESXi 4-Hostsystem neu, um die Änderung in Kraft zu setzen. Starten Sie das System unter Verwendung des Registers **Zusammenfassung** im vSphere Client neu.

Konfigurieren des SNMP-Agenten auf VMware ESXi 4-Systemen

Server Administrator erzeugt SNMP-Traps als Reaktion auf Statusänderungen der Sensoren und anderer überwachter Parameter. Sie müssen ein oder mehrere Trap-Ziele auf dem Server Administrator ausführenden System konfigurieren, um SNMP-Traps an eine Verwaltungsstation zu senden.

Server Administrator unterstützt SNMP-Traps auf VMware ESXi 4, jedoch keine SNMP-Get- und Set-Funktionen, da VMware ESXi 4 die benötigte SNMP-Unterstützung nicht bietet. Sie können die VMware vSphere CLI verwenden, um ein VMware ESXi 4 ausführendes System zu konfigurieren und SNMP-Traps an eine Verwaltungsanwendung wie IT Assistant zu senden.

ANMERKUNG: Weitere Informationen zur Verwendung der VMware vSphere CLI finden Sie auf der VMware Support-Website unter **www.vmware.com/support**.

Konfigurieren des Systems zum Senden von Traps an eine Management Station mittels vSphere CLI

1. Installieren Sie VMware vSphere CLI.
2. Öffnen Sie eine Eingabeaufforderung in dem System, in dem die vSphere CLI installiert ist.
3. Navigieren Sie zu dem Verzeichnis, in dem die vSphere CLI installiert ist. Der Standardpfad unter Linux ist **/usr/bin**, der Standardpfad unter Windows ist **C:\Program Files\VMware\VMware vSphere CLI\bin**.
4. Führen Sie den folgenden Befehl aus:

```
vicfg-snmp.pl --server <server> --username <username> --password <password> -c <community> -t <hostname>/<community>
```

Dabei ist <*server*> der Hostname oder die IP-Adresse des ESXi-Systems, <*username*> der Benutzer im ESXi-System, <*password*> das Passwort des ESXi-Benutzers, <*community*> der SNMP Community-Name und <*hostname*> der Hostname oder die IP-Adresse der Verwaltungsstation.

ANMERKUNG: Die Dateierweiterung **.pl** wird unter Linux nicht benötigt.

ANMERKUNG: Wenn Sie den Benutzernamen und das Kennwort nicht angeben, werden Sie dazu aufgefordert.

Die SNMP-Trap-Konfiguration wird sofort ohne den Neustart von Diensten wirksam.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Installieren von Managed System Software auf unterstützten Linux-Betriebssystemen

Dell™ OpenManage™ Server Administrator Version 6.2- Installationshandbuch

---

Übersicht

Das Installationsprogramm von Dell™ OpenManage™ stellt für das Betriebssystem spezifische Installationsscripts und RPM-Pakete bereit, um Dell OpenManage Server Administrator und andere Managed System Softwarekomponenten zu installieren oder zu deinstallieren. Diese Installationsscripts und RPMs befinden sich im Verzeichnis **SYSMGMT/srvadmin/linux/RPMS/<*operating_system*>**.

Das benutzerdefinierte Installationsscript **srvadmin-install.sh** ermöglicht eine benutzerdefinierte und interaktive Installation. Wenn Sie das Script **srvadmin-install.sh** in Ihre Linux-Scripts integrieren, können Sie Server Administrator auf einem einzelnen System oder auf mehreren Systemen lokal oder über ein Netzwerk installieren.

Die zweite Installationsmethode verwendet die RPM-Pakete von Server Administrator, die in den benutzerdefinierten Verzeichnissen und dem Linux-Befehl **rpm** enthalten sind. Sie können Linux-Scripts schreiben, die Server Administrator auf einem einzelnen System oder auf mehreren Systemen lokal oder über ein Netzwerk installieren.

Die beiden Installationsmethoden zu kombinieren, wird nicht empfohlen und erfordert möglicherweise die manuelle Installation der in den benutzerdefinierten Verzeichnissen enthaltenen RPM-Pakete von Server Administrator über den Linux-Befehl **rpm**.

Informationen über unterstützte Plattformen und unterstützte Betriebssysteme finden Sie in der *Dell Systems Software Support Matrix* auf der Support-Website von Dell unter **http://support.dell.com/support/edocs/software/omswrels/index.htm**.

Softwarelizenzvereinbarung

Die Softwarelizenz für die Red Hat Enterprise Linux- und SUSE Linux Enterprise Server-Version der Dell OpenManage-Software befindet sich auf der DVD *Dell Systems Management Tools and Documentation*. Lesen Sie bitte die Datei **license.txt** . Durch Installieren oder Kopieren von einer der Dateien auf dem von Dell bereitgestellten Datenträger stimmen Sie den Bedingungen in dieser Datei zu. Diese Datei wird auch zum Stamm der Softwarestruktur kopiert, wo Sie die Installation der Dell OpenManage-Software auswählen.

Server Administrator-Gerätetreiber

Server Administrator enthält zwei Gerätetreiber für Linux: Den Systems Management-Basistreiber (dcdbas) und den BIOS-Aktualisierungstreiber (dell_rbu). Server Administrator verwendet diese Treiber, um die Systemverwaltungsfunktionen auf den unterstützten Linux-Betriebssystemen auszuführen. Abhängig vom System lädt Server Administrator einen oder beide Treiber.

Die Gerätetreiber für Linux wurden als Open-Source-Treiber unter der GNU General Public License v2.0 freigegeben. Sie sind ab Kernel 2.6.14 unter Linux-Kernel auf **kernel.org** erhältlich.

Wenn die Server Administrator-Treiber im Betriebssystem enthalten sind, verwendet Server Administrator diese Versionen der Treiber. Wenn die Server Administrator-Treiber nicht im Betriebssystem enthalten sind, verwendet Server Administrator zur Erstellung der Treiber bei Bedarf die Dynamische Kernel-Unterstützung (DKS). Weitere Informationen zu DKS finden Sie im Abschnitt "Dynamische Kernel-Unterstützung".

Die Server Administrator-Treiber sind mit allen unterstützten Betriebssystemversionen von Linux außer VMware ESX 3.5 verfügbar. Server Administrator erstellt die Treiber für VMware ESX 3.5 mit Hilfe der DKS-Funktion.

Dynamische Kernel-Unterstützung

Server Administrator enthält DKS, eine Funktion, die ggf. automatisch einen Gerätetreiber für einen ausgeführten Kernel durch Server Administrator aufbaut.

Wenn Sie während der Installation der Server Administrator-Gerätetreiber die folgende Meldung sehen, hat Server Administrator versucht, die DKS-Funktion zu verwenden, jedoch ohne Erfolg, da bestimmte Voraussetzungen nicht erfüllt waren:

```
Erstellen von <Treiber> mit DKS... [FEHLERHAFT]

wobei <Treiber> dcdbas oder dell_rbu ist
```

ANMERKUNG: Server Administrator protokolliert Nachrichten in der Protokolldatei **/var/log/messages**.

Um DKS zu verwenden, identifizieren Sie, welcher Kernel auf dem verwalteten System ausgeführt wird, und überprüfen Sie die DKS-Voraussetzungen.

Ermittlung des ausgeführten Kernel

1. Melden Sie sich als root beim System an.
2. Geben Sie an einer Konsole den folgenden Befehl ein und drücken Sie <Eingabe>:

   ```
   uname -r
   ```

Das System zeigt eine Meldung an, die den ausgeführten Kernel identifiziert.

Dynamische Kernel-Unterstützung - Voraussetzungen

Die folgenden Abhängigkeiten müssen vor dem Neustart der Managed System Software eingehalten werden, bevor Server Administrator DKS verwenden kann.

- Für den ausgeführten Kernel muss die ladbare Modulunterstützung aktiviert sein.
- Die Quelle zur Erstellung von Kernel-Modulen für den zurzeit ausgeführten Kernel muss unter **/lib/modules/`uname –r`/build** verfügbar sein. Auf Systemen, die SUSE Linux Enterprise Server ausführen, liefert der **Kernel-Quelle**-RPM die notwendige Kernel-Quelle. Auf Systemen, die Red Hat Enterprise Linux ausführen, stellen die **kernel-devel**-RPMs die notwendige Kernel-Quelle zur Erstellung von Kernel-Modulen bereit.
- Das Dienstprogramm GNU make muss installiert sein. Das **make** RPM stellt dieses Dienstprogramm zur Verfügung.
- Der GNU C-Compiler (gcc) muss installiert sein. Das **gcc** RPM enthält diesen Compiler.
- Der GNU Linker (ld) muss installiert sein. Das **binutils** RPM enthält diesen Linker.

Bei Erfüllung dieser Voraussetzungen wird DKS automatisch einen Gerätetreiber erstellen, wenn dieser während des Starts von Server Administrator benötigt wird.

Verwenden der dynamischen Kernel-Unterstützung nach der Installation von Server Administrator

Um Server Administrator zu aktivieren, einen Kernel zu unterstützen, der nicht von einem vorkompilierten Gerätetreiber unterstützt und geladen wird, nachdem Server Administrator installiert wurde, führen Sie folgende Schritte aus: Stellen Sie sicher, dass die DKS-Voraussetzungen auf dem zu verwaltenden System erfüllt werden und starten Sie den neuen Kernel auf dem System.

Server Administrator erstellt einen Gerätetreiber für den auf dem System ausgeführten Kernel beim ersten Start nach dem Laden des Kernel. In der Standardeinstellung startet der Server Administrator während des Systemstarts.

Kopieren dynamisch erstellter Gerätetreiber in Systeme, auf denen der gleiche Kernel ausgeführt wird

Wenn Server Administrator einen Gerätetreiber für den ausgeführten Kernel dynamisch erstellt, installiert er den Gerätetreiber in das Verzeichnis **/lib/modules/<*kernel*>/kernel/drivers/firmware**, wobei **<*kernel*>** der Kernel-Name ist (ausgegeben durch Eingabe von `uname -r`). Wenn ein System den gleichen Kernel ausführt, für den ein Gerätetreiber erstellt wurde, können Sie den neu erstellten Gerätetreiber in das Verzeichnis **/var/omsa/dks/<*kernel*>** auf dem anderen System zur Verwendung durch Server Administrator kopieren. Diese Maßnahme ermöglicht Server Administrator, DKS auf mehreren Systemen zu verwenden, ohne die Kernel-Quelle auf jedem System installieren zu müssen.

Ein Beispiel ist das folgende Szenario: System A führt einen Kernel aus, der von keinem der vorher kompilierten Gerätetreiber des Server Administrator unterstützt wird. Auf System B wird der gleiche Kernel ausgeführt. Führen Sie folgende Schritte durch, um einen Gerätetreiber auf System A zu erstellen und diesen dann zur Verwendung durch Server Administrator auf System B zu kopieren:

1. Stellen Sie sicher, dass die DKS-Voraussetzungen auf System A erfüllt sind.
2. Server Administrator auf System A starten.

   Bei der Installation erstellt der Server Administrator einen Gerätetreiber für den auf System A ausgeführten Kernel.
3. Geben Sie `uname -r` auf System A ein, um den Namen des ausgeführten Kernel zu ermitteln.
4. Kopieren Sie beliebige '**dcdbas.***'- oder **dell_rbu.***-Dateien im Verzeichnis **/lib/modules/<*kernel*>/kernel/drivers/firmware** auf System A in das Verzeichnis **/var/omsa/dks/<*kernel*>** auf System B, wobei **<*kernel*>** der Kernel-Name ist, der bei Eingabe von `uname -r` in Schritt 3 ausgegeben wird.

   ANMERKUNG: Im Verzeichnis **/lib/modules/<*kernel*>/kernel/drivers/firmware** können eine oder mehrere der folgenden Dateien enthalten sein: **dcdbas.*** oder **dell_rbu.***.

   ANMERKUNG: Möglicherweise muss das Verzeichnis **/var/omsa/dks/<*kernel*>** auf System B erstellt werden. Wenn der Kernel-Name z. B 1.2.3-4smp lautet, kann das Verzeichnis durch Eingabe von `mkdir -p /var/omsa/dks/1.2.3-4smp` erstellt werden.
5. Starten Sie Server Administrator auf System B.

Server Administrator stellt fest, dass der Gerätetreiber, den Sie in das Verzeichnis **/var/omsa/dks/<*kernel*>** kopiert haben, den ausgeführten Kernel unterstützt und diesen Gerätetreiber verwendet.

ANMERKUNG: Wenn Server Administrator auf System B deinstalliert wurde, werden die Dateien **/var/omsa/dks/<*kernel*>/*.** , die Sie nach System B kopiert haben, nicht entfernt. Die Dateien müssen gelöscht werden, wenn sie nicht länger benötigt werden.

OpenIPMI-Gerätetreiber

Für die Server Instrumentation-Funktion von Server Administrator ist der OpenIPMI-Gerätetreiber erforderlich, der IPMI-basierte Informationen und Funktionen zur Verfügung stellt.

Alle unterstützten Linux-Systeme enthalten die erforderliche Version des IPMI-Moduls im Standardeinstellungskernel selbst. Sie brauchen nicht den IPMI RPM zu installieren. Weitere Informationen zu den unterstützten Systemen finden Sie in der *Dell Systems Software Support Matrix* auf der Support-Website von Dell unter **http://support.dell.com/support/edocs/software/omswrels/index.htm**.

Verschlechterung der Funktionalität, nachdem der Server Administrator Instrumentation Service gestartet wird

Nachdem Server Administrator installiert wurde, führt der Server Administrator Instrumentation Service bei jedem Start eine Laufzeitprüfung des OpenIPMI-Gerätetreibers durch. Der Server Administrator Instrumentation Service wird immer mit dem Befehl **srvadmin-services.sh start** oder **srvadmin-services.sh restart** gestartet, oder Sie starten das System erneut (wodurch der Server Administrator Instrumentation Service gestartet wird).

Die Installation von Server Administrator blockiert die Installation von Server Administrator-Paketen, wenn derzeit keine ausreichende Version des OpenIPMI-Gerätetreibers auf dem System installiert ist. Jedoch ist es noch möglich, obwohl nicht typisch, dass Sie eine ausreichende Version des OpenIPMI-Gerätetreibers deinstallieren oder ersetzen können, nachdem Server Administrator installiert wurde. Server Administrator kann dies nicht verhindern.

Um eine vom Benutzer deinstallierte oder ersetzte ausreichende Version des OpenIPMI-Gerätetreibers nach der Installation von Server Administrator zu erkennen, überprüft der Server Administrator Instrumentation Service beim Start die OpenIPMI-Gerätetreiberversion. Wenn keine ausreichende Version des OpenIPMI-Gerätetreibers gefunden wird, stuft sich der Server Administrator Instrumentation Service herunter, so dass nicht auf IPMI-basierte Informationen oder Funktionen zugegriffen werden kann. In erster Linie bedeutet dies, dass keine Sondendaten (z. B. Lüfter, Temperaturen und Spannungssondendaten) übermittelt werden.

Installation von Managed System Software

In diesem Abschnitt wird erklärt, wie die Managed System Software mithilfe der folgenden Installationsoptionen installiert wird.

- Verwendung des Shell-Scripts **srvadmin-install.sh** für Schnellinstallationen oder benutzerdefinierte Installationen im interaktiven Modus

  ANMERKUNG: Wenn Sie das Managed System Software-Installationsprogramm von der Dell Support Site unter **support.dell.com** heruntergeladen haben (verfügbar als **.tar.gz**-Datei), befindet sich das Shell-Script **srvadmin-install.sh** als **setup.sh** im Stammverzeichnis.

- Verwendung von RPM-Befehlen für benutzerdefinierte Installationen im interaktiven Modus

Für Informationen über die verschiedenen in Dell OpenManage Version 6.2 verfügbaren Komponenten von Server Administrator und Informationen zur Unterstützung bei der Auswahl der für die Installation erforderlichen Komponenten siehe "Bereitstellungsszenarien für Server Administrator".

Voraussetzungen für die Installation der Managed System Software

- Sie müssen mit root angemeldet sein.
- Für den ausgeführten Kernel muss die ladbare Modulunterstützung aktiviert sein.
- Das Verzeichnis **/opt** muss mindestens 250 MB freien Speicherplatz und die Verzeichnisse **/tmp**, **/etc** und **/var** müssen je mindestens 20 MB freien Speicherplatz aufweisen.
- Das Paket **ucd-snmp** oder **net-snmp**, das mit dem Betriebssystem zur Verfügung gestellt wird, muss installiert werden, wenn Sie SNMP zur Serververwaltung verwenden. Wenn Sie unterstützende Agenten für den Agenten **ucd-snmp** oder **net-snmp** verwenden möchten, müssen Sie die Betriebssystemunterstützung für den SNMP-Standard installieren, bevor Server Administrator installiert wird. Weitere Informationen über die Installation von SNMP entnehmen Sie den Installationsanweisungen für das auf Ihrem System ausgeführte Betriebssystem.

  ANMERKUNG: Wenn Sie ein RPM-Paket unter VMware ESX, Red Hat Enterprise Linux oder SUSE Linux Enterprise Server installieren, importieren Sie zur Vermeidung von Warnungen in Bezug auf den RPM-GPG-Schlüssel, den Schlüssel mit dem folgenden oder einem ähnlichen Befehl:

  ```
  rpm --import /mnt/dvdrom/SYSMGMT/srvadmin/
  linux/RPM-GPG-KEY
  ```

- Sie müssen alle RPMs installieren, die für eine erfolgreiche Installation erforderlich sind.

  Falls VMware ESX (Version 3.5 oder 4), Red Hat Enterprise Linux (Version 4 und 5) oder SUSE Linux Enterprise Server (Version 10 und 11) auf Ihrem System werkseitig installiert wurde, finden Sie weitere Informationen zu den RPMs, die Sie vor Installation der Managed System Software manuell installieren müssen, im Abschnitt "Abhängige RPMs für die Remote-Aktivierung" . In den meisten Fällen ist eine manuelle Installation der RPMs nicht erforderlich.

  Wenn auf Ihrem System kein werkseitig installiertes Linux-Betriebssystem installiert war und Sie kein VMware ESX- (Version 3.5 oder 4), Red Hat Enterprise Linux- (Version 4 und 5) oder SUSE Linux Enterprise Server-Betriebssystem (Version 9 und 10) mit Dell Systems Build and Update Utility installiert haben, müssen Sie die erforderlichen RPMs vor der Installation der Managed System Software manuell installieren. Diese Dateien sind auf der

DVD Dell Systems Management Tools and Documentation verfügbar. Wechseln Sie zu **SYSMGMT/srvadmin/linux/RPMS/supportRPMS/**, um die erforderlichen RPM-Dateien für Ihr Linux-Betriebssystem ausfindig zu machen. Installieren Sie mit `rpm -ivh <name_of_RPM>` geeignete RPMs, bevor Sie die Managed System Software installieren.

Installieren der Managed System Software mit von Dell bereitgestellten Datenträgern

Das Installationsprogramm von Dell OpenManage verwendet RPMs, um einzelnen Komponenten zu installieren. Der Datenträger (DVD) ist für eine einfache benutzerdefinierte Installation in Unterverzeichnisse aufgeteilt.

ANMERKUNG: Auf dem Betriebssystem Red Hat Enterprise Linux 5 werden DVDs automatisch mit der Ladeoption **-noexec** geladen. Diese Option bewirkt, dass Sie ausführbare Dateien nicht von der DVD ausführen können. Sie müssen die DVD manuell laden und dann die ausführbaren Dateien ausführen.

Wenn Sie die Software vor der Installation prüfen möchten, folgen Sie diesem Verfahren:

1. Legen Sie die DVD *Dell Systems Management Tools and Documentation* in das DVD-Laufwerk des Systems ein.
2. Laden Sie die DVD ggf. mit Hilfe des folgenden oder eines ähnlichen Befehls:
   `mount /dev/dvdrom /mnt/dvdrom`
3. Nachdem Sie die DVD geladen haben, navigieren Sie zu:
   `cd /mnt/dvdrom/SYSMGMT/srvadmin/linux/`
4. Rufen Sie eine Auflistung der Verzeichnisse ab, die den Befehl `ls` verwenden.

   Folgende Verzeichnisse auf dem Datenträger gehören zu VMware ESX, Red Hat Enterprise Linux und SUSE Linux Enterprise Server:

   - **SYSMGMT/srvadmin/linux/custom**
   - **SYSMGMT/srvadmin/linux/RPMS**
   - **SYSMGMT/srvadmin/linux/supportscripts**

Schnellinstallation

Verwenden Sie für Schnellinstallationen das enthaltene Shell-Script.

ANMERKUNG: Auf dem Red Hat Enterprise Linux 5-Betriebssystem werden DVDs automatisch mit der Ladeoption **-no**exec geladen. Diese Option bewirkt, dass Sie ausführbare Dateien nicht von der DVD ausführen können. Sie müssen die DVD manuell laden und dann die ausführbaren Dateien ausführen.

1. Melden Sie sich mit `root` beim System an, auf dem das unterstützte Red Hat Enterprise Linux- oder SUSE Linux Enterprise Server-Betriebssystem ausgeführt wird und wo die Managed System-Komponenten installiert werden sollen.
2. Legen Sie die DVD *Dell Systems Management Tools and Documentation* in das DVD-Laufwerk ein.
3. Laden Sie die DVD ggf. mit Hilfe des folgenden oder eines ähnlichen Befehls:
   `mount /dev/dvdrom /mnt/dvdrom`
4. Wechseln Sie zum Verzeichnis **SYSMGMT/srvadmin/linux/supportscripts**.
5. Führen Sie das Shell-Script **srvadmin-install.sh** wie unten gezeigt aus. Dieses führt eine Schnellinstallation aus. Das Setup-Programm installiert die folgenden Managed System Software-Funktionen:

   - Server Administrator Web Server
   - Server Instrumentation
   - Storage Management
   - Remote Access Controller

   ```
   sh srvadmin-install.sh --express
   ```

   oder

   ```
   sh srvadmin-install.sh -x
   ```

   Die Server Administrator-Dienste starten nicht automatisch.
6. Starten Sie nach der Installation die Server Administrator-Dienste mithilfe des Scripts **srvadmin-services.sh** durch Verwendung des Befehls **sh srvadmin-services start**.

Benutzerdefinierte Installation

Managed System Software bietet zwei benutzerdefinierte Installationspfade. Der eine ist RPM-basiert und enthält vorkonfigurierte benutzerdefinierte Verzeichnisse, der andere basiert auf Shell-Script.

Benutzerdefinierte Installation unter Verwendung von vorkonfigurierten benutzerdefinierten Verzeichnissen

Alle für ein bestimmtes Betriebssystem spezifischen RPMs sind unterTabelle 7-1 in Gruppen zusammen gefasst aufgeführt. Sie können diese RPMs zur Durchführung einer benutzerdefinierten Installation mit Hilfe von vorkonfigurierten benutzerdefinierten Verzeichnissen verwenden.

Tabelle 7-1. Benutzerdefinierte Installation mithilfe von vorkonfigurierten Verzeichnissen

Verzeichnis	Einzelheiten
Um eine RPM-basierte benutzerdefinierte Installation zu ermöglichen, fügen Sie die RPMs von den folgenden Verzeichnissen hinzu:	
SYSMGMT/srvadmin/linux/custom/ESX35	Enthält Server Administrator mit Befehlszeilenschnittstelle für VMware ESX (Version 3.5)
SYSMGMT/srvadmin/linux/custom/ESX40	Enthält Server Administrator mit Befehlszeilenschnittstelle für VMware ESX (Version 4)
SYSMGMT/srvadmin/linux/custom/RHEL4	Enthält Server Administrator mit der Befehlszeilenschnittstelle für Red Hat Enterprise Linux (Version 4)
SYSMGMT/srvadmin/linux/custom/RHEL5	Enthält Server Administrator mit der Befehlszeilenschnittstelle für Red Hat Enterprise Linux (Version 5)
SYSMGMT/srvadmin/linux/custom/SLES10	Enthält Server Administrator mit der Befehlszeilenschnittstelle für den SUSE Linux Enterprise Server (Version 10)
SYSMGMT/srvadmin/linux/custom/SLES11	Enthält Server Administrator mit der Befehlszeilenschnittstelle für den SUSE Linux Enterprise Server (Version 11)
Wenn Sie zum Beispiel Red Hat Enterprise Linux (Version 4) ausführen, können Sie die Installation individuell einrichten, indem Sie die RPMs von den folgenden Verzeichnissen hinzufügen:	
SYSMGMT/srvadmin/linux/custom/RHEL4/add-StorageManagement	Storage Management-Komponentenpakete für Red Hat Enterprise Linux (Version 4)
SYSMGMT/srvadmin/linux/custom/RHEL4/SA-WebServer	Server Administrator Web Server-Komponentenpakete für Red Hat Enterprise Linux (Version 4)
SYSMGMT/srvadmin/linux/custom/RHEL4/Server-Instrumentation	Server Instrumentation-Pakete für Red Hat Enterprise Linux (Version 4)

Es folgt ein Beispiel für eine RPM-basierte benutzerdefinierte Installation von Server Administrator, einschließlich der Installation der Remote-Aktivierungsfunktion und der Storage Management Service-Komponenten.

ANMERKUNG: Auf dem Betriebssystem Red Hat Enterprise Linux 5 werden DVDs automatisch mit der Ladeoption **-no**exec geladen. Diese Option bewirkt, dass Sie ausführbare Dateien nicht von der DVD ausführen können. Sie müssen die DVD manuell laden und dann die ausführbaren Dateien ausführen.

1. Melden Sie sich mit root beim System an, auf dem das unterstützte VMware ESX-, Red Hat Enterprise Linux- oder SUSE Linux Enterprise Server-Betriebssystem ausgeführt wird und die Managed System- Komponenten installiert werden sollen.

2. Legen Sie die DVD *Dell Systems Management Tools and Documentation* in das DVD-Laufwerk ein.

3. Laden Sie ggf. die DVD mit einem Befehl wie z. B.:
   ```
   mount /dev/dvdrom /mnt/dvdrom
   ```

4. Navigieren Sie zu **SYSMGMT/srvadmin/linux/custom/<*BS*>**, wobei <*BS* entweder **ESX35** oder **ESX40** oder **RHEL4** oder **RHEL5** oder **SLES10** oder **SLES11** ist. Geben Sie das spezifische Verzeichnis des Betriebssystems ein, das Ihrem System entspricht.

5. Geben Sie den folgenden Befehl ein:

   ```
   rpm -ihv Server-Instrumentation/*.rpm
   add-StorageManagement/*.rpm add-RemoteEnablement/*.rpm
   ```

   Die Server Administrator-Dienste starten nicht automatisch.

   ANMERKUNG: Stellen Sie sicher, dass Sie Server Administrator Web Server, Remote-Aktivierung oder Server-Instrumentation installieren, bevor Sie Remote Access Controller oder Storage Management installieren.

ANMERKUNG: Wenn Sie die Remote-Aktivierung installieren möchten, stellen Sie sicher, dass Sie zuvor die abhängigen RPMs installieren. Weitere Informationen zum Installieren der abhängigen RPMs finden Sie unter "Abhängige RPMs für die Remote-Aktivierung".

6. Starten Sie die Server Administrator-Dienste nach der Installation mit dem Befehl:

   ```
   sh srvadmin-services start
   ```

   ANMERKUNG: Sie können Server Administrator auf jedem System installieren, das die Betriebssystem-Abhängigkeiten erfüllt. Auf nicht unterstützten Systemen werden jedoch ggf. einige Server Administrator-Dienste nicht gestartet.

ANMERKUNG: Wenn Dell OpenManage Server Administrator auf einem System installiert ist, können Abhängigkeitsprobleme auftreten, die mit RPMs in Verbindung stehen. Sie können diese Probleme beheben, indem Sie die fehlenden RPM-Dateien von **SYSMGMT/srvadmin/linux/RPMS/supportRPMS/opensource-components** installieren. Wenn die RPMs in diesem Verzeichnis nicht verfügbar sind, installieren Sie die RPMs vom Betriebssystemdatenträger. Wenn sie nicht auf dem Datenträger verfügbar sind, suchen Sie die RPMs im Internet.

Shell-Script zum Ausführen der benutzerdefinierten Installation verwenden

Sie können das benutzerdefinierte Installationsscript des Server Administrator im interaktiven Modus ausführen.

Die grundlegende Verwendung des Scripts ist:

```
srvadmin-install.sh [OPTION]...
```

Benutzerdefiniertes Installationsdienstprogramm von Server Administrator

Dieses Dienstprogramm wird im interaktiven Modus ausgeführt, wenn Sie keine Optionen angeben, und es wird im Hintergrundmodus ausgeführt, wenn Sie eine oder mehrere Optionen angeben.

Die Optionen sind:

[**-x|--express**] installiert alle Komponenten (einschließlich **RAC**, falls verfügbar); alle weiteren durchlaufenen Optionen werden ignoriert.

[**-d|--dellagent**] installiert **Server Instrumentation**-Komponenten.

[**-c|--cimagent**] installiert **Remote Enablement**-Komponenten.

[**-s|--storage**] installiert **Storage Management**, einschließlich **Server Instrumentation**.

[**-r|--rac**] installiert zutreffende **RAC**-Komponenten, einschließlich **Server Instrumentation**.

[**-w|--web**] installiert **Server Administrator Web Server**.

[**-u|--update**] erweitert zutreffende Server Administrator-Komponenten.

[-h|--help] zeigt diesen Hilfetext an.

Optionen, die neben den oben genannten Optionen verwendet werden können:

[**-p|--preserve**] bewahrt die Bildschirmanzeige, ohne zu löschen.

ANMERKUNG: Wenn Sie die Option **[-p | --preserve]** während der benutzerdefinierten Installation nicht verwenden, werden die Verlaufsinformationen auf dem Bildschirm gelöscht.

[-a|--autostart] startet die installierten Dienste, nachdem die Komponenten installiert wurden.

Shell-Script zur Ausführung einer unbeaufsichtigten benutzerdefinierten Installation im interaktiven Modus verwenden

Dieses Verfahren verwendet das Installations-Shell-Script, um Sie während der Installation nach der Installation von spezifischen Komponenten zu fragen.

1. Melden Sie sich mit root beim System an, auf dem das unterstützte Red Hat Enterprise Linux- oder SUSE Linux Enterprise Server-Betriebssystem ausgeführt wird und die Managed System-Komponenten installiert werden sollen.
2. Legen Sie die DVD *Dell Systems Management Tools and Documentation* in das DVD-Laufwerk ein.
3. Laden Sie die DVD ggf. mit dem folgenden Befehl:
   `mount /dev/dvdrom /mnt/dvdrom`
4. Navigieren Sie zu **SYSMGMT/srvadmin/linux/supportscripts**, falls Sie die DVD verwenden.
5. Führen Sie das Script mit dem Befehl sh `srvadmin-install.sh` aus und akzeptieren Sie die Bedingungen der Endnutzer- Lizenzvereinbarung.

   Durch das Ausführen des Befehls wird eine Liste von Komponentenoptionen angezeigt. Falls Komponenten bereits installiert wurden, werden sie separat aufgeführt und enthalten ein Häkchen neben ihrem Namen. Die Optionen zur benutzerdefinierten Installation von Server Administrator werden angezeigt.
6. Drücken Sie <c>, um zu kopieren, <i>, um zu installieren, <r> für Reset und Neustart oder <q> , um abzubrechen. Wenn Sie C drücken, werden Sie aufgefordert, den absoluten Zielpfad einzugeben.

   Wenn die Installation abgeschlossen ist, weist das Script eine Option zum Start der Dienste auf.
7. Drücken Sie <n>, um zu beenden. Sie können die Dienste später manuell starten.

Benutzerdefiniertes Installationsscript zur Ausführung im Hintergrundmodus

Es folgt ein Beispiel für eine benutzerdefinierte Installation im Hintergrundmodus unter Verwendung des Shell-Scripts **srvadmin-install.sh**:

1. Melden Sie sich mit root beim System an, auf dem das unterstützte Red Hat Enterprise Linux- oder SUSE Linux Enterprise Server-Betriebssystem ausgeführt wird und die Managed System-Komponenten installiert werden sollen.
2. Legen Sie die DVD *Dell Systems Management Tools and Documentation* in das DVD-Laufwerk ein.
3. Laden Sie die DVD ggf. mit Hilfe des folgenden oder eines ähnlichen Befehls: `mount /dev/dvdrom /mnt/dvdrom`.
4. Navigieren Sie zum Verzeichnis **SYSMGMT/srvadmin/linux/supportscripts**.

5. Zur Installation von Storage Management Service-Komponenten geben Sie den folgenden Befehl ein.

   `sh srvadmin-install.sh --storage` (dies sind lange Optionen)

   oder

   `sh srvadmin-install.sh -s` (dies sind kurze Optionen)

   ANMERKUNG: Lange Optionen können mit kurzen Optionen und umgekehrt kombiniert werden.

   Die Server Administrator-Dienste starten nicht automatisch.

6. Starten Sie die Server Administrator-Dienste nach der Installation mit dem Befehl:

   `sh srvadmin-services start`

ANMERKUNG: Melden Sie sich nach dem Installieren von Service Administrator ab und dann wieder an, um auf die Server Administrator Befehlszeilenschnittstelle (CLI) zuzugreifen.

Abhängige RPMs für die Remote-Aktivierung

Falls Sie die Remote-Aktivierungsfunktion installieren möchten, müssen Sie bestimmte abhängige RPMs installieren und diese konfigurieren, bevor Sie die Funktion installieren.

Die abhängigen RPMs sind auf der DVD *Dell Systems Management Tools and Documentation* unter **srvadmin\linux\RPMS\supportRPMS**\opensource-components verfügbar. Installieren Sie die folgenden RPMs:

- **libcmpiCppImpl0-2.0.0Dell-x.x.rhel5.i386.rpm**
- **libwsman1-2.1.5Dell-x.x.rhel5.i386.rpm**
- **openwsman-client-2.1.5Dell-x.x.rhel5.i386.rpm**
- **openwsman-server-2.1.5Dell-x.x.rhel5.i386.rpm**
- **sblim-sfcb-1.3.2Dell-x.x.rhel5.i386.rpm**
- **sblim-sfcc-2.1.5Dell-x.x.rhel5.i386.rpm**

Beispiel: Wenn Sie die abhängigen RPMs unter Red Hat Enterprise Linux 5.3 installieren, wählen Sie die folgenden Dateien unter **srvadmin\linux\RPMS\supportRPMS\opensource-components\RHEL5** aus:

- **libcmpiCppImpl0-2.0.0Dell-1.1.rhel5.i386.rpm**
- **libwsman1-2.1.5Dell-33.1.rhel5.i386.rpm**
- **openwsman-client-2.1.5Dell-33.1.rhel5.i386.rpm**
- **openwsman-server-2.1.5Dell-33.1.rhel5.i386.rpm**
- **sblim-sfcb-1.3.2Dell-13.1.rhel5.i386.rpm**
- **sblim-sfcc-2.1.5Dell-6.1.rhel5.i386.rpm**

Installation von abhängigen RPMs

1. Prüfen Sie, ob die abhängigen RPMs bereits installiert sind. Falls ja, entfernen Sie die installierten RPMs.

2. Stellen Sie sicher, dass Pegasus-RPMs deinstalliert sind.

3. Prüfen Sie, ob die Binärdateien `openwsmand` und `sfcbd` bereits mit make-install installiert sind. Sie können dies prüfen, indem Sie die folgenden Befehle ausführen:

   `openwsman`

   oder

   `sfcbd`

   oder

   Sie können das Vorhandensein der o. g. Binärdateien im Verzeichnis **/usr/local/sbin** prüfen.

4. Falls die Binärdateien installiert sind, deinstallieren Sie diese Binärdateien.

5. Prüfen Sie die erforderlichen Abhängigkeiten für die RPMs `openwsman` und `sfcbd`, die unter Tabelle 7-2 aufgeführt sind.

Tabelle 7-2. Erforderliche Abhängigkeiten

Pakete	Red Hat Enterprise Server	SUSE Linux Enterprise Server
OpenWSMAN	• OpenSSL • LibXML • Pkgconfig • CURL • Chkconfig • Initscript • SBLIM-SFCC	• LibOpenSSL • LibXML • Pkg-config • libCURL • aaa_base • aaa_base • SBLIM-SFCC
SBLIM SFCC	CURL	LibCURL
SBLIM SFCB	• zlib • CURL • PAM • OpenSSL • Chkconfig • Initscript	• zlib • LibCURL • PAM • LibOpenSSL • aaa_base • aaa_base

6. Installieren Sie die abhängigen RPMs.

   Sie können alle RPMs mit einem einzigen Befehl installieren.

   ```
   rpm -ivh rpm1 rpm2 rpm3 rpm4 ... rpmN
   ```

   Sie können die RPMs auch einzeln installieren.

   ANMERKUNG: Wenn Sie die RPMs einzeln installieren, verwenden Sie die folgende Sequenz.

   ```
   rpm -ivh sblim-sfcb-x.x.x.rpm
   ```

   ```
   rpm -ivh sblim-sfcc-x.x.x.rpm
   ```

ANMERKUNG: Installieren Sie die RPMs libwsman und openwsmanClient gleichzeitig, da diese zyklische Abhängigkeit aufweisen.

```
rpm -ivh libwsman1-x.x.x.rpm openwsman-client-x.x.x.rpm
```

```
rpm -ivh openwsman-server-x.x.x.rpm
```

Konfiguration der Post-Installation für die Remote-Aktivierung

Dieser Abschnitt erklärt die Schritte zur Konfiguration der abhängigen RPMs, wenn Sie die Remote-Aktivierung installiert haben.

Das Script zur Konfiguration nach der Installation ist unter **/opt/dell/srvadmin/etc/** auf der DVD *Dell Systems Management Tools and Documentation* verfügbar.

Führen Sie nach der Installation aller abhängigen RPMs und der Remote-Aktivierungsfunktion das Script **autoconf_cim_component.sh** aus.

Bevor Sie das Script **autoconf_cim_component.sh** ausführen, stellen Sie sicher, dass Dell OpenManage installiert ist. Informationen zum Installieren von Dell OpenManage finden Sie unter "Installation von Managed System Software".

Führen Sie den folgenden Befehl aus, um sfbc und openwsman gemäß den Standardkonfigurationen zu konfigurieren.

```
./ autoconf_cim_component.sh
```

Erstellen eines Serverzertifikats für WSMAN

Sie können entweder ein neues Zertifikat für WSMAN erstellen oder ein bestehendes Zertifikat wiederverwenden.

Erstellen eines neuen Zertifikats

Sie können das neue Serverzertifikat für WSMAN erstellen, indem Sie das Script **owsmangencert.sh** im Verzeichnis **/etc/openwsman** ausführen. Dieses Script wird durch den **openwsman**-RPM bereitgestellt. Befolgen Sie die Schritte im Assistenten, um das Serverzertifikat zu erstellen.

Wiederverwenden eines bestehenden Zertifikats

Falls Sie ein selbstsigniertes oder CA-signiertes Zertifikat haben, können Sie das gleiche Zertifikat für den openwsman-Server verwenden, indem Sie die unter [server] Tag in **/etc/openwsman/openwsman.conf** gruppierten Werte ssl_cert_file- und ssl_key_file mit Ihren bestehenden Zertifikatswerten

aktualisieren.

CRL für den openwsman-Client konfigurieren

Sie müssen die Zertifikatsperrliste (CRL) konfigurieren, die vom Server Administrator Web Server verwendet wird. Führen Sie dazu folgende Schritte durch:

1. Geben Sie unter **/etc/openwsman/openwsman_client.conf** eine gültige CRL-Datei an.
2. Wird das Feld freigelassen, wird die CRP-Überprüfung ignoriert.

ANMERKUNG: CRL-Unterstützung ist nur auf SUSE Linux Enterprise Server Version 11 vorhanden. Setzen Sie sich bzgl. anderer Betriebssysteme mit dem Betriebssystemanbieter in Verbindung, damit die erforderliche CURL-Bibliothek mit CRL-Unterstützung geliefert wird.

Ausführen von sfcb und openwsman

Führen Sie sfcb und openwsman aus:

- /etc/init.d/sfcb start
- /etc/init.d/openwsman start

Das verwaltete System ist konfiguriert und für die Nutzung durch Server Administrator Web Server bereit.

Winbind-Konfiguration für openwsman und sfcb für Red Hat Enterprise Linux-Betriebssysteme

1. Sichern Sie die folgenden Dateien:
   - **/etc/pam.d/openwsman**
   - **/etc/pam.d/sfcb**
   - **/etc/pam.d/system-auth**
2. Ersetzen Sie den Inhalt von **/etc/pam.d/openwsman** und **/etc/pam.d/sfcb** durch:

```
auth required pam_stack.so service=system-auth

auth required /lib/security/pam_nologin.so

account required pam_stack.so service=system-auth
```

3. Ersetzen Sie den Inhalt von **/etc/pam.d/system-auth** durch:

```
%PAM-1.0

Diese Datei wurde automatisch erzeugt.

Benutzeränderungen werden beim nächsten Ausführen von authconfig verworfen.

auth required /lib/security/$ISA/pam_env.so

auth sufficient /lib/security/$ISA/pam_unix.so likeauth nullok

auth sufficient /lib/security/$ISA/pam_krb5,so use_first_pass

auth sufficient /lib/security/$ISA/pam_winbind.so use_first_pass

auth required /lib/security/$ISA/pam_deny.so

account required /lib/security/$ISA/pam_unix.so broken_shadow

account sufficient /lib/security/$ISA/pam_succeed_if.so uid 100 quiet

account [default=bad success=ok user_unknown=ignore] /lib/security/$ISA/pam_krb5,so

account [default=bad success=ok user_unknown=ignore] /lib/security/$ISA/pam_winbind.so

account required /lib/security/$ISA/pam_permit.so

password requisite /lib/security/$ISA/pam_cracklib.so retry=3

password sufficient /lib/security/$ISA/pam_unix.so nullok use_authtok md5 shadow
```

```
password sufficient /lib/security/$ISA/pam_krb5,so use_authtok

password sufficient /lib/security/$ISA/pam_winbind.so use_authtok

password required /lib/security/$ISA/pam_deny.so

session required /lib/security/$ISA/pam_limits.so

session required /lib/security/$ISA/pam_unix.so

session optional /lib/security/$ISA/pam_krb5,so
```

Winbind-Konfiguration für openwsman und sfcb für SUSE Linux Enterprise Server-Betriebssysteme

1. Sichern Sie die folgenden Dateien:
   - **/etc/pam.d/openwsman**
   - **/etc/pam.d/sfcb**
   - **/etc/pam.d/system-auth**
   - **/etc/pam.d/common-account**
2. Ersetzen Sie den Inhalt von **/etc/pam.d/openwsman/** und **/etc/pam.d/sfcb** durch:

   ```
   %PAM-1.0

   auth include common-auth

   auth required /lib/security/pam_nologin.so

   account include common-account
   ```

3. Ersetzen Sie den Inhalt von **/etc/pam.d/common-auth** durch:

   ```
   auth required pam_env.so

   auth sufficient pam_unix2.so debug

   auth sufficient pam_winbind.so use_first_pass debug
   ```

4. Ersetzen Sie den Inhalt von **/etc/pam.dcommon-account** durch:

   ```
   account sufficient pam_unix2.so

   account sufficient pam_winbind.so
   ```

Möglichkeiten für das Libssl-Problem

Wenn die durch openwsman vorgeschriebene Bibliothek auf Ihrem System vorhanden ist, versucht das Script **autoconf_cim_component.sh**, das **libssl.so**-Problem zu lösen. Wenn die Bibliothek jedoch nicht vorhanden ist, dann meldet das Script das gleiche Problem. Prüfen Sie, ob die neueste Version der **libssl**-Bibliothek auf Ihrem System installiert ist, und erstellen Sie dann einen Softlink mit **libssl.so**.

Beispiel: Falls sich `libssl.so.0.9.8a` und `libssl.so.0.9.8b` in **/usr/lib** befinden, erstellen Sie einen Softlink mit der neuesten `libssl.so.0.9.8b`.

- `ln -sf /usr/lib/libssl.so.0.9.8b /usr/lib/libssl.so`
- `ldconfig`

Managed System Software deinstallieren

Sie können die Managed System Software über die Red Hat Enterprise Linux-, die SUSE Linux Enterprise Server-, oder die VMware ESX-Befehlszeile deinstallieren.

Voraussetzungen für die Deinstallation von Managed System Software

Sie müssen mit `root` angemeldet sein.

Deinstallieren der Managed System Software über die Red Hat Enterprise Linux- oder SUSE Linux Enterprise Server-Befehlszeile

Beim Installieren von Server Administrator wird ein Deinstallationsscript installiert. Sie können das Script ausführen, indem Sie `srvadmin-uninstall.sh` eingeben und dann die <Eingabetaste> drücken.

Benutzerdefinierte Deinstallation spezifischer Komponenten

Einige einzelne Komponenten von Dell OpenManage können deinstalliert werden, ohne dass Dell OpenManage insgesamt deinstalliert werden muss. Im Folgenden sind einige Beispiele aufgeführt:

Um nur den Server Administrator Web Server zu deinstallieren, verwenden Sie den Befehl:

```
rpm –e `rpm -qa | grep srvadmin-iws`
```

Verwenden Sie zur Deinstallation der Speicherkomponente den folgenden Befehl:

```
rpm –e `rpm -qa | grep srvadmin-storage`
```

Verwendung von Dell OpenManage mit Citrix XenServer Dell Edition™

Dell OpenManage Server Administrator ist bei der Citrix®XenServer Dell Edition bereits installiert, so dass keine weiteren Installationsschritte notwendig sind. Weitere Informationen zur Benutzung von Dell OpenManage mit der Citrix XenServer Dell Edition finden Sie im *Citrix XenServer Dell Edition Solution Guide* unter **http://support.dell.com/support/edocs/software/Citrix/.**

Managed System Software-Installation mit Hilfe von Bereitstellungssoftware von Drittanbietern

Sie können Software, die von Drittanbietern bereitgestellt wird, wie z. B. Altiris Deployment Solution, verwenden, um Managed System Software auf unterstützten Dell Servern zu installieren. Um Managed System Software mit Altiris zu verteilen und installieren, starten Sie die Altiris-Anwendung und importieren Sie **OpenManage_Jobs.bin**, das sich unter **SYSMGMT\srvadmin\support\Altiris** auf der DVD *Dell Systems Management Tools and Documentation* befindet. Geben Sie einen Auftragsordner an, in den **OpenManage_Jobs.bin** importiert werden soll. Sie müssen möglicherweise die Tasks **Script ausführen** und **Datei kopieren** ändern, so dass diese der Bereitstellungsumgebung entsprechen. Nach Fertigstellung können Sie den Auftrag so planen, dass dieser auf unterstützten Dell -Systemen ausgeführt wird, die innerhalb der Altiris Deployment Solution verwaltet werden.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Installieren von Managed System-Software auf Microsoft Windows-Betriebssystemen

Dell™ OpenManage™ Server Administrator Version 6.2- Installationshandbuch

---

Übersicht

In diesem Abschnitt ist die Installation von Managed System-Software auf unter Microsoft® Windows® laufenden Systemen beschrieben.

Auf Microsoft Windows-Betriebssystemen wird ein Autostart-Dienstprogramm angezeigt, wenn Sie die DVD *Dell Systems Management Tools and Documentation* einlegen. Mithilfe dieses Dienstprogramms können Sie die System-Management-Software wählen, die Sie auf Ihren System installieren möchten.

Wenn das Autostart-Programm nicht automatisch gestartet wird, verwenden Sie das Setup-Programm im Verzeichnis **SYSMGMT\srvadmin\windows** auf der DVD *Dell Systems Management Tools and Documentation*. Sie können die Funktionen über das Betriebssystem deinstallieren. Eine Liste der derzeit unterstützten Betriebssysteme finden Sie im Dokument *Dell Systems Software Support Matrix*.

Unbeaufsichtigte und nach Skript ablaufende Installation im Hintergrund

Mithilfe der DVD *Dell Systems Management Tools and Documentation* können Sie eine nicht überwachte und nach Skript im Hintergrund ablaufende Installation der Managed System-Software durchführen. Darüber hinaus können Sie die Funktionen von der Befehlszeile aus installieren und deinstallieren.

Voraussetzungsprüfung für Installationsverfahren

ANMERKUNG: Wenn Sie unterstützende Agenten für das einfache Netzwerkverwaltungsprotokoll (SNMP) verwenden möchten, müssen Sie die Betriebssystemunterstützung für den SNMP-Standard vor oder nach der Installation von Server Administrator installieren. Weitere Informationen zur Installation von SNMP finden Sie in den Installationsanweisungen zum Betriebssystem auf Ihrem System.

Das Setup-Programm (unter **\SYSMGMT\srvadmin\windows**)startet das Voraussetzungsprüfungsprogramm. Das Voraussetzungsprüfungsprogramm überprüft die Voraussetzungen für Softwarekomponenten, ohne die tatsächliche Installation zu starten. In diesem Programm wird ein Statusfenster angezeigt, das Informationen zu Hardware und Software Ihres Systems bietet, die die Installation und den Betrieb einiger Softwarekomponenten beeinflussen können.

Bei der Voraussetzungsprüfung werden drei Arten von Meldungen angezeigt: Informationen, Warnungen und Fehler.

Eine Informationsmeldung beschreibt eine Bedingung, verhindert jedoch nicht die Installation einer Funktion.

Warnmeldungen beschreiben einen Zustand, der die Installation eines Softwareprodukts während einer typischen Installation verhindert. Es wird empfohlen, den die Warnung verursachenden Zustand zu beheben, bevor Sie mit der Installation dieser Software fortfahren. Wenn Sie beschließen fortzufahren, können Sie die Software mittels benutzerdefinierter Installation auswählen und installieren. Wenn beispielsweise keine Intel-Netzwerkschnittstellenkarte (NIC) auf dem System erkannt wird, wird die folgende Meldung angezeigt:

```
An Intel(R) NIC was not detected on this system. This will disable the "Typical" installation of the Intel(R) SNMP Agent.

Use the "Custom" installation setup type later during installation to select this feature if you have an Intel(R) NIC installed.

(Es wurde keine Intel(R)-NIC auf dem System gefunden. Hiermit wird die "typische" Installation des Intel (R) SNMP-Agenten deaktiviert.

Verwenden Sie das "benutzerdefinierte" Installations-Setup später während der Installation, um diese Funktion auszuwählen, wenn eine Intel(R)-NIC installiert ist.)
```

Eine Fehlermeldung beschreibt eine Bedingung, die verhindert, dass eine Softwarefunktion installiert wird. Sie müssen den Zustand, der den Fehler verursacht, beheben, bevor Sie mit der Installation des Softwarefunktion fortfahren. Wenn Sie das Problem nicht lösen, wird die Softwarefunktion nicht installiert.

Verwenden Sie den Befehl `RunPreReqChecks.exe /s` (unter **\SYSMGMT\srvadmin\windows\PreReqChecker**), um die Voraussetzungsprüfung im Hintergrund auszuführen. Weitere Informationen finden Sie unter "Voraussetzungsprüfung".

Anforderungen für die Remote-Aktivierung

Zum Installieren der Funktion "Remote-Aktivierung" müssen auf Ihrem System die folgenden Elemente konfiguriert sein:

- Windows Remote Management (WinRM)

- Durch Zertifizierungsstelle/Selbstsigniertes Zertifikat
- WinRM HTTPS-Listener-Port
- Autorisierung für WinRM- und Windows Management Instrumentation-Server (WMI)

Installieren von WinRM

Installieren Sie WinRM Version 1.1 bei Verwendung des Windows Server 2003-Betriebssystems. Sie können WinRM Version 1.1 von **http://www.microsoft.com/downloads/details.aspx?familyid=845289ca-16cc-4c73-8934-dd46b5ed1d33&displaylang=en** herunterladen und installieren.

Auf Windows Server 2008 R2 und Win7 wird standardmäßig WinRM Version 2.0 installiert. Auf Windows Server 2008 wird standardmäßig WinRM Version 1.1 installiert.

Zertifizierungsstelle - Signiertes/selbstsigniertes Zertifikat

Sie benötigen ein durch die Zertifizierungsstelle (CA) signiertes Zertifikat oder ein selbstsigniertes Zertifikat, um die Funktion "Remote-Aktivierung" auf Ihrem System zu installieren und zu konfigurieren. Es wird empfohlen, ein durch die Zertifizierungsstelle (CA) signiertes Zertifikat zu verwenden. Sie können selbstsignierte Zertifikate auch mit dem SelfSSL-Tool erzeugen.

Verwenden eines durch die Zertifizierungsstelle (CA) signiertes Zertifikats

1. Anfordern eines gültigen, durch die Zertifizierungsstelle (CA) signierten Zertifikats
2. Erstellen des HTTPS-Listeners mit dem durch die Zertifizierungsstelle (CA) signierten gültigen Zertifikat

Anfordern eines gültigen, durch die Zertifizierungsstelle (CA) signierten Zertifikats

1. Klicken Sie auf **Start**→ **Ausführen**.
2. Geben Sie mmc ein und klicken Sie auf **OK**.
3. Klicken Sie auf **Datei**→ **Snap-In hinzufügen/entfernen**.
4. Wählen Sie das Zertifikat aus und verschieben Sie es auf die rechte Seite.
5. Wählen Sie im neuen Dialogfeld **Computerkonto** aus, klicken Sie auf **Weiter** und anschließend auf **Fertigstellen**.
6. Klicken Sie auf **OK**.
7. Erweitern Sie **Zertifikate** in der neu hinzugefügten Struktur.
8. Klicken Sie mit der rechten Maustaste auf **Persönlich** und wählen Sie **Alle Aufgaben**→ **Neues Zertifikat anfordern**.
9. Klicken Sie auf **Weiter**.
10. Wählen Sie den entsprechenden Zertifikattyp "Vorwiegend (Computer)" aus und klicken Sie auf **Registrieren**.
11. Klicken Sie auf **Fertigstellen**.

Erstellen des HTTPS-Listeners mit dem durch die Zertifizierungsstelle (CA) signierten gültigen Zertifikat

Führen Sie das Installationsprogramm aus und klicken Sie auf den Link der Voraussetzungsprüfung, um den HTTPS-Listener zu erstellen.

Erstellen selbstsignierter Zertifikate mithilfe des SelfSSL-Tools

1. Erstellen eines Zertifikats
2. Hinzufügen eines Zertifikats und Aufnahme eines Fingerabdrucks
3. Erstellen des WinRM HTTPS-Listeners

4. Konfigurieren des Umschlagformats für WinRM

Erstellen eines Zertifikats

1. Laden Sie das **IIS Resource Kit** von **http://www.microsoft.com/downloads/details.aspx?FamilyID=56fc92ee- a71a-4c73-b628-ade629c89499&displaylang** herunter.
2. Führen Sie **iis60rkt.exe** aus.
3. Klicken Sie auf **Weiter**.
4. Wählen Sie **Ich akzeptiere** auf dem Bildschirm **Endbenutzer- Lizenzvertrag** aus und klicken Sie auf **Weiter.**
5. Klicken Sie auf **Weiter**.
6. Wählen Sie auf dem Bildschirm **Typ auswählen** die Option **Benutzerdefiniert** aus und klicken Sie auf **Weiter**.
7. Klicken Sie auf **Weiter**.
8. Wählen Sie auf dem Bildschirm **Funktionen auswählen** die Option **SelfSSL 1.0** aus und klicken Sie auf **Weiter**.
9. Klicken Sie auf **Weiter**.
10. Klicken Sie auf **Fertigstellen**.

    Das **SelfSSl**-Tool wurde installiert.
11. Klicken Sie auf **Start→ Programme→ IIS-Ressource→ SelfSSL→ SelfSSL**.
12. Typ
    `selfssl /T /N:CN=<Computername oder Domänenname>.`

Hinzufügen eines Zertifikats und Aufnahme eines Fingerabdrucks

Wenn Internet Information Service (IIS) bereits auf dem System installiert ist, muss der Wert von `CertificateThumbprint` einer leeren Zeichenkette entsprechen. In diesem Fall brauchen Sie die Schritte in diesem Abschnitt nicht durchzuführen. Beispiel:

```
winrm create winrm/config/Listener?Address=*+Transport=HTTPS @{Hostname="<Host_name>";CertificateThumbprint=""}
```

1. Klicken Sie auf **Start→ Ausführen**.
2. Geben Sie `mmc` ein und klicken Sie auf **OK**.
3. Klicken Sie auf **Datei→ Snap-In hinzufügen/entfernen**.
4. Klicken Sie auf **Hinzufügen**.
5. Wählen Sie **Zertifikate** aus und klicken Sie auf **Hinzufügen**.
6. Wählen Sie die Option **Computerkonto** aus und klicken Sie auf **Weiter**.
7. Wählen Sie **Lokaler Computer** aus und klicken Sie auf **Fertigstellen**.
8. Klicken Sie auf **Schließen**.
9. Klicken Sie auf **OK**.
10. Erweitern Sie **Zertifikate (Lokaler Computer)** im linken Navigationsfenster des **Konsolenbildschirms**.
11. Erweitern Sie **Persönlich**.
12. Wählen Sie **Zertifikate** aus.
13. Doppelklicken Sie im rechten Fenster auf das erforderliche Zertifikat.

Der Bildschirm **Zertifikate** wird angezeigt.

14. Klicken Sie auf die Registerkarte **Details**.
15. Wählen Sie **Fingerabdruck** aus.

    Kopieren Sie den Fingerabdruck in die Zwischenablage. Sie können diesem Parameter während der Erstellung des HTTPS-Listeners verwenden.

16. Klicken Sie auf **OK**.

Erstellen des WinRM HTTPS-Listeners

Geben Sie den folgenden Befehl zum Aktivieren des HTTPS-Listeners auf WinRM ein:

```
winrm create winrm/config/Listener?Address=*+Transport=HTTPS @
{Hostname="<host_name>";CertificateThumbprint="6e132c546767bf16a8acf4fe0e713d5b2da43013"}
```

Lassen Sie den Wert für `CertificateThumbprint` (Zertifikat-Fingerabdruck) bei Verwendung von Windows 2008 Small Business Server wie folgt leer:

```
winrm create winrm/config/Listener?Address=*+Transport=HTTPS @{Hostname="<Host_name>";CertificateThumbprint=""}
```

ANMERKUNG: Stellen Sie sicher, dass die Werte von `Hostname` und `CertificateThumbprint` (Zertifikat-Fingerabdruck) richtig sind.

Der HTTP-Listener ist standardmäßig aktiviert und hört Anschluss 80 ab.

Konfigurieren der Benutzerautorisierung für WinRM- und WMI-Server

Für das Bereitstellen von Zugriffsberechtigungen zu WinRM- und WMI-Diensten müssen Benutzer explizit mit den entsprechenden Zugriffsebenen hinzugefügt werden.

ANMERKUNG: Sie müssen sich mit Administratorberechtigungen anmelden, um die Benutzerautorisierung für WinRM- und WMI-Server zu konfigurieren.

ANMERKUNG: Der Administrator ist standardmäßig konfiguriert.

WinRM:

1. Klicken Sie auf **Start** und anschließend auf **Ausführen**.
2. Geben Sie `winrm configsddl` ein und klicken Sie auf **OK**.

   Geben Sie bei Verwendung von WinRM Version 2.0 `winrm configsddl default` ein.

3. Klicken Sie auf **Hinzufügen** und fügen Sie die erforderlichen Benutzer oder Gruppen (lokal/Domäne) zur Liste hinzu.
4. Versehen Sie die jeweiligen Benutzer mit der bzw. den entsprechenden Berechtigung(en) und klicken Sie auf **OK**.

WMI:

1. Klicken Sie auf **Start** und anschließend auf **Ausführen**.
2. Geben Sie `wmimgmt.msc` ein und klicken Sie auf **OK**.

   Der Bildschirm **Windows Management Infrastructure (WMI)** wird angezeigt.

3. Klicken Sie mit der rechten Maustaste im linken Fenster auf den Knoten **WMI-Steuerung (Lokal)** und wählen Sie **Eigenschaften**.

   Der Bildschirm **WMI-Steuerung (Lokal) - Eigenschaften** wird angezeigt.

4. Klicken Sie auf **Sicherheit** und erweitern Sie den **Stamm**-Knoten in der Namespacestruktur.
5. Navigieren Sie zu **Stamm**→ **DCIM**→ **sysman**.
6. Klicken Sie auf **Sicherheit**.

   Der Bildschirm **Sicherheit** wird angezeigt.

7. Klicken Sie auf **Hinzufügen** und fügen Sie die erforderlichen Benutzer oder Gruppen (lokal/Domäne) zur Liste hinzu.
8. Versehen Sie die jeweiligen Benutzer mit der bzw. den entsprechenden Berechtigung(en) und klicken Sie auf **OK**.
9. Klicken Sie auf **OK**.
10. Schließen Sie den Bildschirm **Windows Management Infrastructure (WMI)**.

Konfigurieren der Windows-Firewall für WinRM

1. Öffnen Sie die Systemsteuerung.
2. Klicken Sie auf **Windows Firewall**.
3. Klicken Sie auf die Registerkarte **Ausnahmen**.
4. Markieren Sie das Kontrollkästchen **Windows Remote Management**. Falls das Kontrollkästchen nicht angezeigt wird, klicken Sie auf die Schaltfläche **Programm hinzufügen,** um Windows Remote Management hinzuzufügen.

Konfigurieren des Umschlagformats für WinRM

1. Öffnen Sie eine Befehlszeile.
2. Geben Sie `winrm g winrm/config` ein.
3. Prüfen Sie den Wert des Attributs **MaxEnvelopeSizekb**. Wenn der Wert kleiner als **4608** ist, geben Sie den folgenden Befehl ein:

   ```
   winrm s winrm/config @{MaxEnvelopeSizekb="4608"}
   ```

4. Stellen Sie den Wert für **MaxTimeoutms** auf 3 Minuten ein:

   ```
   winrm s winrm/config @{MaxTimeoutms ="180000"}
   ```

Aktivieren Sie in WinRM Version 2.0 den Kompatibilitätsmodus für WinRM Version 2.0 zur Verwendung von Anschluss 443. WinRM Version 2.0 verwendet standardmäßig Anschluss 5986. Verwenden Sie zum Aktivieren des Kompatibilitätsmodus den folgenden Befehl:

```
winrm s winrm/config/Service @{EnableCompatibilityHttpsListener="true"}
```

Installieren und Aktualisieren von Server Administrator

In diesem Abschnitt wird erklärt, wie Server Administrator mithilfe von zwei Installationsoptionen installiert wird:

- Mit dem Setup-Programm unter **\SYSMGMT\srvadmin\windows** auf der DVD *Dell Systems Management Tools and Documentation*, um Server Administrator und andere Managed System-Software zu installieren.
- Mit der unbeaufsichtigten Installationsmethode über das Windows Installer Engine **msiexec.exe** (siehe Tabelle 5-1), um Server Administrator und andere Managed System-Software auf mehreren Systemen zu installieren.

ANMERKUNG: Der SNMP (Simple Network Management Protocol, Einfaches Netzwerk-Verwaltungsprotokoll)-Dienst wird während der Installation und Deinstallation von Systems Management angehalten und gestartet. Demzufolge werden Dienste wie DSM IT Assistant Connection Service, DSM IT Assistant Network Monitor sowie andere Drittanbieterdienste, die von SNMP abhängig sind, ebenfalls angehalten. Die IT Assistant-Dienste werden zum Ende der Installation oder Deinstallation von Systems Management gestartet. Wenn die Drittanbieterdienste angehalten werden, müssen diese Dienste manuell neu gestartet werden.

ANMERKUNG: Bei modularen Systemen muss Server Administrator auf jedem Servermodul im Gehäuse installiert werden.

ANMERKUNG: Nachdem Sie Server Administrator auf PowerEdge 800-, 830-, 850- und 1800-Systemen installiert haben, werden Sie möglicherweise aufgefordert, Ihr System neu zu starten, wenn Sie beschlossen haben, den Storage Management-Dienst zu installieren.

ANMERKUNG: Während der Installation von Server Administrator auf unterstützten Windows-Systemen müssen Sie, falls die Fehlermeldung **Nicht genügend Speicherplatz vorhanden** angezeigt wird, die Installation abbrechen und freien Speicherplatz schaffen. Schließen Sie Anwendungen oder führen Sie andere Vorgänge aus, die freien Speicherplatz schaffen, bevor Sie die Installation von Server Administrator erneut versuchen.

Das Setup-Programm ruft die Voraussetzungsprüfung auf, die den PCI-Bus des Systems zum Suchen nach installierter Hardware wie z. B. Controller-Karten verwendet.

Das Dell OpenManage-Installationsprogramm enthält die Optionen **Typisches Setup** und **Benutzerdefiniertes Setup** für die Installation von Server Administrator und anderer Managed System-Software.

Informationen zu den verschiedenen in Dell OpenManage verfügbaren Komponenten von Server Administrator und zur Unterstützung bei der Auswahl der zu installierenden erforderlichen Komponenten finden Sie unter "Bereitstellungsszenarien für Server Administrator".

Typische Installation

Wenn Sie die Installation von Server Administrator über die Voraussetzungsprüfung starten und die Option **Typisches Setup** auswählen, installiert das Setup-Programm die folgenden Funktionen der Managed System-Software:

- Server Administrator Web Server
- Server Instrumentation
- Remote-Access-Controller
- Intel SNMP-Agent
- Broadcom SNMP-Agent.

Bei einer **typischen** Installation werden einzelne Management Station-Dienste nicht auf verwalteten Systemen installiert, wenn diese die spezifischen Hardware- und Softwareanforderungen für diesen Dienst nicht erfüllen. Das RAC-Service-Softwaremodul von Dell OpenManage Server Administrator wird z. B. bei einer **typischen** Installation nur dann installiert, wenn das verwaltete System über einen Remote Access Controller verfügt. Sie können jedoch zum **benutzerdefinierten Setup** wechseln und das Softwaremodul des **RAC**-Dienstes zur Installation auswählen.

ANMERKUNG: Die Funktion "Remote-Aktivierung" ist nur über die Option **Benutzerdefiniertes Setup** verfügbar.

ANMERKUNG: Bei der Installation von Server Administrator werden auch einige der erforderlichen Visual C++ Laufzeitkomponenten auf Ihrem System installiert.

Benutzerdefinierte Installation

Die folgenden Abschnitte behandeln die Installation von Server Administrator und anderer Managed System-Software über die Option **Benutzerdefiniertes Setup**.

ANMERKUNG: Management Station und Managed System-Dienste können im selben oder in unterschiedlichen Verzeichnissen installiert werden. Sie können das Verzeichnis für die Installation auswählen.

1. Melden Sie sich mit integrierten Administratorberechtigungen beim System an, auf dem die System Management-Software installiert werden soll.
2. Schließen Sie alle geöffneten Anwendungsprogramme und deaktivieren Sie eventuell vorhandene Virenerkennungssoftware.
3. Legen Sie die DVD *Dell Systems Management Tools and Documentation* in das DVD-Laufwerk Ihres Systems ein. Das Autostart-Menü wird angezeigt.
4. Wählen Sie im Autostart-Menü den Punkt **Dell OpenManage Server Administrator** aus und klicken Sie auf **Installieren**.

   Falls das Autostart-Programm nicht automatisch gestartet wird, wechseln Sie in das Verzeichnis **SYSMGMT\srvadmin\windows** auf der DVD und führen Sie die Datei **setup.exe** aus.

   Der Voraussetzungsstatus-Bildschirm von **Dell OpenManage Server Administrator** wird angezeigt und die Voraussetzungsprüfungen für das verwaltete System werden ausgeführt. Alle relevanten Informations-, Warn- oder Fehlermeldungen werden angezeigt. Lösen Sie alle Fehler- und Warnsituation, falls vorhanden.
5. Klicken Sie auf die Option **Server Administrator installieren, ändern, reparieren oder entfernen**.

   Der Bildschirm **Willkommen beim Installationsassistenten des Dell OpenManage Server Administrator** wird angezeigt.
6. Klicken Sie auf **Weiter**.

   Die **Dell Software-Lizenzvereinbarung** wird eingeblendet.
7. Klicken Sie auf **Ich stimme den Bedingungen des Lizenzvertrags zu** und auf **Weiter**, wenn Sie zustimmen.

   Das Dialogfeld **Setup-Typ** wird geöffnet.
8. Wählen Sie **Benutzerdefiniert** und klicken Sie auf **Weiter**.

   Das Dialogfeld **Benutzerdefiniertes Setup** wird geöffnet.

   Informationen zur Unterstützung bei der Auswahl der Server Administrator-Komponenten für Ihr System finden Sie unter Tabelle 4-1 und Tabelle 4-2.

   Wenn Sie Server Administrator auf einem anderen System als dem Dell PowerEdge-System installieren, zeigt das Installationsprogramm nur die Option **Server Administrator Web Server** an.

   Neben einer ausgewählten Funktion ist ein Festplattenlaufwerksymbol zu sehen. Neben einer Funktion, deren Auswahl aufgehoben wurde, ist ein rotes **X** zu sehen. Wenn die Voraussetzungsprüfung eine Softwarefunktion ohne unterstützende Hardware findet, hebt sie deren Auswahl standardmäßig auf.

   Klicken Sie zur Annahme des Standardverzeichnispfads für die Installation der Managed System-Software auf **Weiter**. Klicken Sie andernfalls auf **Ändern** und wechseln Sie zu dem Verzeichnis, in das die Managed System-Software installiert werden soll. Klicken Sie anschließend auf **OK**. Sie werden zum Dialogfeld **Benutzerdefiniertes Setup** zurückgebracht.
9. Klicken Sie auf **Weiter**, um die zur Installation ausgewählten Softwarefunktionen anzunehmen.

Das Dialogfeld **Zur Installation des Programms bereit** wird angezeigt.

ANMERKUNG: Sie können das Installationsverfahren abbrechen, indem Sie auf **Abbrechen** klicken. Die Installation setzt die durchgeführten Änderungen zurück. Wenn Sie nach einem bestimmten Punkt im Installationsverfahren auf **Abbrechen** klicken, kann die Installation die Änderungen eventuell nicht ordnungsgemäß rückgängig machen und das System verbleibt mit einer unvollständigen Installation. Siehe "Systemwiederherstellung bei einer fehlgeschlagenen Installation".

10. Klicken Sie auf **Installieren**, um die ausgewählten Softwarefunktionen zu installieren.

    Der Bildschirm **Dell OpenManage Server Administrator wird installiert** wird angezeigt. Er bietet Aufschluss über Status und Fortschritt der gerade installierten Softwarefunktionen. Nach der Installation der ausgewählten Funktionen wird das Dialogfeld **Installationsassistent abgeschlossen** geöffnet.

11. Klicken Sie auf **Fertigstellen**, um die Installation von Server Administrator abzuschließen.

    Starten Sie das System neu, wenn Sie dazu aufgefordert werden, um die installierten Managed System-Softwaredienste für den Gebrauch bereitzustellen. Wenn Sie zum Neustart Ihres Systems aufgefordert werden, wählen Sie eine Neustartoption:

    - **Ja, das System jetzt neustarten.**
    - **Nein, das System später neustarten.**

ANMERKUNG: Wenn Sie während der Installation **Remote-Aktivierung** ausgewählt haben, wird die Fehlermeldung "Ein Provider, WinTunnel, wurde im Windows Management Instrumentation-Namespace ROOT\dcim\sysman zur Verwendung des LocalSystem-Kontos registriert. Dieses Konto ist privilegiert und der Provider verursacht u. U. eine Sicherheitsverletzung, wenn das Konto für Benutzeraufforderungen nicht die korrekte Identität annimmt." im Windows-Ereignisprotokoll aufgezeichnet. Sie können diese Meldung einfach ignorieren und mit der Installation fortfahren.

Server Administrator-Installation mit Citrix Application Server

Citrix adressiert alle Laufwerksbuchstaben um, wenn es installiert ist. Wenn Sie beispielsweise Server Administrator auf dem Laufwerk **C:** installieren und anschließend Citrix installieren, kann es den Laufwerksbuchstaben **C:** in **M:** ändern. Aufgrund der Neuzuweisung kann es vorkommen, dass Server Administrator möglicherweise nicht ordnungsgemäß funktioniert.

Wählen Sie zur Vermeidung dieses Problems eine dieser Optionen:

Option 1:

1. Deinstallieren Sie Server Administrator.
2. Installieren Sie Citrix.
3. Installieren Sie Server Administrator neu.

Option 2:

Geben Sie nach der Installation von Citrix den folgenden Befehl ein:

```
msiexec.exe /fa SysMgmt.msi
```

Erweitern der Managed System-Software

Das Dell OpenManage-Installationsprogramm bietet eine **Upgrade**-Option für die Erweiterung von Server Administrator und anderer Managed System-Software.

Das Setup-Programm führt die **Voraussetzungsprüfung** aus, die den PCI-Bus des Systems zum Suchen nach installierter Hardware wie z. B. Controller-Karten verwendet.

Das Setup-Programm installiert oder aktualisiert alle Managed System-Softwarefunktionen, die der spezifischen Hardwarekonfiguration des Systems entsprechen.

VORSICHTSHINWEIS: Dell OpenManage Array Manager wird nicht mehr unterstützt. Wenn Sie ein mit Array Manager installiertes System erweitern (installiert mit der Dell OpenManage Version 5.0 oder höher), wird Array Manager während des Upgrade-Vorgangs entfernt. Sie können stattdessen den Storage Management-Dienst verwenden.

ANMERKUNG: Alle Benutzereinstellungen werden während der Aktualisierung beibehalten.

In den folgenden Verfahren ist die Aktualisierung von Server Administrator und anderer Managed System-Software beschrieben.

Erweiterungsrichtlinien

- Sie können Versionen von Server Administrator, die älter als Version 5.0 sind, nicht auf Version 6.2 aktualisieren. Sie müssen zuerst auf eine höhere Server Administrator-Version als 5.0 und anschließend auf Server Administrator Version 6.2 aktualisieren.
- Wenn Server Instrumentation auf dem verwalteten System installiert ist, stellen Sie sicher, dass Sie Server Administrator Web Server Version 6.1 oder höher installieren. Wenn eine frühere Version von Server Administrator Web Server installiert wird, wird möglicherweise ein Fehler angezeigt.

- Wenn Server Administrator Web Server Version 6.2 installiert ist, stellen Sie sicher, dass Sie Server Instrumentation Version 6.2 auf Ihrem verwalteten System installieren. Der Zugriff auf eine frühere Version von Server Administrator mit Server Administrator Web Server Version 6.2 kann die Anzeige eines Fehlers bewirken.

Erweitern

1. Legen Sie die DVD *Dell Systems Management Tools and Documentation* in das DVD-Laufwerk Ihres Systems ein. Das Autostart-Menü wird angezeigt.

2. Klicken Sie auf **Dell OpenManage Server Administrator** und auf **Installieren**.

   Falls das Autostart-Programm nicht automatisch startet, wechseln Sie in das Verzeichnis **SYSMGMT\srvadmin\windows** auf der DVD und führen Sie die Datei **setup.exe** aus.

   Der **Voraussetzungsstatus-Bildschirm des Dell OpenManage Server Administrator** wird angezeigt und die Voraussetzungsprüfungen für die verwaltete Station werden ausgeführt. Alle relevanten Informations-, Warnungs- oder Fehlermeldungen werden angezeigt.

3. Klicken Sie auf die Option **Server Administrator installieren, ändern, reparieren oder entfernen**.
   Der Bildschirm **Willkommen beim Installationsassistenten des Dell OpenManage Server Administrator** wird angezeigt.

4. Klicken Sie auf **Weiter**.

   Die **Dell Software-Lizenzvereinbarung** wird angezeigt

5. Klicken Sie auf **Ich stimme den Bedingungen des Lizenzvertrags zu** und auf **Weiter,** falls Sie zustimmen.

   Das Dialogfeld **Setup-Typ** wird geöffnet.

6. Setzen Sie die Installation wie im Abschnitt "Benutzerdefinierte Installation" beschrieben ab "Schritt 8" fort.

Ändern

Wenn Sie Server Administrator-Komponenten hinzufügen/entfernen möchten:

1. Wechseln Sie zur Windows **Systemsteuerung**.

2. Doppelklicken Sie auf **Software**.

3. Klicken Sie auf **Dell OpenManage Server Administrator** und auf **Ändern**.

   Das Dialogfeld **Willkommen beim Installationsassistenten des Dell OpenManage Server Administrator** wird geöffnet.

4. Klicken Sie auf **Weiter**.

   Das Dialogfeld **Programmpflege** wird geöffnet.

5. Wählen Sie die Option **Modifizieren** und klicken Sie auf **Weiter**.

   Das Dialogfeld **Benutzerdefiniertes Setup** wird geöffnet.

6. Zur Auswahl einer bestimmten Managed System-Softwareanwendung klicken Sie auf den Dropdown-Pfeil neben der aufgeführten Funktion und wählen entweder **Diese Funktion wird installiert**, um die Funktion zu installieren, oder **Diese Funktion wird nicht verfügbar sein**, wenn die Funktion ignoriert werden soll.

   Neben einer ausgewählten Funktion ist ein Festplattenlaufwerksymbol zu sehen. Neben einer Funktion, deren Auswahl aufgehoben wurde, ist ein rotes **X** zu sehen. Wenn die Voraussetzungsprüfung eine Softwarefunktion ohne unterstützende Hardware findet, hebt sie deren Auswahl standardmäßig auf.

7. Klicken Sie auf **Weiter,** um die zur Installation ausgewählten Softwarefunktionen anzunehmen.

   Das Dialogfeld **Bereit zum Ändern des Programms** wird angezeigt.

8. Klicken Sie auf **Installieren,** um die ausgewählten Softwarefunktionen zu installieren.

   Der Bildschirm **Dell OpenManage Server Administrator installieren** wird geöffnet. Status und Fortschritt der Installation der Softwarefunktionen werden in Meldungen angezeigt.

   Bei der Installation der ausgewählten Funktionen wird das Dialogfeld **Installationsassistent abgeschlossen** geöffnet.

9. Klicken Sie auf **Fertigstellen,** um die Installation von Server Administrator abzuschließen.

   Starten Sie das System neu, wenn Sie dazu aufgefordert werden, um die installierten Managed System-Softwaredienste für den Gebrauch

bereitzustellen. Wenn Sie zum Neustart Ihres Systems aufgefordert werden, wählen Sie eine Neustartoption:

- **Ja, das System jetzt neustarten.**
- **Nein, das System später neustarten.**

ANMERKUNG: Wenn Sie das Installationsprogramm von einem anderen System aus ausführen und versuchen, eine Komponente mit der Option **Ändern** hinzuzufügen, zeigt das Installationsprogramm möglicherweise einen Fehler an. Dieser Fehler kann auftreten, wenn die Quelle des Systems, von der aus Sie das Installationsprogramm ausgeführt haben, beschädigt ist. Dies kann durch Überprüfen des Registrierungseintrags **HKLM\Software\Classes\Installer\Products\<GUID>\sourcelist\lastusedsource** überprüft werden. Wenn der Wert für **lastusedsource** (zuletzt verwendete Quelle) eine negative Zahl ist, bedeutet dies, dass die Quelle beschädigt ist.

Reparatur

Wenn Sie eine möglicherweise beschädigte installierte Server Administrator-Komponente reparieren möchten:

1. Wechseln Sie zur Windows **Systemsteuerung**.
2. Doppelklicken Sie auf **Software**.
3. Klicken Sie auf **Dell Server Administrator** und auf **Ändern**.

   Das Dialogfeld **Willkommen beim Installationsassistenten des Dell OpenManage Server Administrator** wird geöffnet.
4. Klicken Sie auf **Weiter**.

   Das Dialogfeld **Programmpflege** wird geöffnet.
5. Wählen Sie die Option **Reparatur** und klicken Sie auf **Weiter**.

   Das Dialogfeld **Bereit zur Reparatur des Programms** wird angezeigt.
6. Klicken Sie auf **Installieren**, um die ausgewählten Softwarefunktionen zu installieren.

   Der Bildschirm **Dell OpenManage Server Administrator installieren** wird geöffnet. Status und Fortschritt der Installation der Softwarefunktionen werden in Meldungen angezeigt.

   Nachdem die ausgewählten Funktionen installiert wurden, wird das Dialogfeld **Installationsassistent abgeschlossen** angezeigt.
7. Klicken Sie auf **Fertigstellen**, um die Installation von Server Administrator abzuschließen.

   Wenn Sie zum Neustart Ihres Systems aufgefordert werden, wählen Sie eine Neustartoption:

   - **Ja, das System jetzt neustarten**.
   - **Nein, das System später neustarten.**

Systemwiederherstellung bei einer fehlgeschlagenen Installation

Der Microsoft Software Installer (MSI) verfügt über die Fähigkeit, ein System nach einer fehlerhaften Installation in seinen voll funktionierenden Zustand zurückzusetzen. Dies erfolgt mit einem Rückgängig-Vorgang für jede Standardmaßnahme, die während der Installation, Erweiterung oder Deinstallation ausgeführt wird. Dieser Vorgang umfasst die Wiederherstellung von gelöschten oder überschriebenen Dateien, Registrierungsschlüsseln und anderen Ressourcen. Dateien, die während des Verlaufs einer Installation bzw. Entfernung gelöscht oder überschrieben werden, werden von Windows temporär gespeichert, damit sie nötigenfalls wiederhergestellt werden können. Dies ist eine Art des Zurücksetzens. Nach dem erfolgreichen Abschluss einer Installation werden alle temporären Sicherungsdateien gelöscht.

Neben dem Zurücksetzen von MSI-Standardmaßnahmen ist die Bibliothek von Dell OpenManage auch in der Lage, Befehle rückgängig zu machen, die in der INI-Datei zu jeder Anwendung aufgeführt werden, wenn ein Zurücksetzen stattfindet. Der ursprüngliche Zustand aller Dateien, die durch Dell OpenManage-Installationsmaßnahmen geändert wurden, wird beim Zurücksetzen wiederhergestellt.

Wenn die MSI-Engine die Installationsfolge durchläuft, ignoriert sie alle Maßnahmen, die als Zurücksetz-Maßnahmen eingeplant sind. Wenn eine benutzerdefinierte Maßnahme, eine MSI-Standardmaßnahme oder eine Dell OpenManage-Installationsmaßnahme fehlschlägt, wird ein Zurücksetzungsvorgang gestartet.

Eine einmal abgeschlossene Installation kann nicht mehr rückgängig gemacht werden. Die abgewickelte Installation ist nur als Sicherheitsnetz gedacht, das das System während einer Installationssitzung schützt. Eine installierte Anwendung kann jedoch einfach deinstalliert werden.

ANMERKUNG: Das Installieren und Entfernen von Treibern wird nicht als Teil der Installationstransaktion ausgeführt und kann deshalb nicht zurückgesetzt werden, wenn während der Ausführung ein schwerwiegender Fehler auftritt.

ANMERKUNG: Installationen, Deinstallationen und Upgrades, die während der Installationsbereinigung oder nach Abschluss der Installationstransaktion abgebrochen wurden, können nicht rückgängig gemacht werden.

Fehlgeschlagene Updates

Vom Hersteller bereit gestellte MSI-Patches und -Updates müssen auf die MSI-Pakete des Originalherstellers angewandt werden. Wenn Sie absichtlich oder

zufällig ein MSI-Paket neu verpacken oder direkte Änderungen daran vornehmen, sind die Patches und Updates eventuell fehlerhaft. MSI-Pakete dürfen nicht neu verpackt werden; hierbei werden dieFunktionsstruktur und die GUIDs verändert, die alle bereitgestellten Patches und Updates zerstören. Wenn es notwendig ist, Änderungen an einem vom Hersteller bereitgestellten MSI-Paket vorzunehmen, sollte dazu immer eine **.mst**-Transformationsdatei verwendet werden.

Windows Installer-Protokollierung

Windows enthält einen in der Registry aktivierten Protokollierungsdienst, der bei der Diagnose von Problemen mit dem Windows Installer hilft. Zum Aktivieren dieses Protokollierungsdiensts während einer im Hintergrund ablaufenden Installation öffnen Sie den Registrierungseditor und erstellen den folgenden Pfad und die folgenden Schlüssel:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer
Reg_SZ: Logging
Value: voicewarmup
```

Die Buchstaben im Wertefeld können sich in beliebigen Reihenfolge befinden. Mit jedem Buchstaben wird ein anderer Protokollierungsmodus eingeschaltet. Jeder Buchstabe hat für MSI Version 3.1 die folgende eigentliche Funktion:

v - Ausführliche Ausgabe
o - Meldungen für unzureichenden Speicherplatz
i - Statusmeldungen
c - Erste UI-Parameter
e - Alle Fehlermeldungen
w - Nicht-schwerwiegende Warnhinweise
a - Start von Aktionen
r - Maßnahmenspezifische Datensätze
m - Informationen zu unzureichendem Speicher oder schwerwiegender Beendigung
u - Benutzeranforderungen
p - Terminaleigenschaften
+ - Anhängen an vorhandene Datei
! - Durchlassen jeder Zeile in das Protokoll
"*" - Platzhalter, Protokollieren aller Informationen außer der Option v. Geben Sie zum Einschließen der Option v "/l*v" an.

Nach ihrer Aktivierung können Sie die erstellten Protokolldateien im Verzeichnis %TEMP-% finden. Zu den in diesem Verzeichnis generierten Protokolldateien gehören u. a.:

- **Installation von Managed System**
  - **SysMgmt.log**
- **Installation von Management Station**
  - **MgmtSt.log**

Diese speziellen Protokolldateien werden standardmäßig erstellt, wenn die Benutzerschnittstelle (UI) für die Voraussetzungsprüfung ausgeführt wird.

Unbeaufsichtigte Installation der Managed System Software

Das Dell OpenManage-Installationsprogramm enthält die Option **Typisches Setup** und **Benutzerdefiniertes Setup** für das unbeaufsichtigte Installationsverfahren.

Die unbeaufsichtigte Installation ermöglicht die Installation von Server Administrator auf mehreren Systemen gleichzeitig. Eine unbeaufsichtigte Installation kann durch Erstellen eines dafür vorgesehenen Pakets durchgeführt werden, das alle erforderlichen Managed System-Softwaredateien enthält. Die unbeaufsichtigte Installation stellt außerdem verschiedene Funktionen bereit, mit denen Sie Informationen über unbeaufsichtigte Installationen konfigurieren, überprüfen und anzeigen können.

Durch Verwendung eines Softwareverteilungshilfsprogramms von einem unabhängigen Softwareanbieter (ISV) wird das Paket zur unbeaufsichtigten Installation für die Remote-Systeme bereitgestellt. Wenn das Paket verteilt wird, wird das Installationsskript zur Installation der Software ausgeführt.

Erstellen und Verteilen des Pakets für unbeaufsichtigte typische Installation

Die Option **Typisches Setup** zur unbeaufsichtigten Installation verwendet die DVD *Dell Systems Management Tools and Documentation* als Paket für die unbeaufsichtigte Installation. Das Programm `msiexec.exe /i SysMgmt.msi /qb` greift auf die DVD zu, um die Software-Lizenzvereinbarung anzunehmen und alle erforderlichen Server Administrator-Funktionen auf ausgewählten Remote-Systemen zu installieren. Der Befehl `msiexec.exe /i SysMgmt.msi /qb` installiert Server Administrator-Funktionen auf jedem Remote-System basierend auf der Hardwarekonfiguration des Systems.

ANMERKUNG: Wenn eine unbeaufsichtigte Installation abgeschlossen ist, können Sie die Befehlszeilenschnittstellenfunktion (CLI) von Server Administrator nur verwenden, wenn Sie ein neues Konsolenfenster öffnen und CLI-Befehle von dort ausführen. Die Ausführung von CLI-Befehlen von demselben Konsolenfenster, in dem Server Administrator installiert wurde, ist nicht möglich.

Sie können dem Remote-System das DVD-Image verfügbar machen, indem Sie entweder den gesamten Datenträgerinhalt verteilen oder dem Speicherort des DVD-Images ein Laufwerk des Zielsystems zuordnen.

Zuweisung eines Laufwerks zur Funktion als Paket für die unbeaufsichtigte typische Installation

1. Geben Sie ein Image der DVD *Dell Systems Management Tools and Documentation* für jedes Remote-System frei, auf dem Sie Server Administrator installieren wollen.

Geben Sie hierzu die DVD direkt frei oder kopieren Sie die gesamte DVD auf ein Laufwerk und geben Sie diese Kopie dann frei.

2. Erstellen Sie ein Skript, das dem in Schritt Schritt 1 freigegebenen Laufwerk ein Laufwerk von den Remote-Systemen zuweist. Dieses Skript sollte `msiexec.exe /i Mapped Drive\SYSMGMT\srvadmin\windows\SystemsManagement\SysMgmt.msi /qb` ausführen, nachdem das Laufwerk zugewiesen wurde.

3. Konfigurieren Sie die Verteilungssoftware des unabhängigen Softwareanbieters zur Verteilung und führen Sie das in Schritt Schritt 2 erstellte Skript aus.

4. Verteilen Sie das Skript mithilfe der Softwareverteilungstools eines unabhängigen Softwareanbieters an die Zielsysteme.

   Das Skript wird ausgeführt, um Server Administrator auf jedem Remote-System zu installieren.

5. Starten Sie jedes Remote-System neu, um Server Administrator zu aktivieren.

Verteilen der gesamten DVD als Paket für unbeaufsichtigte typische Installation

1. Verteilen Sie das gesamte Image der DVD *Dell Systems Management Tools and Documentation* an die Zielsysteme.

2. Konfigurieren Sie die Verteilungssoftware des unabhängigen Softwareanbieters, um den Befehl `msiexec.exe /i DVD Drive\SYSMGMT\srvadmin\windows\SystemsManagement\ SysMgmt.msi /qb` vom DVD-Image auszuführen.

   Das Programm wird ausgeführt, um Server Administrator auf jedem Remote-System zu installieren.

3. Starten Sie jedes Remote-System neu, um Server Administrator zu aktivieren.

Erstellen und Verteilen von Paketen für unbeaufsichtigte benutzerdefinierte Installation

Gehen Sie folgendermaßen vor, um ein Paket für unbeaufsichtigte benutzerdefinierte Installation zu erstellen:

1. Kopieren Sie das Verzeichnis **SYSMGMT\srvadmin\windows** von der DVD auf das Festplattenlaufwerk des Systems.

2. Erstellen Sie ein Stapelskript, das die Installation mit der Windows Installer Engine (**msiexec.exe**) ausführt.

   ANMERKUNG: Bei einer benutzerdefinierten unbeaufsichtigten Installation muss jede erforderliche Funktion als ein Befehlszeilenschnittstellen-Parameter (CLI-Parameter) enthalten sein, damit sie installiert wird.

   Ein Beispiel ist `msiexec.exe /i SysMgmt.msi ADDLOCAL=SA,IWS,BRCM /qb`. (Weitere Details und verfügbare Funktionsidentifikationen finden Sie unter "Parameter zur individuellen Einrichtung".)

3. Legen Sie das Stapelskript im **Windows**-Verzeichnis auf dem Festplattenlaufwerk des Systems ab.

Verteilen von Paketen für die benutzerdefinierte unbeaufsichtigte Installation

ANMERKUNG: Das Installationspaket **SysMgmt.msi** für Server Administrator, das beim unbeaufsichtigten **benutzerdefinierten Setup** verwendet wird (siehe "Erstellen und Verteilen von Paketen für unbeaufsichtigte benutzerdefinierte Installation"), befindet sich auf der DVD im Verzeichnis **SYSMGMT\srvadmin\windows\SystemsManagement.**

1. Konfigurieren Sie die Verteilungssoftware des unabhängigen Softwareanbieters so, dass sie das Stapelskript nach Verteilung des Installationspakets ausführt.

2. Verteilen Sie das Paket zur benutzerdefinierten unbeaufsichtigten Installation mithilfe der Verteilungssoftware des unabhängigen Softwareanbieters an die Remote-Systeme.
   Das Stapelskript installiert Server Administrator zusammen mit den angegebenen Funktionen auf jedem Remote-System.

3. Starten Sie jedes Remote-System neu, um Server Administrator zu aktivieren.

Bestimmen der Speicherorte für Protokolldateien

Bei einer Managed System-MSI-Installation führen Sie den folgenden Befehl aus, um eine unbeaufsichtigte Installation mit festgelegtem Speicherort der Protokolldatei auszuführen:

```
msiexec.exe /i SysMgmt.msi /l*v "C:\openmanage\logs\SysMgmt.log"
```

Merkmale der unbeaufsichtigten Installation

Die unbeaufsichtigte Installation besitzt die folgenden Merkmale:

- Eine Reihe von optionalen Befehlszeileneinstellungen, um die unbeaufsichtigte Installation individuell einzurichten
- Parameter zur individuellen Einrichtung, um spezifische Softwarefunktionen zur Installation zu bestimmen
- Ein Voraussetzungsprüfungsprogramm, das den Abhängigkeitsstatus ausgewählter Softwarefunktionen überprüft, ohne eine Installation durchzuführen

Optionale Befehlszeileneinstellungen

In Tabelle 5-1 werden die optionalen Einstellungen aufgeführt, die für den MSI Installer **msiexec.exe** verfügbar sind. Die optionalen Einstellungen werden in der Befehlszeile nach **msiexec.exe** mit jeweils einem Leerzeichen zwischen den einzelnen Einstellungen eingegeben.

ANMERKUNG: Umfassende Details zu allen Befehlszeilenschaltern für das Windows Installer-Tool erhalten Sie unter **support.microsoft.com**.

Tabelle 5-1. Befehlszeileneinstellungen für MSI Installer

Einstellung	Ergebnis
`/i <Paket|Produktcode>`	Mit diesem Befehl wird ein Produkt installiert oder konfiguriert. **/i SysMgmt.msi** - Installiert die Server Administrator-Software.
`/i SysMgmt.msi/qn`	Über diesen Befehl wird eine Neuinstallation von Version 6.1. durchgeführt.
`/x <Paket|Produktcode>`	Mit diesem Befehl wird ein Produkt deinstalliert. **/x SysMgmt.msi** - Deinstalliert die Server Administrator-Software.
`/q[n|b|r|f]`	Mit diesem Befehl wird die Benutzeroberflächen (UI)-Ebene eingestellt. **/q** oder **/qn** - keine UI. Diese Option wird für im Hintergrund ablaufende und unbeaufsichtigte Installationen verwendet. **/qb** - elementare UI. Diese Option wird für Installationen verwendet, die unbeaufsichtigt, aber nicht im Hintergrund ablaufen. **/qr** - reduzierte UI. Diese Option wird für unbeaufsichtigte Installationen verwendet, wobei der Fortschritt der Installation in einem modalen Dialogfeld angezeigt wird. **/qf** – volle UI. Diese Option wird für beaufsichtigte Standardinstallationen verwendet.
`/f[p|o|e|d|c|a|u|m|s|v] <Paket|Produktcode>`	Mit diesem Befehl wird ein Produkt repariert. **/fp** - Mit dieser Option wird ein Produkt nur dann neu installiert, wenn eine Datei fehlt. **/fo** - Mit dieser Option wird ein Produkt neu installiert, wenn eine Datei fehlt oder die ältere Version einer Datei installiert ist. **/fe** - Mit dieser Option wird ein Produkt neu installiert, wenn eine Datei fehlt oder die ältere oder gleiche Version einer Datei installiert ist. **/fd** - Mit dieser Option wird ein Produkt neu installiert, wenn eine Datei fehlt oder eine andere Version einer Datei installiert ist. **/fc** - Mit dieser Option wird ein Produkt neu installiert, wenn eine Datei fehlt oder der gespeicherte Prüfsummenwert nicht mit dem berechneten übereinstimmt. **/fa** - Mit dieser Option wird die Neuinstallation aller Dateien erzwungen. **/fu** - Mit dieser Option werden alle erforderlichen benutzerspezifischen Registrierungseinträge neu geschrieben. **/fm** - Mit dieser Option werden alle erforderlichen systemspezifischen Registrierungseinträge neu geschrieben. **/fs** - Mit dieser Option werden alle vorhandenen Verknüpfungen überschrieben. **/fv** - Diese Option wird von der Quelle ausgeführt und das lokale Paket wird erneut gecacht. Verwenden Sie für die erste Installation einer Anwendung oder Funktion nicht die Option **/fv** für eine Neuinstallation.
`INSTALLDIR=<Pfad>`	Mit diesem Befehl wird das Produkt an einem festgelegten Standort installiert. Wenn Sie ein Installationsverzeichnis mit diesem Schalter angeben können, muss es manuell vor der Ausführung der CLI-Installationsbefehle erstellt werden, ansonsten wird es fehlerhaft ausgeführt ohne eine Fehlermeldung anzugeben. **/i SysMgmt.msi INSTALLDIR=c:\OpenManage /qn** – Mit diesem Befehl wird ein Produkt zu einem spezifischen Standort unter Verwendung von **c:\OpenManage** als Installationsstandort installiert.

Mit dem Befehl `msiexec.exe /i SysMgmt.msi /qn` werden beispielsweise Server Administrator-Funktionen auf jedem Remote-System basierend auf der Hardwarekonfiguration des Systems installiert. Diese Installation wird im Hintergrund und unbeaufsichtigt durchgeführt.

Parameter zur individuellen Einrichtung

ANMERKUNG: Die CLI-Parameter REINSTALL und REMOVE müssen in Großbuchstaben eingegeben werden, da bei ihnen zwischen Groß- und Kleinschreibung unterschieden wird.

Die CLI-Anpassungsparameter **REINSTALL** und **REMOVE** bieten eine Möglichkeit, die exakten Softwarefunktionen festzulegen, die installiert, neu installiert oder deinstalliert werden sollen, wenn sie im Hintergrund oder unbeaufsichtigt ausgeführt werden. Mithilfe der Parameter zur individuellen Einrichtung können Sie mit demselben unbeaufsichtigten Installationspaket Softwarefunktionen für verschiedene Systeme gezielt installieren, neu installieren oder deinstallieren. So kann beispielsweise ausgewählt werden, dass Server Administrator, jedoch nicht der RAC-Dienst auf einer bestimmten Gruppe von Servern installiert wird und dass Server Administrator, jedoch nicht der Storage Management-Dienst auf einer anderen Gruppe von Servern installiert wird. Sie können auch eine oder mehrere Funktionen auf einer bestimmten Gruppe von Servern deinstallieren.

ANMERKUNG: Die in Tabelle 5-2 erwähnten Softwarefunktions-IDs unterscheiden zwischen Groß- und Kleinschreibung.

Tabelle 5-2. Softwarefunktions-IDs

Funktions-ID	Beschreibung
ALLE	Alle Funktionen
BRCM	Broadcom NIC-Agent
INTEL	IntelNIC-Agent
IWS	Dell OpenManage Server Administrator Web Server
OMSM	Server Administrator Storage Management Service
RmtMgmt	Remote-Aktivierung
RAC4	Remote Access Controller (DRAC 4)
RAC5	Remote Access Controller (DRAC 5)
iDRAC	Integrierter Dell Remote Access Controller
SA	Server Administrator

ANMERKUNG: Nur iDRAC6 wird auf *xx*1*x* -Systemen unterstützt.

Sie können den Parameter **REINSTALL** zur individuellen Einrichtung auf der Befehlszeile einsetzen und die Funktions-ID (oder IDs) der Softwarefunktion, die Sie erneut installieren möchten, zuweisen. Beispiel:

```
msiexec.exe /i SysMgmt.msi REINSTALL=BRCM /qb.
```

Mit diesem Befehl wird die Installation für Dell OpenManage Systems Management ausgeführt und nur der Broadcom-Agent wird in einem unbeaufsichtigten Modus, jedoch nicht im Hintergrundmodus neu installiert.

Sie können den Parameter **REMOVE** zur individuellen Einrichtung auf der Befehlszeile einsetzen und die Funktions-ID (oder IDs) der Softwarefunktion, die Sie deinstallieren möchten, zuweisen. Beispiel:

```
msiexec.exe /i SysMgmt.msi REMOVE=BRCM /qb.
```

Mit diesem Befehl wird die Installation für Dell OpenManage Systems Management ausgeführt und nur der Broadcom-Agent wird in einem unbeaufsichtigten Modus, aber nicht im Hintergrundmodus deinstalliert.

Sie können Funktionen auch durch Ausführung des Programms **msiexec.exe** installieren, neu installieren und deinstallieren. Beispiel:

```
msiexec.exe /i SysMgmt.msi REMOVE=BRCM /qb
```

Mit diesem Befehl wird die Installation für Managed System-Software ausgeführt und der Broadcom-Agent deinstalliert. Diese Ausführung findet in einem unbeaufsichtigten Modus, aber nicht im Hintergrundmodus statt.

ANMERKUNG: Ein GUID (Globaler eindeutiger Kennzeichner, Globally Unique Identifier) ist 128 Bit lang und der zur Erstellung eines GUID verwendete Algorithmus garantiert, dass jeder GUID einmalig ist. Die Produkt-GUID kennzeichnet die Anwendung eindeutig. In diesem Fall lautet die Produkt-GUID für Server Administrator {54C04D53-C3C3-46EA-A75F-7AFF4BEB727C}.

MSI-Rückgabecode

Ein Eintrag im Anwendungsereignisprotokoll wird in der Datei **SysMgmt.log** gespeichert. Tabelle 5-3 zeigt einige der Fehlercodes an, die von der Windows Installer Engine **msiexec.exe** zurückgegeben wurden.

Tabelle 5-3. Windows Installer-Rückgabecodes

Fehlercode	Wert	Beschreibung
ERROR_SUCCESS	0	Die Maßnahme wurde erfolgreich abgeschlossen.
ERROR_INVALID_PARAMETER	87	Einer der Parameter war ungültig.
ERROR_INSTALL_USEREXIT	1602	Der Benutzer hat die Installation abgebrochen.
ERROR_SUCCESS_REBOOT_REQUIRED	3010	Zum Abschluss der Installation ist ein Neustart erforderlich. Diese Meldung weist auf eine erfolgreiche Installation hin.

ANMERKUNG: Umfassende Details zu allen von den Windows Installer-Funktionen **msiexec.exe** und **InstMsi.exe** zurückgegebenen Fehlercodes finden Sie unter **support.microsoft.com**.

Deinstallieren der Managed System-Software

Sie können die Managed System-Softwarefunktionen mithilfe der DVD *Systems Management Tools and Documentation* oder über Ihr Betriebssystem deinstallieren. Des Weiteren können Sie eine unbeaufsichtigte Deinstallation auf mehreren Systemen gleichzeitig durchführen.

Deinstallieren der Managed System-Software mit von Dell bereitgestelltem Datenträger

1. Legen Sie die DVD *Dell Systems Management Tools and Documentation* in das DVD-Laufwerk Ihres Systems ein.

   Falls das Setup-Programm nicht automatisch startet, führen Sie **setup.exe** im Verzeichnis **SYSMGMT\srvadmin\windows** der DVD aus.

   Der Voraussetzungsstatus-Bildschirm von **Dell OpenManage Server Administrator** wird angezeigt und die Voraussetzungsprüfungen für das verwaltete System werden ausgeführt. Alle relevanten Informations-, Warn- oder Fehlermeldungen, die während der Prüfung erkannt wurden, werden angezeigt.

2. Klicken Sie auf die Option **Server Administrator installieren, ändern, reparieren oder entfernen**.

   Der Bildschirm **Willkommen beim Installationsassistenten des Dell OpenManage Server Administrator** wird angezeigt.

3. Klicken Sie auf **Weiter**.

   Das Dialogfeld **Programmpflege** wird geöffnet.

   In diesem Dialogfeld können Sie das Programm ändern, reparieren oder entfernen.

4. Wählen Sie die Option **Entfernen** und klicken Sie auf **Weiter**.

   Das Dialogfeld **Programm entfernen** wird geöffnet.

5. Klicken Sie auf **Entfernen**.

   Der Bildschirm **Dell OpenManage Server Administrator deinstallieren** wird angezeigt und bietet Aufschluss über den Status und Fortschritt der Software-Funktionen, die deinstalliert werden.

   Nachdem die ausgewählten Funktionen deinstalliert wurden, wird das Dialogfeld **Installationsassistent abgeschlossen** angezeigt.

6. Klicken Sie auf **Fertigstellen**, um die Deinstallation von Server Administrator abzuschließen.

   Starten Sie das System neu, wenn Sie dazu aufgefordert werden, um die Deinstallation erfolgreich abzuschließen. Wenn Sie zum Neustart Ihres Systems aufgefordert werden, wählen Sie eine Neustartoption:

   - **Ja, das System jetzt neustarten.**
   - **Nein, das System später neustarten.**

   Alle Server Administrator-Funktionen werden deinstalliert.

Deinstallieren der Managed System-Softwarefunktionen über das Betriebssystem

1. Wechseln Sie zur Windows **Systemsteuerung**.
2. Doppelklicken Sie auf **Software**.
3. Klicken Sie auf **Dell OpenManage Server Administrator** und auf **Entfernen**.

   Das Dialogfeld **Software** wird geöffnet.

4. Klicken Sie auf **Ja**, um die Deinstallation von Server Administrator zu bestätigen.

   Der Bildschirm **Dell OpenManage Server Administrator** wird angezeigt und bietet Aufschluss über Status und Fortschritt der Deinstallation der Softwarefunktionen.

   Starten Sie das System neu, wenn Sie dazu aufgefordert werden, um die Deinstallation erfolgreich abzuschließen. Wenn Sie zum Neustart Ihres Systems aufgefordert werden, wählen Sie eine Neustartoption:

   - **Ja, das System jetzt neustarten.**
   - **Nein, das System später neustarten.**

   Alle Server Administrator-Funktionen werden deinstalliert.

Unbeaufsichtigte Deinstallation mithilfe des des Produkt-GUID

Wenn Ihnen die Installations-DVD oder das MSI-Paket während einer Deinstallation nicht zur Verfügung steht, können Sie die Dell OpenManage Systems Management-Software auf Managed Systems oder Management Stations unter Windows mit der folgenden Befehlszeile deinstallieren. In diesen Fälle können Sie die Paket-GUIDs zur Deinstallation des Produkts verwenden.

Verwenden Sie für Managed Systems den folgenden Befehl:

```
msiexec.exe /x {54C04D53-C3C3-46EA-A75F-7AFF4BEB727C}
```

Durchführen der unbeaufsichtigten Deinstallation der Managed System-Software

Das Dell OpenManage-Installationsprogramm enthält ein Verfahren für eine unbeaufsichtigte Deinstallation. Die unbeaufsichtigte Deinstallation ermöglicht es Ihnen, die Managed System-Software von mehreren Systemen gleichzeitig zu deinstallieren. Das Paket für unbeaufsichtigte Deinstallation wird unter Verwendung eines Softwareverteilungstools von einem unabhängigen Softwareanbieter (ISV) an die Remote-Systeme verteilt. Wenn das Paket verteilt wird, wird das Deinstallationsskript zur Deinstallation der Software ausgeführt.

Verteilen des Pakets zur unbeaufsichtigten Deinstallation

Die DVD *Dell Systems Management Tools and Documentation* ist so vorkonfiguriert, dass sie sich wie das Paket der unbeaufsichtigten Deinstallation verhält. Gehen Sie zur Verteilung des Pakets an ein oder mehrere Systeme folgendermaßen vor:

1. Konfigurieren Sie die Verteilungssoftware des unabhängigen Softwareanbieters so, dass der Befehl `msiexec.exe /x DVD Drive\SYSMGMT\srvadmin\windows\SystemsManagement\ SysMgmt.msi /qb` ausgeführt wird, wenn Sie die DVD verwenden, nachdem das Paket der unbeaufsichtigten Deinstallation verteilt wurde.

2. Verteilen Sie das Paket der unbeaufsichtigten typischen Deinstallation mithilfe der Verteilungssoftware des unabhängigen Softwareanbieters an die Remote-Systeme.

   Das Programm wird ausgeführt und deinstalliert die Managed System-Software auf allen Remote-Systemen.

3. Starten Sie Ihr System neu, damit der Deinstallationsvorgang abgeschlossen werden kann.

Befehlszeileneinstellungen für die unbeaufsichtigte Deinstallation

In Tabelle 5-1 werden Befehlszeileneinstellungen aufgeführt, die für die unbeaufsichtigte Deinstallation verfügbar sind. Die optionalen Einstellungen werden in der Befehlszeile nach `msiexec.exe /x SysMgmt.msi` mit jeweils einem Leerzeichen zwischen den einzelnen Einstellungen eingegeben.

Mit dem Befehl `msiexec.exe /x SysMgmt.msi /qb` wird beispielsweise die unbeaufsichtigte Deinstallation ausgeführt und deren Status wird während der Ausführung angezeigt.

Mit dem Befehl `msiexec.exe /x SysMgmt.msi /qn` wird die unbeaufsichtigte Deinstallation ausgeführt, jedoch im Hintergrund (ohne Anzeigefenster).

Installation der Managed System-Software mithilfe von Bereitstellungssoftware von Drittanbietern

Sie können Software von Drittanbietern wie z. B. Altiris Deployment Solution verwenden, um die Managed System-Software auf unterstützten Dell Systemen zu installieren. Zum Verteilen und Installieren von Server Administrator mit Altiris starten Sie die Altiris-Anwendung und importieren **OpenManage_Jobs.bin** im Verzeichnis **SYSMGMT\srvadmin\support\Altiris** auf der DVD *Dell Systems Management Tools and Documentation*. Geben Sie einen Auftragsordner an, in den **OpenManage_Jobs.bin** importiert werden soll. Sie müssen möglicherweise die Tasks **Skript ausführen** und **Datei kopieren** ändern, so dass diese der Bereitstellungsumgebung entsprechen. Nach der Fertigstellung können Sie den Auftrag so planen, dass er auf unterstützten Dell-Systemen ausgeführt wird, die innerhalb der Altiris Deployment Solution verwaltet werden.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Einführung

Dell™ OpenManage™ Server Administrator Version 6.2- Installationshandbuch

---

Übersicht

Dieses Handbuch enthält Informationen, die Sie bei der Installation von Dell™ OpenManage™ Server Administrator auf verwalteten Systemen unterstützen. Ein *verwaltetes System* ist ein System, auf dem unterstützte Instrumentationsagenten installiert sind, mit denen das System durch Server Administrator ermittelt und nach seinem Status abgefragt werden kann. Server Administrator bietet einfach verwendbare Verwaltung und Administration von lokalen und Remote-Systemen durch ein umfassendes Angebot von integrierten Verwaltungsdiensten. Weitere Informationen über Server Administrator finden Sie unter "Dell OpenManage Server Administrator".

Dieses Dokument enthält außerdem Informationen zum Installieren und Verwenden der **Remote-Aktivierungsfunktion** von Dell OpenManage Server Administrator. Es bietet Informationen zur Verwendung des Dell OpenManage Server Administrator Web Servers zur Verwaltung von Remote-Systemen. Die **Remote-Aktivierungsfunktion** wird derzeit auf den Betriebssystemen Microsoft® Windows®, Microsoft Hyper-V™, Hyper-V Server, Linux, VMware® ESXi und Citrix™ XenServer™ 5.5 unterstützt.

Außerdem bietet dieses Handbuch Informationen und Anleitungen zur Konfiguration Ihrer Systeme vor und während einer Bereitstellung oder einer Aktualisierung. Die folgenden Themen werden in diesem Dokument behandelt:

- Dell OpenManage Security
- Setup und Administration
- Bereitstellungsszenarien für Server Administrator
- Installieren von Managed System-Software auf Microsoft Windows-Betriebssystemen
- Installation von Dell OpenManage Software auf Microsoft Windows Server 2008 Core und Microsoft Hyper-V Server
- Installieren von Managed System Software auf unterstützten Linux-Betriebssystemen
- Dell OpenManage auf VMware ESXi Software
- Verwenden von Microsoft Active Directory
- Voraussetzungsprüfung
- Häufig gestellte Fragen

ANMERKUNG: Wenn Sie Management Station-Software und Managed System-Software auf demselben System installieren, sollten Sie identische Softwareversionen verwenden, um Systemkonflikte zu vermeiden.

Dell OpenManage Systems Management Software

Dell OpenManage Systems Management-Software ist eine Anwendungs-Suite für Dell Systeme. Diese Software ermöglicht Ihnen, Ihre Systeme mit proaktiver Überwachung, Diagnose, Benachrichtigung und im Remote-Zugriff zu verwalten.

Die Dell Systems Management-Software umfasst 3 DVDs:

- DVD *Dell Systems Management Tools and Documentation*
- DVD *Dell Server Updates*
- DVD *Dell Management Console*

DVD Dell Systems Management Tools and Documentation

Hinsichtlich der Verwendung der DVD *Dell Systems Management Tools and Documentation* kann ein System wie folgt klassifiziert werden:

- Verwaltetes System

  Ein verwaltetes System ist ein beliebiges System, das unter Verwendung von Dell OpenManage Server Administrator (ein Systems Management Tools auf der DVD) überwacht und verwaltet wird. Sie können Systeme verwalten, indem Sie Server Administrator lokal oder remote über einen unterstützten Web-Browser ausführen. Für weitere Informationen über Server Administrator, siehe "Dell OpenManage Server Administrator".

- Management Station

  Eine Management Station kann ein beliebiger Computer (Laptop, Desktop oder Server) sein, der verwendet werden kann, um ein verwaltetes System bzw. mehrere verwaltete Systeme im Remote-Zugriff von einer zentralen Stelle aus zu verwalten. Die folgenden Anwendungen umfassen die Dell Management Station-Software, die Sie unter Verwendung der DVD *Dell Systems Management Tools and Documentation* installieren können:

  - Active Directory Snap-In

- BMC Utilities
- DRAC Tools

Informationen zum Installieren dieser Anwendungen finden Sie im *Installationshandbuch zur Dell OpenManage Management Station Software* auf der DVD *Dell Systems Management Tools and Documentation* oder unter **http://support.dell.com/support/edocs/software/omswrels/index.htm**. Dieser Link enthält außerdem Dokumentationen zu Dell OpenManage-Anwendungen.

Die DVD *Dell Systems Management Tools and Documentation* enthält außerdem die folgenden Produkte:

Dell Systems Build and Update Utility

Funktionalität

Sie können das Dell Systems Build and Update Utility für folgende Aufgaben verwenden:

- Aktualisieren der Systemfirmware und Installieren eines Betriebssystems.
- Aktualisieren der Firmware und des BIOS in einer Vorbetriebssystemumgebung auf mehreren Systemen.
- Konfigurieren der Systemhardware.
- Anpassen des Server Update Utility (SUU) und Nutzung des SSU zur Aktualisierung Ihres Systems.

Informationen zur Durchführung dieser Aufgaben und Einzelheiten zum Dell Systems Build and Update Utility finden Sie im *Benutzerhandbuch zum Dell Systems Build and Update Utility* unter **http://support.dell.com/support/edocs/software/omswrels/index.htm**.

Speicherort auf der DVD

<DVD root>

Dell OpenManage Server Administrator

Funktionalität

Dell OpenManage Server Administrator liefert umfassende integrierte Verwaltungslösungen, die für Systemadministratoren und wurde für Systemadministratoren konzipiert, um Systeme auf einem Netzwerk lokal und im Remote-Zugriff zu verwalten. Server Administrator ist die einzige Installation auf dem verwalteten System und ist sowohl lokal als auch im Remote-Zugriff über die Homepage von Server Administrator zugänglich. Auf Systeme, die im Remote-Zugriff überwacht werden, haben Sie über Einwähl-, LAN- oder Wireless-Verbindungen Zugang. Server Administrator gewährleistet die Sicherheit seiner Verwaltungsverbindungen durch rollenbasierte Access Control (RBAC), Authentifizierung sowie Industriestandard-SSL-Verschlüsselung (Standard Secure Socket Layer).

Informationen zum Installieren von Server Administrator finden Sie unter "Installieren von Managed System-Software auf Microsoft Windows-Betriebssystemen" oder "Installieren von Managed System Software auf unterstützten Linux-Betriebssystemen".

Einzelheiten zur Verwendung von Server Administrator finden Sie im *Benutzerhandbuch zum Dell OpenManage Server Administrator* unter **http://support.dell.com/support/edocs/software/omswrels/index.htm**.

Der Speicherverwaltungsdienst bietet erweiterte Funktionen zum Verwalten von lokal verbundenen RAID- und Nicht-RAID-Festplattenspeichern eines Systems.

Der Speicherverwaltungsdienst bietet die folgenden Funktionen:

- Erlaubt die Anzeige des Status der lokalen und der Remote-Speichermedien, die an das überwachte System angeschlossen sind.
- Unterstützt SAS, SCSI, SATA und ATA, jedoch nicht Fibre Channel.
- Das Ausführen von Controller- und Gehäusefunktionen bei allen unterstützten RAID- and Nicht-RAID-Controllern und -Gehäusen von einer einzelnen grafischen oder Befehlszeilenschnittstelle aus und ohne den Einsatz von BIOS-Dienstprogrammen.
- Schützt Daten durch das Konfigurieren von Datenredundanz, das Vergeben von Ersatzgeräten oder das Neu-Erstellen fehlerhafter Laufwerke.

Speicherort auf der DVD

```
<DVD_drive>\SYSMGMT\srvadmin
```

DVD Dell Server Updates

Die DVD *Dell Server Updates* ist Bestandteil des Dell OpenManage Abodienst-Kits zusammen mit der DVD *Dell Systems Management Tools and Documentation*. Die DVD *Dell Server Updates* ist nur für Kunden verfügbar, die den Abodienst abonniert haben.

Die DVD *Dell Server Updates* enthält Dell Update Packages (DUPs) und Dell OpenManage Server Update Utility (SUU). DUPs ermöglichen Administratoren, eine große Auswahl an Systemkomponenten gleichzeitig zu aktualisieren und Scripts auf sich ähnelnde Gruppen von Dell-Systemen anzuwenden, um Systemsoftwarekomponenten auf die gleiche Versionsstufe zu bringen.

SUU ist eine Anwendung, die Aktualisierungen für das System identifiziert und diese auf das System anwendet. Das SUU kann zum Aktualisieren des Dell-Systems oder zum Anzeigen verfügbarer Aktualisierungen für jedes System verwendet werden, welches das SUU unterstützt.

Die DVD *Dell Server Updates* unterstützt Sie beim Installieren, Konfigurieren und Aktualisieren von Programmen und Betriebssystemen. Die DVD enthält auch neuere Versionen von Software für Ihr System.

Für weitere Informationen zu DUPs und SUU, siehe das *Benutzerhandbuch zu den Dell Update Packages* und das *Benutzerhandbuch zum Dell OpenManage Server Update Utility* unter **http://support.dell.com/support/edocs/software/omswrels/index.htm**.

Weitere Informationen zum Abodienst finden Sie unter **www.dell.com/openmanagesubscription**, oder wenden Sie sich an Ihren Verkaufsberater.

DVD Dell Management Console

Die Dell Verwaltungskonsole ist eine webbasierte Systems Management Software, mit der Sie Geräte in Ihrem Netzwerk erkennen und inventarisieren können. Die Software bietet zudem erweiterte Funktionen, z. B. Zustands- und Leistungsüberwachung von vernetzten Geräten und Patch-Verwaltungsfunktionen für Dell-Systeme.

Die DVD *Dell Management Console* ist mit allen Dell-Systemen *xx*0*x* und neueren Systemen verfügbar. Sie können die Dell Verwaltungskonsole auch unter **www.dell.com/openmanage** herunterladen.

Weitere nützliche Dokumente

Zusätzlich zu diesem Handbuch können Sie die folgenden Handbücher entweder auf der Support-Website von Dell unter **http://support.dell.com/support/edocs/software/omswrels/index.htm** oder auf der DVD *Dell Systems Management Tools and Documentation* finden:

- *Das Benutzerhandbuch zum Dell Unified Server Configurator* enthält Informationen zur Verwendung von Unified Server Configurator.
- Das *Benutzerhandbuch zur Dell-Verwaltungskonsole* enthält Informationen zur Installation, Konfiguration und Verwendung der Dell-Verwaltungskonsole. Die Dell Verwaltungskonsole ist eine webbasierte Systems Management-Software, mit der Sie Geräte in Ihrem Netzwerk erkennen und inventarisieren können. Die Software bietet zudem erweiterte Funktionen, wie Zustands- und Leistungsüberwachung von vernetzten Geräten und Patch-Verwaltungsfunktionen für Dell Systeme.
- Das *Benutzerhandbuch zum Dell Systems Build and Update Utility* liefert Informationen zur Verwendung des Systems Build and Update-Dienstprogramms.
- Die *Dell Systems Software Support Matrix* bietet Informationen über verschiedene Dell-Systeme, über die von diesen Systemen unterstützten Betriebssysteme und über die Dell OpenManage-Komponenten, die auf diesen Systemen installiert werden können.
- Das *Benutzerhandbuch zum Dell OpenManage Server Administrator* beschreibt die Installation und den Einsatz von Server Administrator. Server Administrator bietet einfach verwendbare Verwaltung und Administration von lokalen und Remote-Systemen durch ein umfassendes Angebot von integrierten Verwaltungsdiensten.
- Das *Referenzhandbuch zum Dell OpenManage Server Administrator SNMP* enthält die SNMP-Verwaltungsinformationsbasis (MIB). Die SNMP-MIB definiert Variablen, welche die Standard-MIB erweitern, so dass sie Fähigkeiten von Systemverwaltungsagenten einschließen.
- Das *Referenzhandbuch zum Dell OpenManage Server Administrator-CIM* dokumentiert den Anbieter des Allgemeinen Informationsmodells (CIM), der eine Erweiterung der Standard-Verwaltungs-Objektformatdatei (MOF) ist. Dieses Handbuch erklärt die unterstützten Klassen von Verwaltungsobjekten.
- Das *Dell OpenManage Server Administrator-Meldungs-Referenzhandbuch* enthält die Meldungen, die im Meldungsprotokoll auf der Startseite von Server Administrator oder auf der Ereignisanzeige des Betriebssystems angezeigt werden. Das Handbuch erklärt Text, Schweregrad und Ursache jeder Warnmeldung, die vom Server Administrator ausgegeben wird.
- Das *Benutzerhandbuch für die Dell OpenManage Server Administrator-Befehlszeilenschnittstelle* dokumentiert die gesamte Befehlszeilenschnittstelle (CLI) von Server Administrator, einschließlich einer Erklärung der CLI-Befehle zur Ansicht von Systemstatus, Zugriff auf Protokolle, Erstellen von Berichten, Konfigurieren verschiedener Komponentenparameter und Festlegen kritischer Schwellenwerte.
- Das *Benutzerhandbuch zum Dell OpenManage IT Assistant* enthält Informationen zur Installation, Konfiguration und Verwendung von IT Assistant. IT Assistant bietet einen zentralen Zugriffspunkt, um Systeme auf einem lokalen Netzwerk (LAN) oder einem Weitverkehrsnetzwerk (WAN) zu überwachen und verwalten. IT Assistant gibt dem Administrator eine umfassende Ansicht des Unternehmens und kann so die Systembetriebszeit erhöhen, sich wiederholende Aufgaben automatisieren und Unterbrechungen kritischer Geschäftsvorgänge verhindern.
- Das *Dell Remote Access Controller 5-Benutzerhandbuch* enthält vollständige Informationen zur Installation und Konfiguration eines DRAC 5-Controllers und zur Verwendung des DRAC 5 zum Remote-Zugriff auf ein nicht-betriebsfähiges System.
- Das *Benutzerhandbuch zum Integrated Dell Remote Access Controller* enthält vollständige Informationen zur Konfiguration und Verwendung des Integrated Dell Remote Access Controllers zur Remote-Verwaltung und -Überwachung des Systems und seiner freigegebenen Ressourcen über ein Netzwerk.
- Das *Benutzerhandbuch für die Dell Update Packages* enthält Informationen zum Abrufen und Verwenden von Dell Update Packages für Windows und Linux als Teil Ihrer Systemaktualisierungsstrategie.
- Das *Benutzerhandbuch für das Dell OpenManage Server Update Utility* gibt Auskunft über die Verwendung des Dell OpenManage Server Update Utility.
- Das Softwarepaket (DVD) enthält Infodateien für Anwendungen, die sich auf dem Datenträger befinden.

Anfordern von technischer Unterstützung

Wenn Sie eines der in diesem Handbuch beschriebenen Verfahren nicht verstehen oder wenn Ihr Produkt nicht wie erwartet funktioniert, stehen Ihnen verschiedene Hilfsmittel zur Verfügung. Weitere Informationen finden Sie unter "Wie Sie Hilfe bekommen" im *Hardware-Benutzerhandbuch* für das System.

Außerdem sind Dell-Unternehmensschulungen und -Zertifizierungen verfügbar; weitere Informationen finden Sie unter **www.dell.com/training**. Dieser Service wird eventuell nicht überall angeboten.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Verwenden von Microsoft Active Directory

Dell™ OpenManage™ Server Administrator Version 6.2- Installationshandbuch

---

Konrollieren des Zugriffs auf das Netzwerk

Wenn Sie Active Directory®-Dienstsoftware verwenden, können Sie sie so konfigurieren, dass der Zugriff auf Ihr Netzwerk kontrolliert wird. Dell hat die Active Directory-Datenbank so geändert, dass Remote-Verwaltungsauthentifizierung und -genehmigung unterstützt werden. Dell™ OpenManage™ IT Assistant und Dell OpenManage Server Administrator können jetzt ebenso wie iDRAC (Integrated Dell Remote Access Controllers) und DRAC (Dell Remote Access Controllers) über eine Schnittstelle mit Active Directory verbunden werden. Mit diesem Tool können Sie Benutzer und Berechtigungen von einer zentralen Datenbank aus hinzufügen und kontrollieren.

Active Directory-Schemaerweiterungen

Die Active Directory-Daten befinden sich in einer verteilten Datenbank von **Attributen** und **Klassen**. Ein Beispiel für eine Active Directory-**Klasse** ist die **Benutzer**-Klasse. **Attribute** der Benutzerklasse können beispielsweise der Vorname des Benutzers, sein Nachname, die Telefonnummer usw. sein. Alle **Attribute** oder **Klassen**, die einem vorhandenen Active Directory-Schema hinzugefügt werden, müssen mit einer eindeutigen Kennung (ID) definiert werden. Für die Aufrechterhaltung eindeutiger IDs in der gesamten Branche verwaltet Microsoft eine Datenbank von Active Directory-Objektkennzeichnern (OIDs).

Das Active Directory-Schema legt die Regeln dafür fest, welche Daten in die Datenbank aufgenommen werden können. Zur Erweiterung des Schemas im Active Directory erhielt Dell einmalige OIDs, Namenserweiterungen und verbundene Attribut-IDs für die neuen Attribute und Klassen im Verzeichnisdienst.

Die Dell Dateierweiterung lautet: dell

Die Dell Basis-OID lautet: 1.2.840.113556.1.8000.1280

Der Dell LinkID-Bereich lautet: 12070 bis 12079

Die von Microsoft verwaltete Active Directory-OID-Datenbank kann unter **msdn.microsoft.com/certification/ADAcctInfo.asp** durch Eingabe der Erweiterung *dell* eingesehen werden.

Übersicht über die Active Directory-Schemaerweiterungen

Dell hat Klassen oder Gruppen von Objekten erstellt, die vom Benutzer entsprechend ihrer spezifischen Bedürfnisse konfiguriert werden können. Zu den neuen Klassen im Schema gehören eine Zuordnungs-, eine Produkt- und eine Berechtigungsklasse. Ein Zuordnungsobjekt verbindet die Benutzer oder Gruppen mit einer bestimmten Reihe von Berechtigungen und mit Systemen (Produktobjekten) im Netzwerk. Mit diesem Modell erhält ein Administrator Kontrolle über die verschiedenen Kombinationen von Benutzern, Berechtigungen und Systemen oder RAC-Geräten im Netzwerk, ohne dass die Verfahren kompliziert werden.

Active Directory - Objektübersicht

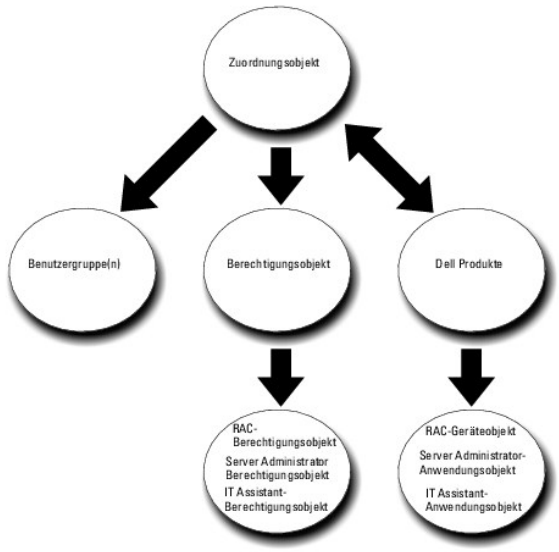
Für jedes System, das Sie zur Authentifizierung und Genehmigung bei Active Directory integrieren möchten, muss es mindestens ein Zuordnungsobjekt und ein Produktobjekt geben. Das Produktobjekt stellt das System dar. Das Zuordnungsobjekt verbindet es mit Benutzern und Berechtigungen. Sie können so viele Zuordnungsobjekte erstellen, wie Sie benötigen.

Jedes Zuordnungsobjekt kann mit so vielen Benutzern, Gruppen von Benutzern und Produktobjekten verbunden werden, wie gewünscht. Die Benutzer und Produktobjekte können von jeder beliebigen Domäne sein. Jedes Zuordnungsobjekt kann jedoch nur mit einem Berechtigungsobjekt verbunden sein. Dieses Verhalten ermöglicht es einem Administrator zu steuern, welche Benutzer über welche Rechte auf bestimmten Systemen verfügen.

Das Produktobjekt verbindet das System mit dem Active Directory für Authentifizierungs- und Genehmigungsabfragen. Wenn ein System zum Netzwerk hinzugefügt wird, muss der Administrator das System und sein Produktobjekt mit seinem Active Directory-Namen konfigurieren, so dass Benutzer Authentifizierung und Genehmigung mit Active Directory ausführen können. Darüber hinaus muss der Administrator das System zu mindestens einem Zuordnungsobjekt hinzufügen, damit sich Benutzer authentifizieren können.

Abbildung 9-1 zeigt, dass das Zuordnungsobjekt die Verbindung bereitstellt, die für die gesamte Authentifizierung und Genehmigung erforderlich ist.

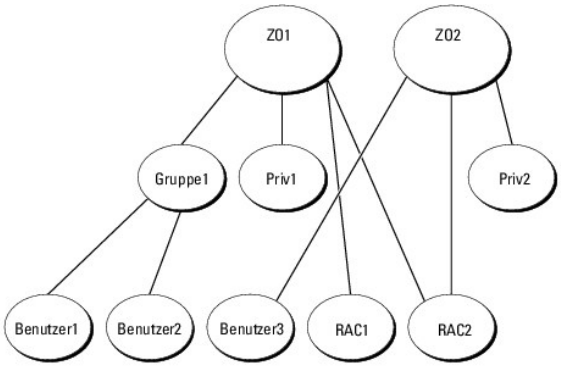
Abbildung 9-1. Typisches Setup für Active Directory-Objekte



Sie können Active Directory-Objekte außerdem in einer einzelnen Domäne oder in mehreren Domänen einrichten. Das Einrichten von Objekten in einer einzelnen Domäne bleibt immer gleich. Es spielt keine Rolle, ob Sie RAC-, Server Administrator- oder IT Assistant-Objekte einrichten. Wenn die Einrichtung jedoch in mehreren Domänen erfolgt, gibt es einige Unterschiede.

Beispiel: Es liegen zwei DRAC 4-Karten (RAC1 und RAC2) und drei existierende Active Directory-Benutzer (Benutzer1, Benutzer2 und Benutzer3) vor. Sie möchten Benutzer1 und Benutzer2 eine Administratorberechtigung auf beiden DRAC 4-Karten geben und Benutzer3 eine Anmeldungsberechtigung auf der RAC2-Karte. Abbildung 9-2 zeigt, wie Sie die Active Directory-Objekte in diesem Szenario einrichten können.

Abbildung 9-2. Einrichten von Active Directory-Objekten in einer einzelnen Domäne



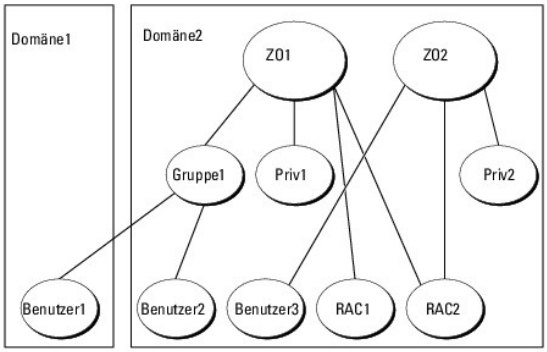
Gehen Sie folgendermaßen vor, um die Objekte für das Szenario mit einer Domäne einzurichten:

1. Erstellen Sie zwei Zuordnungsobjekte.
2. Erstellen Sie zwei RAC-Produktobjekte, RAC1 und RAC2, die die zwei DRAC 4-Karten darstellen sollen.
3. Erstellen Sie zwei Berechtigungsobjekte, Ber1 und Ber2, wobei Ber1 über alle Berechtigungen (Administrator) und Ber2 über Anmeldungsberechtigungen verfügt.
4. Ordnen Sie Benutzer1 und Benutzer2 in Gruppe1 ein.
5. Fügen Sie Gruppe1 als Mitglieder im Zuordnungsobjekt 1 (ZO1), Ber1 als Berechtigungsobjekte in ZO1 sowie RAC1 und RAC2 als RAC-Produkte in ZO1 hinzu.
6. Fügen Sie Benutzer3 als Mitglieder im Zuordnungsobjekt 2 (ZO2), Ber2 als Berechtigungsobjekte in ZO2 und RAC2 als Produkte von RAC in ZO2 hinzu.

Weitere Informationen finden Sie unter "Hinzufügen von Benutzern und Berechtigungen zum Active Directory".

Abbildung 9-3 zeigt, wie Active Directory-Objekte in mehreren Domänen für RAC eingerichtet werden. In diesem Szenario verfügen Sie über zwei DRAC 4-Karten (RAC1 und RAC2) und drei vorhandene Active Directory-Benutzer (Benutzer1, Benutzer2 und Benutzer3). Benutzer1 ist in Domäne1, aber Benutzer2 und Benutzer3 sind in Domäne2. Sie möchten Benutzer1 und Benutzer2 Administratorrechte sowohl auf der RAC1- als auch auf der RAC2-Karte geben und Benutzer3 eine Anmeldungsberechtigung auf der RAC2-Karte.

Abbildung 9-3. Einrichten von Active Directory-Objekten von RAC in mehreren Domänen

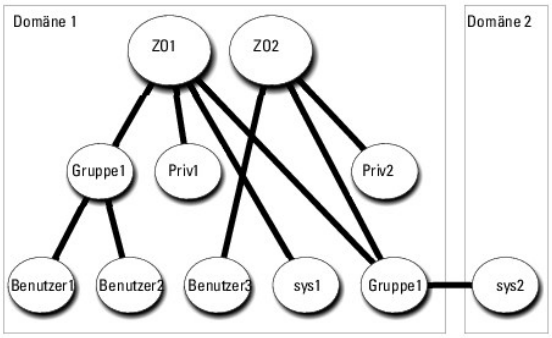


Gehen Sie folgendermaßen vor, um die Objekte für dieses Szenario mit mehreren Domänen einzurichten:

1. Stellen Sie sicher, dass sich die Gesamtstrukturfunktionen der Domäne im systemeigenen oder im Windows 2003-Modus befinden.
2. Erstellen Sie in einer beliebigen Domäne zwei Zuordnungsobjekte, ZO1 (mit der Reichweite Universell) und ZO2. Die Abbildung zeigt die Objekte in Domäne2.
3. Erstellen Sie zwei RAC-Geräteobjekte, RAC1 und RAC2, die die zwei Remote-Systeme darstellen sollen.
4. Erstellen Sie zwei Berechtigungsobjekte, Ber1 und Ber2, wobei Ber1 alle Berechtigungen (Administrator) hat und Ber2 Anmeldungsberechtigungen.
5. Ordnen Sie Benutzer1 und Benutzer2 in Gruppe1 ein. Die Gruppenreichweite von Gruppe1 muss universell sein.
6. Fügen Sie Gruppe1 als Mitglieder im Zuordnungsobjekt 1 (ZO1), Ber1 als Berechtigungsobjekte in ZO1 sowie RAC1 und RAC2 als Produkte in ZO1 hinzu.
7. Fügen Sie Benutzer3 als Mitglieder im Zuordnungsobjekt 2 (ZO2), Ber2 als Berechtigungsobjekte in ZO2 und RAC2 als Produkt in ZO2 hinzu.

Bei Server Administrator oder IT Assistant können die Benutzer andererseits in einer einzelnen Zuordnung in getrennten Domänen sein, ohne dass sie zu einer universellen Gruppe hinzugefügt werden müssen. Im Folgenden wird ein sehr ähnliches Beispiel verwendet, um zu demonstrieren, wie Server Administrator- oder IT Assistant-*Systeme* in getrennten Domänen das Setup von Verzeichnisobjekten beeinflussen. Anstelle der RAC-Geräte liegen zwei Systeme vor, die Server Administrator (Server Administrator-Produkte Sys1 und Sys2) ausführen. Sys1 und Sys2 befinden sich in verschiedenen Domänen. Sie können alle im Active Directory vorhandenen Benutzer oder Gruppen verwenden. Abbildung 9-4 zeigt, wie die Active Directory-Objekte von Server Administrator für dieses Beispiel eingerichtet werden.

Abbildung 9-4. Einrichten von Active Directory-Objekten von Server Administrator in mehreren Domänen



Gehen Sie folgendermaßen vor, um die Objekte für dieses Szenario mit mehreren Domänen einzurichten:

1. Stellen Sie sicher, dass sich die Gesamtstrukturfunktionen der Domäne im systemeigenen oder im Windows 2003-Modus befinden.
2. Erstellen Sie in einer beliebigen Domäne zwei Zuordnungsobjekte, ZO1 und ZO2. Die Abbildung zeigt die Objekte in Domäne1.
3. Erstellen Sie zwei Server Administrator-Produkte, Sys1 und Sys2, die die zwei Systeme darstellen sollen. Sys1 ist in Domäne1 und Sys2 ist in Domäne2.
4. Erstellen Sie zwei Berechtigungsobjekte, Ber1 und Ber2, wobei Ber1 alle Berechtigungen (Administrator) hat und Ber2 Anmeldungsberechtigungen.
5. Ordnen Sie Sys2 in Gruppe1 ein. Die Gruppenreichweite von Gruppe1 muss universell sein.

6. Fügen Sie Benutzer1 und Benutzer2 als Mitglieder im Zuordnungsobjekt 1 (ZO1), Ber1 als Berechtigungsobjekt in ZO1 sowie Sys1 und Gruppe1 als Produkte in ZO1 hinzu.

7. Fügen Sie Benutzer3 als Mitglied im Zuordnungsobjekt 2 (ZO2), Ber2 als Berechtigungsobjekt in ZO2 und Gruppe1 als Produkt in ZO2 hinzu.

Beachten Sie, dass in diesem Fall keines der Zuordnungsobjekte die Reichweite Universell haben muss.

Konfigurieren von Active Directory für den Zugriff auf Ihre Systeme

Bevor Sie Active Directory zum Zugriff auf Ihre Systeme verwenden können, müssen Sie sowohl die Active Directory-Software als auch die Systeme konfigurieren.

1. Erweitern Sie das Active Directory-Schema (siehe "Erweitern des Active Directory-Schemas").

2. Erweitern Sie das Snap-In von Active Directory-Benutzern und - Computern (siehe "Installieren der Dell Erweiterung zum Snap-In von Active Directory-Benutzern und -Computern").

3. Fügen Sie Active Directory Systembenutzer und ihre Berechtigungen hinzu (siehe "Hinzufügen von Benutzern und Berechtigungen zum Active Directory").

4. Aktivieren Sie nur für RAC-Systeme SSL auf jedem Domänen-Controller.

5. Konfigurieren Sie die Active Directory-Eigenschaften des Systems mit der webbasierten Schnittstelle oder der CLI (siehe "Konfigurieren von Systemen oder Geräten").

Konfigurieren des Active Directory-Produktnamens

So konfigurieren Sie den Active Directory-Produktnamen:

1. Suchen Sie die Datei **omsaoem.ini** im Installationsverzeichnis.

2. Bearbeiten Sie die Datei, indem Sie die Zeile "adproductname=text" hinzufügen, wobei Text dem Namen des Produktobjekts entspricht, das Sie im Active Directory erstellt haben.
   Die Datei **omsaoem.ini** enthält z. B. die folgende Syntax, wenn der Active Directory-Produktname auf omsaApp konfiguriert ist.

   ```
   productname=Server Administrator

   startmenu=Dell OpenManage Applications

   autdbid=omsa

   accessmask=3

   adsupport=true

   adproductname=omsaApp
   ```

3. Starten Sie den **DSM SA-Verbindungsdienst** neu, nachdem Sie die Datei **omsaoem.ini** gespeichert haben.

Erweitern des Active Directory-Schemas

RAC-, Server Administrator- und IT Assistant-Schemaerweiterungen sind verfügbar. Sie müssen nur das Schema für Software oder Hardware erweitern, die Sie verwenden. Jede Erweiterung muss individuell angewandt werden, um den Vorteil der softwarespezifischen Einstellungen zu erhalten. Durch Erweitern des Active Directory-Schemas werden Schema-Klassen und -Attribute, Beispielberechtigungen und Zuordnungsobjekte sowie eine organisatorische Einheit für Dell zum Schema hinzugefügt.

ANMERKUNG: Zur Erweiterung des Schemas müssen Sie über **Schema-Admin**-Berechtigungen auf dem Schemamaster FSMO (Flexibler Einzelbetriebsmaster) -Funktionsbesitzer der Domänengesamtstruktur verfügen.

Das Schema kann auf zwei verschiedene Arten erweitert werden. Sie können das Dell Schema Extender-Dienstprogramm oder die LDIF-Scriptdatei (Lightweight Directory Interchange Format) verwenden.

ANMERKUNG: Bei Verwendung der LDIF-Scriptdatei wird die organisatorische Einheit für Dell wird nicht hinzugefügt.

Die LDIF-Scriptdateien und der Dell Schema Extender befinden sich in den folgenden Verzeichnissen der DVD *Dell Systems Management Tools and Documentation*:

- **<DVD-Laufwerk>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\<Installationstyp>\LDIF Files**
- **<DVD-Laufwerk>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_ Tools\<Installationstyp>\Schema Extender**

Tabelle 9-1 listet die Ordnernamen und den <Installationstyp> auf.

Tabelle 9-1. Ordnernamen und Installationstypen

Ordnername	Installationstyp
ITA7	IT Assistant Version 7.0 oder höher
OMSA	Dell OpenManage Server Administrator
Remote_Management	RAC 4, RAC 5, CMC und iDRAC auf modularen *xx*0*x*-Systemen
Remote_Management_Advanced	iDRAC auf *xx*1*x*-Systemen **ANMERKUNG:** Nur iDRAC6 wird auf *xx*1*x* -Systemen unterstützt.

Lesen Sie zur Verwendung der LDIF-Dateien die Anleitungen in der Infodatei im LDIF-Dateiverzeichnis. Gehen Sie zur Verwendung des Dell Schema Extender zur Erweiterung des Active Directory-Schemas wie in "Verwenden des Dell Schema Extender" beschrieben vor.

Sie können den Schema Extender oder die LDIF-Dateien an einem beliebigen Standort kopieren und ausführen.

Verwenden des Dell Schema Extender

VORSICHTSHINWEIS: Der Dell Schema Extender verwendet die Datei SchemaExtenderOem.ini. Damit sichergestellt ist, dass das Dienstprogramm Dell Schema Extender richtig funktioniert, sollten Sie den Namen oder den Inhalt der Datei nicht verändern.

1. Klicken Sie im **Willkommenbildschirm auf Weiter**.
2. Lesen Sie die Warnung und klicken Sie wieder auf **Weiter**.
3. Wählen Sie entweder **Aktuelle Anmeldeinformationen verwenden** oder geben Sie einen Benutzernamen und ein Kennwort mit Schema-Administratorrechten ein.
4. Klicken Sie auf **Weiter**, um den Dell Schema Extender auszuführen.
5. Klicken Sie auf **Fertigstellen**.

   Verweden Sie zum Überprüfen der Schema-Erweiterung das Active Directory Schema-Snap-In in der Microsoft Management Console (MMC), um das Vorhandensein der folgenden Klassen (aufgeführt in Tabelle 9-2, Tabelle 9-5, Tabelle 9-7, Tabelle 9-8, Tabelle 9-9 und Tabelle 9-10) und Attribute (aufgeführt in Tabelle 9-11 und Tabelle 9-12) zu bestätigen. Weitere Informationen zur Aktivierung und Verwendung von Active Directory Schema finden Sie in der Microsoft-Dokumentation.
   Snap-in im MMC.

Weitere Informationen zu Klassendefinitionen für DRAC finden Sie im *Dell Remote Access Controller 4-Benutzerhandbuch* und im *Dell Remote Access Controller 5-Benutzerhandbuch*.

Weitere Informationen zu Klassendefinitionen für iDRAC finden Sie im *Integrated Dell Remote Access Controller-Benutzerhandbuch*.

Tabelle 9-2. Klassendefinitionen für dem Active Directory hinzugefügte Klassen Schema

Klassenname	Zugewiesene Objekt-Identifikationsnummer (OID)	Klassentyp
dellAssociationObject	1.2.840.113556.1.8000.1280.1.1.1.2	Strukturklasse
dellPrivileges	1.2.840.113556.1.8000.1280.1.1.1.4	Strukturklasse
dellProduct	1.2.840.113556.1.8000.1280.1.1.1.5	Strukturklasse
dellOmsa2AuxClass	1.2.840.113556.1.8000.1280.1.2.1.1	Erweiterungsklasse
dellOmsaApplication	1.2.840.113556.1.8000.1280.1.2.1.2	Strukturklasse
dellIta7AuxClass	1.2.840.113556.1.8000.1280.1.3.1.1	Erweiterungsklasse
dellItaApplication	1.2.840.113556.1.8000.1280.1.3.1.2	Strukturklasse

Tabelle 9-3. dellAssociationObject Class

OID	1.2.840.113556.1.8000.1280.1.1.1.2
Beschreibung	Diese Klasse stellt das Dell Zuordnungsobjekt dar. Das Zuordnungsobjekt stellt die Verbindung zwischen den Benutzern und den Geräten oder Produkten bereit.
Klassentyp	Strukturklasse
SuperClasses	Gruppe
Attribute	dellProductMembers dellPrivilegeMember

Tabelle 9-4. dellPrivileges Class

OID	**1.2.840.113556.1.8000.1280.1.1.1.4**
Beschreibung	Diese Klasse wird als Container-Klasse für die Berechtigungen von Dell (Genehmigungsrechte) verwendet.
Klassentyp	Strukturklasse
SuperClasses	Benutzer
Attribute	dellRAC4Privileges dellRAC3Privileges dellOmsaAuxClass dellItaAuxClass

Tabelle 9-5. dellProduct Class

OID	**1.2.840.113556.1.8000.1280.1.1.1.5**
Beschreibung	Das ist die Hauptklasse, aus der alle Produkte von Dell abgeleitet werden.
Klassentyp	Strukturklasse
SuperClasses	Computer
Attribute	dellAssociationMembers

Tabelle 9-6. dellOmsa2AuxClass Class

OID	**1.2.840.113556.1.8000.1280.1.2.1.1**
Beschreibung	Diese Klasse wird verwendet, um die Berechtigungen (Genehmigungsrechte) für den Server Administrator zu definieren.
Klassentyp	Erweiterungsklasse
SuperClasses	Keine
Attribute	dellOmsaIsReadOnlyUser dellOmsaIsReadWriteUser dellOmsaIsAdminUser

Tabelle 9-7. dellOmsaApplication Class

OID	**1.2.840.113556.1.8000.1280.1.2.1.2**
Beschreibung	Diese Klasse stellt die Server Administrator-Anwendung dar. Server Administrator muss als dellOmsaApplication im Active Directory konfiguriert werden. Diese Konfiguration ermöglicht es der Server Administrator-Anwendung, LDAP-Abfragen zum Active Directory zu senden.
Klassentyp	Strukturklasse
SuperClasses	dellProduct
Attribute	dellAssociationMembers

Tabelle 9-8. dellIta7AuxClass Class

OID	**1.2.840.113556.1.8000.1280.1.3.1.1**
Beschreibung	Diese Klasse wird verwendet, um die Berechtigungen (Genehmigungsrechte) für den IT Assistant zu definieren.
Klassentyp	Erweiterungsklasse
SuperClasses	Keine
Attribute	dellItaIsReadOnlyUser dellItaIsReadWriteUser dellItaIsAdminUser

Tabelle 9-9. dellItaApplication Class

OID	**1.2.840.113556.1.8000.1280.1.3.1.2**
Beschreibung	Diese Klasse stellt die IT Assistant-Anwendung dar. IT Assistant muss als dellItaApplication im Active Directory konfiguriert werden. Diese Konfiguration ermöglicht es IT Assistant, LDAP-Protokollabfragen zum Active Directory zu senden.
Klassentyp	Strukturklasse
SuperClasses	dellProduct
Attribute	dellAssociationMembers

Tabelle 9-10. Allgemeine zum Active Directory-Schema hinzugefügte Attribute

Attributname/Beschreibung	**Zugewiesener OID/Syntax-**	**Einzelbewertung**

	Objektkennzeichner	
dellPrivilegeMember Die Liste von dellPrivilege-Objekten, die zu diesem Attribut gehören.	1.2.840.113556.1.8000.1280.1.1.2.1 Eindeutiger Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellProductMembers Die Liste von dellRacDevices-Objekten, die zu dieser Funktion gehören. Dieses Attribut ist die Vorwärtsverbindung zur dellAssociationMembers-Rückwärtsverbindung. Link-ID: 12070	1.2.840.113556.1.8000.1280.1.1.2.2 Eindeutiger Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellAssociationMembers Liste der dellAssociationObjectMembers, die zu diesem Produkt gehören. Dieses Attribut ist die Rückwärtsverbindung zum Attribut dellProductMembers. Link-ID: 12071	1.2.840.113556.1.8000.1280.1.1.2.14 Eindeutiger Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE

Tabelle 9-11. Zum Active Directory-Schema hinzugefügte Server Administrator-spezifische Attribute Verzeichnisschema

Attributname/Beschreibung	Zugewiesener OID/Syntax-Objektkennzeichner	Einzelbewertung
dellOmsaIsReadOnlyUser TRUE, wenn der Benutzer Nur-Lesen-Rechte in Server Administrator hat	1.2.840.113556.1.8000.1280.1.2.2.1 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellOmsaIsReadWriteUser TRUE, wenn der Benutzer Lese-Schreib-Rechte in Server Administrator hat	1.2.840.113556.1.8000.1280.1.2.2.2 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellOmsaIsAdminUser TRUE, wenn der Benutzer Administratorrechte in Server Administrator hat	1.2.840.113556.1.8000.1280.1.2.2.3 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE

Tabelle 9-12. IT Assistant-spezifische zum Active Directory-Schema hinzugefügte Attribute Verzeichnisschema

Attributname/Beschreibung	Zugewiesener OID/Syntax-Objektkennzeichner	Einzelbewertung
dellItaIsReadWriteUser TRUE, wenn der Benutzer Lesen-Schreiben-Rechte in IT Assistant hat	1.2.840.113556.1.8000.1280.1.3.2.1 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellItaIsAdminUser TRUE, wenn der Benutzer Administratorrechte in IT Assistant hat	1.2.840.113556.1.8000.1280.1.3.2.2 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellItaIsReadOnlyUser TRUE, wenn der Benutzer Nur-Lesen-Rechte in IT Assistant hat	1.2.840.113556.1.8000.1280.1.3.2.3 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE

Active Directory-Benutzer und Computer Snap-In

Installieren der Dell Erweiterung zum Snap-In von Active Directory-Benutzern und - Computern

Wenn Sie das Active Directory-Schema erweitern, müssen Sie auch das Snap-In von Active Directory-Benutzern und -Computern erweitern, damit der Administrator Produkte, Benutzer und Benutzergruppen, Zuordnungen sowie Berechtigungen verwalten kann. Sie brauchen das Snap-In nur einmal zu erweitern, selbst dann, wenn Sie mehrere Schema-Erweiterungen hinzugefügt haben. Sie müssen das Snap-in auf jedem System installieren, das Sie zur Verwaltung dieser Objekte verwenden möchten.

Wenn Sie die Systemverwaltungssoftware mit der DVD *Dell Systems Management Tools and Documentation* installieren, können Sie das Snap-In installieren, indem Sie während des Installationsverfahrens die Option **Active Directory Snap-In** auswählen.

Für 64-Bit-Windows-Betriebssysteme befindet sich das Snap-In-Installationsprogramm unter `<DVD-Laufwerk>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_SnapIn64`.

ANMERKUNG: Sie müssen das Administrator Pack auf jeder Management Station installieren, die die neuen Active Directory-Objekte verwaltet. Die Installation wird im folgenden Abschnitt ("Öffnen des Snap-In von Active Directory-Benutzern und Computern") beschrieben. Wenn Sie das Administrator Pack nicht installieren, können Sie das neue Objekt nicht im Container anzeigen.

ANMERKUNG: Weitere Informationen zum Snap-In von Active Directory-Benutzern und -Computern finden Sie in der Microsoft -Dokumentation.

Öffnen des Snap-In von Active Directory-Benutzern und Computern

ANMERKUNG: Auf Windows 2000 Server können Sie das Schema erweitern, die Dell-Erweiterung jedoch nicht im Snap-In installieren.

Gehen Sie folgendermaßen vor, um das erweiterte Schema auf den unter Windows 2000 laufenden Domain Controllern zu verwalten:

Herstellen einer Verbindung zu einem Windows 2000 Server Domain Controller über einen anderen Domain Controller

1. Klicken Sie auf **Start**→ **Verwaltung**→ **Active Directory Benutzer und Computer**.
2. Klicken Sie im linken Fenster auf **Active Directory Benutzer und Computer**.
3. Klicken Sie auf **Mit Domain Controller verbinden**, um die Verbindung zu einem anderen Domain Controller herzustellen.
4. Geben Sie den Namen des Windows 2000 Domain Controller ein.

Herstellen einer Verbindung zu einem Windows 2000 Server Domain Controller über ein lokales System

1. Auf dem lokalen System muss das entsprechende Microsoft Administratorpaket installiert sein.
2. Klicken Sie zur Installation dieses Administratorpakets auf **Start**→ **Ausführen**, geben Sie **MMC** ein und drücken Sie die <Eingabetaste>.

   Das **Microsoft Management Console (MMC)**-Fenster wird angezeigt.
3. Klicken Sie auf **Datei**.
4. Klicken Sie auf **Snap-In hinzufügen/entfernen**.
5. Klicken Sie auf **Hinzufügen**.
6. Wählen Sie **Active Directory-Benutzer- und Computer-Snap-In** aus und klicken Sie auf **Hinzufügen**.
7. Klicken Sie auf **Schließen** und anschließend auf **OK**.

Hiermit wird eine Verbindung zum aktuellen Domain Controller hergestellt. Wenn es sich hierbei nicht um den Windows 2000 Domain Controller handelt, fahren Sie mit den Schritten unter "Herstellen einer Verbindung zu einem Windows 2000 Server Domain Controller über einen anderen Domain Controller**"** fort.

Gehen Sie zum Öffnen des Snap-In von Active Directory-Benutzern und -Computern folgendermaßen vor:

1. Wenn Sie sich auf dem Domain Controller befinden, klicken Sie auf **Start**→ **Admin-Hilfsprogramme**→ **Active Directory Benutzer und Computer**. Wenn Sie sich nicht auf dem Domänen-Controller befinden, muss das entsprechende Microsoft-Administrator Pack auf Ihrem lokalen System installiert sein. Klicken Sie zur Installation dieses Administratorpakets auf **Start**→ **Ausführen**, geben Sie MMC und drücken Sie die **Eingabetaste**.

   Das Fenster Microsoft Management Console (MMC) wird geöffnet.
2. Klicken Sie auf **Datei** im **Konsole 1**-Fenster.
3. Klicken Sie auf **Snap-In hinzufügen/entfernen**.
4. Klicken Sie auf **Hinzufügen**.
5. Wählen Sie das Snap-In von **Active Directory-Benutzern und -Computern** und klicken Sie auf **Hinzufügen**.
6. Klicken Sie auf **Schließen** und anschließend auf **OK**.

Hinzufügen von Benutzern und Berechtigungen zum Active Directory

Das Dell-erweiterte Active Directory-Benutzer und -Computer-Snap-In ermöglicht das Hinzufügen von DRAC-, Server Administrator- und IT Assistant-Benutzer und -Berechtigungen durch Erstellen von RAC-, Zuordnungs- und Berechtigungsobjekten. Gehen Sie zum Hinzufügen eines Objekts wie im entsprechenden Unterabschnitt beschrieben vor.

Produktobjekt erstellen

ANMERKUNG: Server Administrator- und IT Assistant-Benutzer müssen Produktgruppen des Typs Universell verwenden, um Domänen mit ihren Produktobjekten zu umfassen.

ANMERKUNG: Wenn Sie typische universelle Produktgruppen von einzelnen Domänen hinzufügen, müssen Sie ein Zuordnungsobjekt mit universeller Reichweite erstellen. Die mit dem Dell Schema Extender-Dienstprogramm erstellten Standard-Zuordnungsobjekte sind lokale Domänengruppen, die nicht mit typischen universellen Produktgruppen anderer Domänen funktionieren.

Klicken Sie im Fenster **Console Root** (MMC) mit der rechten Maustaste auf einen Container.

1. Wählen Sie **Neu**.
2. Wählen Sie entweder ein RAC-, ein Server Administrator- oder ein IT Assistant-Objekt aus, je nachdem, welches Sie installiert haben.

   Das Fenster **Neues Objekt** wird geöffnet.
3. Geben Sie einen Namen für das neue Objekt ein. Dieser Name muss mit dem **Active Directory-Produktnamen** übereinstimmen (siehe "Konfigurieren von Active Directory mit CLI auf Systemen die Server Administrator ausführen".
4. Wählen Sie das entsprechende **Produktobjekt**.
5. Klicken Sie auf **OK**.

Erstellen von Berechtigungsobjekten

Berechtigungsobjekte müssen in derselben Domäne wie das Zuordnungsobjekt, dem sie zugeordnet werden, erstellt werden.

1. Klicken Sie im Fenster **Console Root** (MMC) mit der rechten Maustaste auf einen Container.
2. Wählen Sie **Neu**.
3. Wählen Sie entweder ein RAC-, ein Server Administrator- oder ein IT Assistant-Objekt aus, je nachdem, welches Sie installiert haben.

   Das Fenster **Neues Objekt** wird geöffnet.
4. Geben Sie einen Namen für das neue Objekt ein.
5. Wählen Sie das entsprechende **Berechtigungsobjekt**.
6. Klicken Sie auf **OK**.
7. Klicken Sie mit der rechten Maustaste auf das Berechtigungsobjekt, das Sie erstellt haben, und wählen Sie **Eigenschaften**.
8. Klicken Sie auf die entsprechende Registerkarte **Berechtigungen** und wählen Sie die Berechtigungen aus, die der Benutzer haben soll (weitere Informationen finden Sie unter Tabelle 9-2 und Tabelle 9-8).

Erstellen von Zuordnungsobjekten

Das Zuordnungsobjekt wird von einer Gruppe abgeleitet und muss einen Gruppentyp enthalten. Die Zuordnungsreichweite legt den Sicherheitsgruppentyp für das Zuordnungsobjekt fest. Wenn Sie ein Zuordnungsobjekt erstellen, müssen Sie die Zuordnungsreichweite wählen, die für den Typ von Objekten gilt, welche Sie hinzufügen möchten. Die Auswahl von **Universell** bedeutet beispielsweise, dass die Zuordnungsobjekte nur zur Verfügung stehen, wenn die Active Directory-Domäne im Einheitlichen Modus oder darüber funktioniert.

1. Klicken Sie im Fenster **Console Root** (MMC) mit der rechten Maustaste auf einen Container.
2. Wählen Sie **Neu**.
3. Wählen Sie entweder ein RAC-, ein Server Administrator- oder ein IT Assistant-Objekt aus, je nachdem, welches Sie installiert haben.

   Das Fenster **Neues Objekt** wird geöffnet.
4. Geben Sie einen Namen für das neue Objekt ein.
5. Wählen Sie **Zuordnungsobjekt**.
6. Wählen Sie die Reichweite für das **Zuordnungsobjekt**.
7. Klicken Sie auf **OK**.

Hinzufügen von Objekten zu einem Zuordnungsobjekt

Mit dem Fenster **Zuordnungsobjekt-Eigenschaften** können Sie Benutzer oder Benutzergruppen, Berechtigungsobjekte, Systeme, RAC-Geräte sowie System- oder Gerätegruppen zuordnen.

ANMERKUNG: RAC-Benutzer müssen Universelle Gruppen verwenden, um Domänen mit ihren Benutzern oder RAC-Objekten zu umfassen.

Sie können Gruppen von Benutzern und Produkten hinzufügen. Sie können Dell-spezifische Gruppen auf die gleiche Art und Weise erstellen wie andere Gruppen.

So fügen Sie Benutzer oder Benutzergruppen hinzu:

1. Klicken Sie mit der rechten Maustaste auf das **Zuordnungsobjekt** und wählen Sie **Eigenschaften**.
2. Wählen Sie die Registerkarte **Benutzer** und klicken Sie auf **Hinzufügen**.
3. Geben Sie den Benutzer- oder Benutzergruppennamen ein oder durchsuchen Sie die vorhandenen Namen, um einen auszuwählen, und klicken Sie auf **OK**.

Klicken Sie auf die Registerkarte **Berechtigungsobjekt**, um das Berechtigungsobjekt der Zuordnung hinzuzufügen, die die Berechtigungen der Benutzer oder Benutzergruppe bei Authentifizierung eines Systems definiert.

ANMERKUNG: Sie können einem Zuordnungsobjekt nur ein Berechtigungsobjekt hinzufügen.

So fügen Sie eine Berechtigung hinzu:

1. Wählen Sie die Registerkarte **Berechtigungsobjekt** und klicken Sie auf **Hinzufügen**.
2. Geben Sie den Berechtigungsobjekt-Namen ein oder suchen Sie nach einem Namen und klicken Sie auf **OK**.

Klicken Sie auf die Registerkarte **Produkte**, um der Zuordnung ein oder mehrere Systeme oder Geräte hinzuzufügen. Die zugeordneten Objekte legen die mit dem Netzwerk verbundenen Produkte fest, die für die definierten Benutzer- oder Benutzergruppen verfügbar sind.

ANMERKUNG: Sie können einem Zuordnungsobjekt mehrere Systeme oder RAC-Geräte hinzufügen.

So fügen Sie Produkte hinzu:

1. Wählen Sie die Registerkarte **Produkte** und klicken Sie auf **Hinzufügen**.
2. Geben Sie den System-, Geräte- oder Gruppennamen ein und klicken Sie auf **OK**.
3. Klicken Sie im Fenster **Eigenschaften** auf **Anwenden** und anschließend auf **OK**.

Konfigurieren von Systemen oder Geräten

Anleitungen zur Konfiguration von Server Administrator- oder IT Assistant-Systemen mit CLI-Befehlen finden Sie unter "Konfigurieren von Active Directory mit CLI auf Systemen die Server Administrator ausführen.". Für DRAC-Benutzer bietet das *Dell Remote Access Controller 4-Benutzerhandbuch* oder das *Dell Remote Access Controller 5-Benutzerhandbuch* weitere Informationen. Für iDRAC-Benutzer bietet das *Integrated Dell Remote Access Controller-Benutzerhandbuch* weitere Informationen.

ANMERKUNG: Die Systeme, auf denen Server Administrator und/oder IT Assistant installiert sind, müssen ein Teil der Active Directory-Domäne sein und sollten außerdem über Computerkonten auf der Domäne verfügen.

Konfigurieren von Active Directory mit CLI auf Systemen die Server Administrator ausführen.

Sie können den Befehl **omconfig preferences dirservice** zur Konfiguration des Active Directory-Dienstes verwenden. Die Datei ***product*oem.ini** wurde geändert, um diese Änderungen widerzuspiegeln. Wenn **adproductname** nicht in der Datei ***product*oem.ini** vorhanden ist, wird ein Standardname zugewiesen. Der Standardwert lautet ***Systemname-Software-Produktname***, wobei ***Systemname*** dem Namen des Systems entspricht, auf dem Server Administrator ausgeführt wird, und ***Software-Produktname*** sich auf den Namen des in der Datei **omprv32.ini (als *Computername*-omsa)** definierten Softwareprodukts bezieht.

ANMERKUNG: Dieser Befehl steht nur auf Systemen zur Verfügung, die unter einem Windows-Betriebssystem laufen.

ANMERKUNG: Starten Sie den Server Administrator-Dienst nach der Konfiguration des Active Directory neu.

Tabelle 9-13 zeigt die gültigen Parameter für den Befehl.

Tabelle 9-13. Konfigurationsparameter des Active Directory-Dienstes

Name=Wert-Paar	Beschreibung
prodname=<Text>	Gibt das Softwareprodukt an, für das die Active Directory-Konfigurationsänderungen gelten sollen. *Prodname* bezieht sich auf den Namen des in der Datei **omprv32.ini** definierten Produkts. Für Server Administrator ist dies *omsa*.
enable=<true |	**true:** Aktiviert den Authentifizierungs-Support des Active Directory-Diensts.

false>	**false**: Deaktiviert den Authentifizierungs-Support des Active Directory-Diensts.
adprodname=<text>	Gibt den Namen des Produkts an, wie es im Active Directory-Service definiert ist. Dieser Name verbindet das Produkt mit den Active Directory-Berechtigungsdaten für die Benutzer-Authentifizierung.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Voraussetzungsprüfung

Dell™ OpenManage™ Server Administrator Version 6.2- Installationshandbuch

---

Befehlszeilenbetrieb der Voraussetzungsprüfung

Sie können die Voraussetzungsprüfung im Hintergrund ausführen, indem Sie runprereqchecks.exe /s vom Verzeichnis **SYSMGMT\srvadmin\windows\PreReqChecker** auf der DVD *Dell Systems Management Tools and Documentation* ausführen**.** Nach Ausführung der Voraussetzungsprüfung wird eine HTML-Datei (**omprereq.htm**) im Verzeichnis **%Temp%** erstellt. Diese Datei enthält die Ergebnisse der Voraussetzungsprüfung. Das Verzeichnis **Temp** ist normalerweise nicht **X:\Temp**, sondern **X:\Dokumente und Einstellungen\Benutzername\Lokale Einstellungen\Temp.** Um **%TEMP%** zu finden, wechseln Sie zu einer Eingabeaufforderung und geben Sie echo %TEMP% ein.

Ergebnisse für ein Managed System stehen unter dem folgenden Schlüssel:

HKEY_LOCAL_MACHINE\Software\Dell Computer Corporation\OpenManage\PreReqChecks\MN

Bei Ausführung der Voraussetzungsprüfung im Hintergrundmodus ist der Rückgabecode von **runprereqchecks.exe** die Zahl, die mit dem höchsten Schweregradzustand aller Softwareprodukte verknüpft ist. Die Zahlen des Rückgabecodes sind die gleichen wie jene, die in der Registrierung verwendet werden. Tabelle 10-1 zeigt die Codes, die zurückgegeben werden.

Tabelle 10-1. Rückgabecodes der im Hintergrund ausgeführten Voraussetzungsprüfung

Rückgabecode	Beschreibung
0	Keine Zustände sind mit der Software verbunden.
1	Informationszustände sind mit der Software verbunden. Dies verhindert die Installation des Softwareprodukts nicht.
2	Warnungszustände sind mit der Software verbunden. Es wird empfohlen, dass Sie die Zustände beheben, die die Warnung verursachen, bevor Sie mit der Installation der Software fortfahren.
3	Fehlerzustände sind mit der Software verbunden. Es ist notwendig, die Zustände zu beheben, die den Fehler verursachen, bevor Sie mit der Installation dieser Software fortfahren. Wenn die Fehler nicht behoben werden, wird die Software nicht installiert.
-1	Ein Microsoft® Windows® Script Host (WSH)-Fehler. Die Voraussetzungsprüfung wird nicht ausgeführt.
-2	Das Betriebssystem wird nicht unterstützt. Die Voraussetzungsprüfung wird nicht ausgeführt.
-3	Der Benutzer hat keine Administratorrechte. Die Voraussetzungsprüfung wird nicht ausgeführt.
-4	Kein durchgeführter Rückgabecode.
-5	Der Benutzer konnte das Arbeitsverzeichnis nicht zu **%TEMP%** ändern. Die Voraussetzungsprüfung wird nicht ausgeführt.
-6	Das Zielverzeichnis existiert nicht. Die Voraussetzungsprüfung wird nicht ausgeführt.
-7	Ein interner Fehler ist aufgetreten. Die Voraussetzungsprüfung wird nicht ausgeführt.
-8	Die Software wird bereits ausgeführt. Die Voraussetzungsprüfung wird nicht ausgeführt.
-9	Der Windows Script Host ist beschädigt, weist eine falsche Version auf oder ist nicht installiert. Die Voraussetzungsprüfung wird nicht ausgeführt.
-10	Bei der Scripting-Umgebung ist ein Fehler aufgetreten. Die Voraussetzungsprüfung wird nicht ausgeführt.

Jedem Softwareprodukt wird nach der Voraussetzungsprüfung ein Wertsatz zugewiesen. Tabelle 10-2 stellt die Liste der Funktions-IDs für jede Softwarefunktion bereit. Die Funktionskennung besteht aus einer 2 bis 5 Zeichen langen Bezeichnung.

ANMERKUNG: Die in Tabelle 10-2 erwähnten Softwarefunktions-IDs unterscheiden zwischen Groß- und Kleinschreibung.

Tabelle 10-2. Software Funktions-IDs für Managed Systems Software

Funktions-ID	Beschreibung
ALLE	Alle Funktionen
BRCM	Broadcom NIC-Agent
INTEL	Intel® NIC-Agent
IWS	Dell OpenManage Server Administrator Web Server
OMSM	Server Administrator Storage Management Service
RAC4	Remote Access Controller (DRAC 4)
RAC5	Dell Remote Access Controller (DRAC 5)
iDRAC	Integrierter Dell Remote Access Controller
SA	Server Administrator
RmtMgmt	Remoteaktivierung

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Dell OpenManage Security

Dell™ OpenManage™ Server Administrator Version 6.2- Installationshandbuch

---

Sicherheitsfunktionen

Die Dell™ OpenManage™ Systems Management-Softwarekomponenten bieten die folgenden Sicherheitsfunktionen:

- Authentifizierung für Benutzer durch die auf der Hardware gespeicherten Benutzer-IDs und Kennwörter oder durch Verwendung des optionalen Microsoft® Active Directory®.
- Support für Netzwerk-Informationsdienste (NIS), Winbind, Kerberos und das Lightweight Directory Access Protocol (LDAP) sind Authentifizierungsprotokolle für Linux-Betriebssysteme.
- Funktionsbasierte Befugnis, die es ermöglicht, bestimmte Berechtigungen für die einzelnen Benutzer zu konfigurieren.
- Konfiguration von Benutzer-ID und Kennwort in den meisten Fällen über die webbasierte Schnittstelle oder die Befehlszeilenschnittstelle (CLI).
- SSL-Verschlüsselung von 128 Bit und 40 Bit (für Länder, in denen 128 Bit nicht unterstützt wird).

  ANMERKUNG: Telnet unterstützt keine SSL-Verschlüsselung.

- Konfiguration der Sitzungszeitüberschreitung (in Minuten) über die webbasierte Schnittstelle oder die Befehlszeilenschnittstelle (CLI).
- Schnittstellenkonfiguration – Korrekt konfigurierte Schnittstellen sind notwendig, damit die Dell OpenManage Systems Management-Software durch Firewalls eine Verbindung zu einem Remote-Gerät herstellen kann.

  ANMERKUNG: Für Informationen zu Schnittstellen, die verschiedene Dell OpenManage Systems Management-Komponenten verwenden, siehe das Benutzerhandbuch zur entsprechenden Komponente.

Sicherheitsverwaltung

Dell bietet Sicherheits- und Zugriffsverwaltung über die rollenbasierte Zugriffskontrolle (RBAC), Authentifizierung und Verschlüsselung oder über Active Directory (oder über Winbind, Kerberos, LDAP oder NIS auf Linux-Betriebssystemen) für die webbasierte und die Befehlszeilenoberfläche.

RBAC

RBAC erreicht Sicherheit durch Festlegung der Vorgänge, die von Benutzern in besonderen Funktionen ausgeführt werden können. Jedem Benutzer werden eine oder mehrere Funktionen zugeteilt, und jeder Funktion sind eine oder mehrere Benutzerberechtigungen zugewiesen, die für Benutzer in dieser Funktion zugelassen sind. Mit RBAC kann die Sicherheitsverwaltung der Organisationsstruktur genau entsprechen. Informationen über das Einrichten von Benutzern finden Sie in der Betriebssystemdokumentation.

Benutzerberechtigungen

Server Administrator gewährt unterschiedliche Zugriffsrechte basierend auf den dem Benutzer zugewiesenen Gruppenberechtigungen. Die drei Benutzerebenen sind *Benutzer*, *Hauptbenutzer* und *Administrator*.

Benutzer können die meisten Informationen anzeigen.

Hauptbenutzer können Warnungsgrenzwerte einstellen und konfigurieren, welche Warnungsmaßnahmen ausgeführt werden sollen, wenn ein Warnungs- oder Fehlerereignis eintritt.

Administratoren können Maßnahmen zum Herunterfahren konfigurieren und durchführen, automatische Wiederherstellungsmaßnahmen konfigurieren, falls ein Betriebssystem auf einem System nicht mehr reagiert, und Hardware-, Ereignis- und Befehlsprotokolle löschen. Administratoren können Warnungsmaßnahmen konfigurieren, einschließlich das Senden von E-Mails, wenn eine Warnung generiert wurde.

Server Administrator erteilt Nur-Lesen-Zugriff an Benutzer, die mit normalen Benutzerberechtigungen angemeldet sind, Lese- und Schreibzugriff an Benutzer mit Hauptbenutzerberechtigungen und Lese-, Schreib- und Administrator-Zugriffsrechte an Benutzer, die mit Administratorrechten angemeldet sind. Siehe Tabelle 2-1.

Tabelle 2-1. Benutzerberechtigungen

Benutzerberechtigungen	Zugriffstyp		
	Admin	Schreiben	Lesen
Benutzer			X

Hauptbenutzer		X	X
Administrator	X	X	X

Admin-Zugriff erlaubt Ihnen, das Managed System herunterzufahren.

Schreibzugriff erlaubt Ihnen, die Werte auf dem Managed System zu modifizieren oder einzustellen.

Lesezugriff erlaubt Ihnen, die vom Server Administrator gemeldeten Daten anzuzeigen. Lesezugriff lässt keine Änderung oder Einstellung von Werten auf dem Managed System zu.

Berechtigungsebenen für den Zugriff auf Server Administrator-Dienste

In Tabelle 2-2 wird zusammengefasst, welche Benutzerebenen die Berechtigung zum Zugriff auf die Server Administrator-Dienste sowie deren Verwaltung besitzen.

Tabelle 2-2. Server Administrator-Benutzerberechtigungsebenen

Service	**Erforderliche Benutzerberechtigungsebene**	
	Ansicht	**Verwaltung**
Instrumentation	B, H, A	H, A
Remotezugriff	B, H, A	A
Aktualisierung	B, H, A	A
Storage Management	B, H, A	A

Tabelle 2-3 definiert die Abkürzungen der Benutzerberechtigungsebenen, die in Tabelle 2-2 verwendet werden.

Tabelle 2-3. Legende der Server Administrator-Benutzerberechtigungsebenen

U	Benutzer
P	Hauptbenutzer
A	Administrator

Authentifizierung

Das Server Administrator-Authentifizierungsschema stellt sicher, dass die Zugriffstypen den korrekten Benutzerberechtigungen zugewiesen werden. Wenn die CLI aufgerufen wird, validiert das Server Administrator-Authentifizierungsschema außerdem den Kontext, in dem das aktuelle Verfahren ausgeführt wird. Dieses Authentifizierungsschema stellt sicher, dass alle Server Administrator-Funktionen unabhängig davon korrekt authentifiziert werden, ob sie über die Startseite des Server Administrators oder über die CLI aufgerufen werden.

Microsoft Windows Authentifizierung

Für unterstützte Windows®-Betriebssysteme verwendet die Server Administrator-Authentifizierung zum Authentifizieren Integrated Windows Authentication (früher bekannt als NTLM). Dieses Authentifizierungssystem ermöglicht die Integration der Server Administrator-Sicherheit in ein Gesamtsicherheitsschema für Ihr Netzwerk.

Red Hat® Enterprise Linux- und SUSE® Linux Enterprise Server-Authentifizierung

Bei unterstützten Red Hat® Enterprise Linux®- und SUSE® Linux Enterprise Server-Betriebssystemen basiert die Server Administrator-Authentifizierung auf der Bibliothek der Pluggable Authentication Modules (PAM). Mit dieser dokumentierten Funktionsbibliothek kann ein Administrator feststellen, wie einzelne Anwendungen die Benutzer authentifizieren.

Verschlüsselung

Zugriff auf Server Administrator erfolgt über eine sichere HTTPS-Verbindung mittels Secure Socket Layer-Technologie (SSL) zur Sicherung und zum Schutz der Identität des verwalteten Systems. Java Secure Socket Extension (JSSE) wird von unterstützten Windows-, Red Hat Enterprise Linux- und SUSE Linux Enterprise Server-Betriebssystemen zum Schutz der über die Socket-Verbindung übertragenen Benutzeranmeldeinformationen und anderer sensibler Daten verwendet, wenn ein Benutzer auf Server Administrator zugreift.

Microsoft Active Directory

Die Active Directory Service-Software (ADS) fungiert als zentrale Autorität für die Netzwerksicherheit. ADS erlaubt dem Betriebssystem, eine Benutzeridentität zu überprüfen und den Zugriff dieses Benutzers auf Netzwerkressourcen zu steuern. Für Dell OpenManage-Anwendungen, die auf unterstützten Windows-Plattformen ausgeführt werden, bietet Dell Schema-Erweiterungen für Kunden, um ihre Active Directory-Datenbank zu modifizieren und die Remote-

Verwaltungsauthentifizierung und Autorisierung zu unterstützen. IT Assistant, Server Administrator und Dell Remote Access Controller können eine Schnittstelle zu Active Directory herstellen, um Benutzer und Berechtigungen von einer zentralen Datenbank aus hinzuzufügen und zu kontrollieren. Informationen zur Verwendung von Active Directory finden Sie unter "Verwenden von Microsoft Active Directory".

Authentifizierungprotokolle für Linux-Betriebssysteme

Dell OpenManage-Anwendungen (Version 5.2 und später) unterstützen Netzwerk-Informationsdienste (NIS), Winbind, Kerberos und Lightweight Directory Access Protocol (LDAP) Authentifizierungsprotokolle für Linux-Betriebssysteme.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Installation von Dell OpenManage Software auf Microsoft Windows Server 2008 Core und Microsoft Hyper-V Server

Dell™ OpenManage™ Server Administrator Version 6.2- Installationshandbuch

---

Einführung

Die Installationsoption Server Core der Betriebssysteme Microsoft® Windows Server® 2008 und Hyper-V™ Server bietet eine minimale Umgebung für die Ausführung von spezifischen Serverrollen, die die Wartungs- und Verwaltungsanforderungen sowie die Angriffsfläche für diese Serverrollen reduzieren. Eine Windows Server 2008 Core- oder Hyper-V Server-Installation installiert nur eine Untergruppe der Binärdateien, die von den unterstützten Serverrollen benötigt werden. Zum Beispiel wird die Explorer-Shell nicht als Teil der Windows Server 2008 Core- oder Hyper-V Server-Installation installiert. Stattdessen ist die Standard-Benutzeroberfläche für eine Windows Server 2008 Core- oder Hyper-V Server-Installation die Eingabeaufforderung.

ANMERKUNG: Das Betriebssystem von Windows Server 2008 Core oder Hyper-V Server unterstützt keine auf eine graphische Benutzeroberfläche (GUI) basierende Installation der Dell™ OpenManage™-Softwarekomponenten. Sie müssen die OpenManage-Software im Modus der Befehlszeilenschnittstelle (CLI) auf Server Core installieren. Weitere Informationen über Server Core finden Sie auf der Microsoft-Website.

ANMERKUNG: Sie müssen als integrierter Administrator angemeldet sein, um Systems Management Software auf Windows Server 2008 und Windows Vista® zu installieren. In der Windows Server 2008-Hilfe finden Sie Informationen über das integrierte Administratorkonto.

Installation der Managed System- und Management Station-Software

Dieser Abschnitt enthält Anleitungen zur Installation von Managed System und Management Station-Software auf dem Betriebssystem Windows Server 2008 Core oder Hyper-V Server im CLI-Modus.

Ausführen von PreReqChecker im CLI-Modus

Führen Sie PreReqChecker vor der Installation der Dell OpenManage-Software aus. Weitere Informationen zur Ausführung der Voraussetzungsprüfung im CLI-Modus finden Sie unter "Voraussetzungsprüfung".

Da auf Windows Server 2008 Core oder Hyper-V Server keine GUI verfügbar ist, müssen Sie die Voraussetzungsprüfung im CLI-Modus ausführen.

- **Managed System-Software:** Geben Sie runprereqchecks.exe /s in die Eingabeaufforderung ein. Die Datei **runprereqchecks.exe** befindet sich unter **SYSMGMT\srvadmin\windows\prereqchecker** auf der DVD *Dell Systems Management Tools and Documentation*.

  ANMERKUNG: Ein negativer Return-Code (-1 bis -10) zeigt einen Fehler bei der Ausführung des Hilfsprogramms zur Voraussetzungsprüfung an. Mögliche Ursachen für negative Return-Codes umfassen Softwarerichtlinien-Restriktionen, Script-Beschränkungen, Mangel an Ordnerberechtigungen und Formatauflagen. Weitere Informationen zu Return-Codes von PreReqChecker finden Sie unter "Rückgabecodes der im Hintergrund ausgeführten Voraussetzungsprüfung".

  ANMERKUNG: Wenn Sie auf den Rückgabewert 2 oder 3 stoßen, wird empfohlen, die Datei **omprereq.htm** im temporären Windows-Ordner **%TEMP%** zu kontrollieren. Um **%TEMP%** zu finden, führen Sie den Befehl echo %TEMP% aus.

  ANMERKUNG: **omprereq.htm** ist eine HTML-Datei. Übertragen Sie diese Datei an einen anderen Computer mit einem installierten Browser, um die Datei zu lesen.

Häufige Ursachen für einen Rückgabewert 2 der Voraussetzungsprüfung:

- Einer der Speicher-Controller oder Treiber besitzt abgelaufene Firmware oder Treiber. Siehe **firmwaredriverversions_<*lang*>.html** (wobei **<lang>** Sprache bedeutet) oder **firmwaredriverversions.txt** aus dem Ordner **%TEMP%**. Um **%TEMP%** zu finden, führen Sie den Befehl echo %TEMP% aus.
- RAC-Komponentensoftware Version 4 steht für eine Standardinstallation nicht zur Auswahl, es sei denn, das Gerät wurde auf dem System erkannt. In diesem Fall erstellt die Voraussetzungsprüfung eine Warnmeldung.
- Intel®- und Broadcom®-Agenten werden nur für eine Standardinstallation ausgewählt, wenn die entsprechenden Geräte auf dem System erkannt wurden. Wenn die entsprechenden Geräte nicht gefunden wurden, erstellt die Voraussetzungsprüfung eine Warnmeldung.
- Die auf Ihrem System ausführenden DNS- oder WINS-Server können einen Warnzustand für RAC-Software auslösen. Weitere Informationen finden Sie im jeweiligen Abschnitt in der Infodatei von Server Administrator.
- Installieren Sie Managed System- und Management Station-RAC-Komponenten nicht im selben System. Installieren Sie nur die Managed System-RAC-Komponenten, da diese die erforderliche Funktionalität bieten.

Häufige Ursachen für einen Rückgabewert 3 (Fehler) der Voraussetzungsprüfung:

- Sie sind nicht mit integrierten Administratorrechten angemeldet.
- Das MSI-Paket ist fehlerhaft oder eine der erforderlichen XML-Dateien sind fehlerhaft.
- Beim Kopieren von einer DVD und von einer Netzwerkfreigabe sind Fehler und Netzwerkzugangsprobleme aufgetreten.
- Die Voraussetzungsprüfung hat erkannt, dass im Moment eine andere MSI-Paketinstallation durchgeführt wird oder ein Neustart bevorsteht: **HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\Windows\CurrentVersion\Installer\InProgress** zeigt an, dass gerade eine andere MSI-Paketinstallation durchgeführt wird. **HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Control\\Session Manager\\PendingFileRenameOperations** zeigt an, dass ein Neustart bevorsteht.

- Die x64-Edition von Windows 2008 Core wird ausgeführt, da einige Komponenten für die Installation deaktiviert sind.

Stellen Sie sicher, dass jede Fehler- oder Warnsituation behoben wird, bevor Sie mit der Installation von OpenManage-Softwarekomponenten von Dell fortfahren.

Managed System-Software im CLI-Modus installieren

1. Stellen Sie sicher, dass alle Fehler oder Warnungen, die von der Voraussetzungsprüfung erkannt wurden, vor der Installation von Managed System-Komponenten behoben werden.

2. Starten Sie die MSI-Datei mit dem Befehl `msiexec /i SysMgmt.msi` aus der Eingabeaufforderung. Die MSI-Datei **SysMgmt.msi** befindet sich unter **SYSMGMT\srvadmin\windows\SystemsManagement** auf der DVD *Dell Systems Management Tools and Documentation*.

Um die lokalisierte Version der Managed System-Software zu installieren, geben Sie `msiexec /I SysMgmt.msi TRANSFORMS= <languauge_transform>.mst` in die Eingabeaufforderung ein. Ersetzen Sie **<language_transform>.mst** mit der entsprechenden Sprachdatei.

- **1031.mst** (Deutsch)
- **1034.mst** (Spanisch)
- **1036.mst** (Französisch)
- **1041.mst** (Japanisch)
- **2052.mst** (Vereinfachtes Chinesisch)

ANMERKUNG: Weitere Informationen zu optionalen Befehlszeileneinstellungen für das MSI-Installationsprogramm finden Sie unter "Befehlszeileneinstellungen für MSI Installer".

Deinstallation der Systems Management-Software

Um Managed System-Software zu deinstallieren, führen Sie den Befehl `msiexec /x sysmgmt.msi` in der Eingabeaufforderung aus.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Setup und Administration

Dell™ OpenManage™ Server Administrator Version 6.2- Installationshandbuch

---

Bevor Sie beginnen

- Lesen Sie die Voraussetzungen für die Installation, um sicherzustellen, dass Ihr System die Mindestanforderungen erfüllt.
- Lesen Sie die jeweiligen Dell OpenManage-Infodateien und die *Dell Systems Software Support Matrix* auf der Support-Website von Dell unter **http://support.dell.com/support/edocs/software/omswrels/index.htm**. Diese Dateien enthalten die neuesten Informationen zu Software-, Firmware- und Treiberversionen sowie Informationen zu bekannten Problemen.
- Wenn Sie eine Anwendung auf den Medien ausführen, schließen Sie diese vor der Installation der Server Administrator-Anwendungen.
- Lesen Sie die Installationsanweisungen für Ihr Betriebssystem.
- Stellen Sie auf Linux-Betriebssystemen sicher, dass alle RPM-Pakete des Betriebssystems, die die Server Administrator-RPMs vorschreiben, installiert sind.

Voraussetzungen für die Installation

In diesem Abschnitt werden die allgemeinen Voraussetzungen für Dell OpenManage Server Administrator beschrieben und Informationen zu folgenden Punkten bereitgestellt:

- "Unterstützte Betriebssysteme und Webbrowser"
- "Systemanforderungen"

Spezifische Voraussetzungen für ein Betriebssystem werden als Teil der Installationsvorgänge aufgeführt.

Unterstützte Betriebssysteme und Webbrowser

Unterstützte Betriebssysteme und Webbrowser finden Sie in der *Dell Systems Software Support Matrix* auf der Support-Website von Dell unter **http://support.dell.com/support/edocs/software/omswrels/index.htm**.

ANMERKUNG: Das Dell OpenManage-Installationsprogramm bietet mehrsprachigen Support für die Betriebssysteme Windows Storage Server 2003 R2, Microsoft Windows Storage Server 2003 R2, Express x64-Edition mit Unified Storage, Microsoft Windows Storage Server 2003 R2, Workgroup x64-Edition mit Unified Storage und Windows Server 2008 (x86 und x64) R2 an. Das Multilingual User Interface Pack ist ein Satz sprachenspezifischer Ressourcendateien, die zur englischen Version eines unterstützten Windows-Betriebssystems hinzugefügt werden können. Das Dell OpenManage 6.2-Installationsprogramm unterstützt jedoch nur sechs Sprachen: Englisch, Deutsch, Spanisch, Französisch, vereinfachtes Chinesisch und Japanisch.

ANMERKUNG: Wenn die Multilingual User Interface (MUI, mehrsprachige Benutzeroberfläche) auf nicht-Unicode-Sprachen wie vereinfachtes Chinesisch oder Japanisch eingestellt ist, stellen Sie den Systemstandort auf vereinfachtes Chinesisch oder Japanisch ein. So können Meldungen der Voraussetzungsprüfung angezeigt werden. Dies liegt daran, dass nicht-Unicode-Anwendungen nur ausgeführt werden, wenn der Systemstandort (auf XP auch **Sprache für nicht-Unicode-Programme** genannt) der Anwendungssprache angepasst ist.

Systemanforderungen

Dell OpenManage Server Administrator muss auf jedem zu verwaltenden System installiert werden. Dann können Sie jedes System verwalten, indem Sie Server Administrator lokal oder per Remote-Zugriff über einen unterstützten Web-Browser ausführen.

Anforderungen für das Managed System

- Eines von "Unterstützte Betriebssysteme und Webbrowser".
- Mindestens 2 GB RAM
- Mindestens 512 MB an freier Festplattenspeicherkapazität
- Administratorrechte
- Eine TCP/IP-Verbindung zum Managed System und zum Remote-System zur vereinfachten Verwaltung des Remote-Systems.
- Einer der Unterstützte Systemverwaltungs-Protokollstandards (s. "Unterstützte Systemverwaltungs-Protokollstandards")
- Maus, Tastatur und Monitor zur lokalen Verwaltung eines Systems. Für den Monitor ist eine Mindestauflösung von 800 x 600 erforderlich. Die empfohlene Bildschirmauflösung ist 1024 x 768.

- Der RAC-Dienst von Server Administrator erfordert, dass ein Remote Access Controller (RAC) auf dem zu verwaltenden System installiert ist. Das entsprechende Benutzerhandbuch zum Dell Remote Access Controller enthält alle Software- und Hardwareanforderungen

  ANMERKUNG: Die RAC-Software wird als Teil der Option **Typisches Setup** installiert, wenn die Managed System Software installiert wird, vorausgesetzt, das Managed System erfüllt alle Anforderungen der RAC-Installation. Das entsprechende Benutzerhandbuch zum Dell Remote Access Controller enthält alle Software- und Hardwareanforderungen.

- Der Storage Management-Dienst des Server Administrator erfordert für eine ordnungsgemäße Verwaltung, dass Dell OpenManage Server Administrator auf dem System installiert ist. Vollständige Software- und Hardwareanforderungen finden Sie im *Benutzerhandbuch zum Dell OpenManage Server Administrator Storage Management*.

- Microsoft Software Installer (MSI) Version 3.1 oder höher

  ANMERKUNG: Dell OpenManage-Software erkennt die MSI-Version auf Ihrem System. Wenn die Version niedriger ist als 3.1, werden Sie von der Voraussetzungsprüfung aufgefordert, ein Upgrade auf MSI-Version 3.1 durchzuführen. Nach der Aktualisierung von MSI auf Version 3.1 kann ein Neustart des Systems erforderlich sein, um andere Software-Anwendungen wie Microsoft SQL Server zu installieren.

Unterstützte Systemverwaltungs-Protokollstandards

Ein unterstützter Systemverwaltungs-Protokollstandard muss vor der Installation von Management Station- oder Managed-System-Software auf dem Managed System installiert sein. Auf unterstützten Windows- und Linux-Betriebssystemen unterstützt Dell OpenManage das Allgemeine Informationsmodell bzw. Windows Management Instrumentation (CIM/WMI) und das Simple Network Management Protocol (SNMP). Das mit dem Betriebssystem gelieferte SNMP-Paket muss installiert werden.

ANMERKUNG: Informationen über die Installation eines Verwaltungsprotokollstandards für unterstützte Systeme auf Ihrem verwalteten System entnehmen Sie der Dokumentation Ihres Betriebssystems.

Tabelle 3-1 zeigt die Verfügbarkeit der Systemverwaltungsstandards für jedes unterstützte Betriebssystem.

Tabelle 3-1. Verfügbarkeit des Systemverwaltungsprotokolls nach Betriebssystemen

Betriebssystem	SNMP	CIM/WMI
Unterstützte Microsoft Windows-Betriebssysteme	Auf dem Installationsdatenträger des Betriebssystems verfügbar.	Immer installiert
Unterstützte Red Hat Enterprise Linux-Betriebssysteme	Installieren Sie das mit dem Betriebssystem gelieferte SNMP-Paket.	Verfügbar. Installieren Sie die auf der DVD *Dell Systems Management Tools and Documentation* enthaltenen CIM-Pakete **SFCB/SFCC/CMPI-Devel**
Unterstützte SUSE Linux Enterprise Server-Betriebssysteme.	Installieren Sie das mit dem Betriebssystem gelieferte SNMP-Paket.	Verfügbar. Installieren Sie die auf der DVD *Dell Systems Management Tools and Documentation* enthaltenen CIM-Pakete **SFCB/SFCC/CMPI-Devel**

Windows Server 2003 R2 und der R2 IPMI-Gerätetreiber

Die Informationen in diesem Abschnitt betreffen nur Dell PowerVault *x*00- und Dell PowerEdge *x8xx*- oder neuere Systeme.

Windows Server 2003 R2 und Windows Storage Server R2 enthalten eine optionale Komponente namens Hardware Management. Diese Komponente enthält einen IPMI-Treiber. Während der Installation wird von der Komponente der IPMI-Treiber installiert und aktiviert.

Beim Start von Server Administrator wird zuerst festgestellt, ob der Windows Server 2003 R2 IPMI-Treiber aktiviert ist. Wenn dieser aktiviert ist, stellt Server Administrator dann anhand des IPMI-Treibers vom Windows Server 2003 R2 die IPMI-basierten Funktionen zur Verfügung. Wenn der IPMI-Treiber vom Windows Server 2003 R2 nicht aktiviert ist, verwendet der Server Administrator seine eigene interne IPMI-Unterstützung, um die IPMI-basierten Funktionen zur Verfügung zu stellen. Es wird empfohlen, für Server Administrator den IPMI-Treiber vom Windows Server 2003 R2 anstelle der internen IPMI-Unterstützung zu verwenden. Wenn Ihr System auf dem Windows Server 2003 R2 oder Windows Storage Server R2 ausgeführt wird, wird empfohlen, dass Sie nach der Installation von Server Administrator auch die optionale Hardware Management-Komponente von R2 installieren.

Um den Windows Server 2003 R2 IPMI-Treiber auf Dell PowerVault *x00*-Systemen zu installieren, führen Sie folgenden zusätzlichen Schritt aus:

- Führen Sie den folgenden Befehl von einem Befehls-Shell aus:

```
Rundll32 ipmisetp.dll, AddTheDevice
```

Nachdem Sie die Hardware Management-Komponente auf Windows Server 2003 R2 installiert haben, müssen Sie den Dienst **DSM SA Data Manager** neu starten, so dass Server Administrator von der Verwendung der internen IPMI-Unterstützung auf die Verwendung des IPMI-Treibers vom Windows Server 2003 R2 wechseln kann. Um das Dienstprogramm neu zu starten, können Sie entweder das Dienstprogramm manuell oder das System neu starten.

Wenn Sie den Windows Server 2003 R2-IPMI-Treiber später entweder direkt manuell deinstallieren oder die Hardware Management-Komponente deinstallieren (wodurch der Treiber deinstalliert wird), müssen Sie den Dienst **DSM SA Data Manager** neu starten, so dass Server Administrator von der Verwendung des IPMI-Treibers vom Windows Server 2003 R2 auf die Verwendung der internen IPMI-Unterstützung wechseln kann. Um das Dienstprogramm neu zu starten, können Sie entweder das Dienstprogramm manuell oder das System neu starten.

Digitale Zertifikate

Alle Pakete von Server Administrator für Microsoft sind mit einem Dell Zertifikat digital signiert. Dies hilft, die Integrität der Installationspakete zu garantieren. Wenn diese Pakete neu verpackt, bearbeitet oder auf eine andere Weise manipuliert werden, wird die Digitalsignatur ungültig. Diese Manipulation führt zu einem nicht unterstützten Installationspaket und die Voraussetzungsprüfung erlaubt die Softwareinstallation nicht.

Konfigurieren eines unterstützten Webbrowsers

Für eine Liste unterstützter Web-Browser, siehe "Unterstützte Betriebssysteme und Webbrowser".

ANMERKUNG: Stellen Sie sicher, dass der Webbrowser zur Umgehung des Proxy-Servers für lokale Adressen eingestellt ist.

Anzeigen lokalisierter Versionen der webbasierten Schnittstelle

Verwenden Sie **Regionale und Sprachoptionen** in der Windows **Systemsteuerung**, um lokalisierte Versionen der Web-basierten Schnittstelle auf Systemen anzuzeigen, die Windows-Betriebssysteme ausführen.

Microsoft Active Directory

Wenn Sie die Active Directory Service-Software verwenden, können Sie diese konfigurieren, um den Zugriff auf Ihr Netzwerk zu kontrollieren. Dell hat die Active Directory-Datenbank so modifiziert, dass Remote-Verwaltungsauthentifizierung und -genehmigung unterstützt werden. Dell OpenManage Server Administrator, IT Assistant und Dell Remote Access Controllers können eine Verbindung zu Active Directory herstellen. Mit diesem Hilfsprogramm können Sie Benutzer und Berechtigungen von einer zentralen Datenbank aus hinzufügen und kontrollieren. Wenn Sie Active Directory verwenden, um Benutzerzugriff auf Ihr Netzwerk zu kontrollieren, lesen Sie "Verwenden von Microsoft Active Directory".

SNMP-Agenten konfigurieren

Dell OpenManage Software unterstützt den SNMP-Systemverwaltungsstandard auf allen unterstützten Betriebssystemen. Sie können die SNMP-Unterstützung je nach Betriebssystem und Betriebssysteminstallation installieren oder nicht installieren. Vor der Installation der Dell OpenManage-Software muss ein unterstützter Systemverwaltungsprotokollstandard, z. B. SNMP, installiert werden. Weitere Informationen finden Sie unter "Voraussetzungen für die Installation".

Sie können den SNMP-Agenten zur Änderung des Community-Namens, Aktivierung von Set-Vorgängen und Senden von Traps an eine Management Station konfigurieren. Zur Konfiguration des SNMP-Agenten für die korrekte Interaktion mit Verwaltungsanwendungen wie z. B. IT Assistant führen Sie die im Folgenden beschriebenen Verfahren aus.

ANMERKUNG: Die Standardkonfiguration des SNMP-Agenten enthält normalerweise einen SNMP-Community-Namen wie z. B. "public". Ändern Sie aus Sicherheitsgründen die Standard-SNMP-Community-Namen. Informationen zum Ändern von SNMP Community-Namen erhalten Sie im entsprechenden untenstehenden Abschnitt für Ihr Betriebssystem. Zusätzliche Richtlinien erhalten Sie im Artikel **Securing an SNMP Environment** (Sichern einer SNMP-Umgebung) von Mai 2003 im Magazin Dell Power Solutions. Dieses Magazin ist auch unter **www.dell.com/powersolutions** erhältlich.

Die folgenden Abschnitte enthalten schrittweise Anleitungen für die Konfiguration des SNMP-Agenten für jedes unterstützte Betriebssystem.

- Konfigurieren von SNMP-Agenten für Systeme, auf denen unterstützte Windows-Betriebssysteme ausgeführt werden
- Konfigurieren von SNMP-Agenten auf Systemen, auf denen unterstützte Red Hat Enterprise Linux-Betriebssysteme ausgeführt werden
- Konfigurieren von SNMP-Agenten auf Systemen, auf denen unterstützte SUSE Linux Enterprise Server-Betriebssysteme ausgeführt werden

Konfigurieren von SNMP-Agenten für Systeme, auf denen unterstützte Windows-Betriebssysteme ausgeführt werden

Dell OpenManage-Software verwendet die SNMP-Dienste, die vom Windows SNMP-Agenten bereitgestellt werden. Zum Herstellen einer Verbindung zu einer System Administrator-Sitzung werden die folgenden zwei Methoden unterstützt: SNMP und CIM/WMI. Sie können den SNMP-Agenten zur Änderung des Community-Namens, Aktivierung von Set-Vorgängen und Senden von Traps an eine Verwaltungsstation konfigurieren. Zur Konfiguration des SNMP-Agenten für die korrekte Interaktion mit Verwaltungsanwendungen wie IT Assistant führen Sie die im folgenden beschriebenen Verfahren aus.

ANMERKUNG: Weitere Einzelheiten zur SNMP-Konfiguration finden Sie in der Dokumentation des Betriebssystems.

Aktivieren von SNMP-Zugriff mit Remote-Hosts auf Windows Server 2003

Standardmäßig nimmt der Windows Server 2003 keine SNMP-Pakete von Remote-Hosts an. Für Systeme mit Windows Server 2003 muss der SNMP-Dienst so konfiguriert werden, dass er SNMP-Pakete von Remote-Hosts annimmt, wenn geplant ist, das System von Remote-Hosts aus über SNMP-Verwaltungsanwendungen zu verwalten.

ANMERKUNG: Ein Neustart des Systems für Änderungsverwaltungsfunktionen erfordert keine SNMP Set-Vorgänge.

Damit ein System mit dem Betriebssystem Windows Server 2003 SNMP-Pakete von Remote-Hosts empfangen kann, führen Sie folgende Schritte aus:

1. Öffnen Sie das Fenster **Computerverwaltung**.
2. Erweitern Sie das Symbol **Computerverwaltung** im Fenster, falls erforderlich.
3. Erweitern Sie das Symbol **Dienste und Anwendungen** und klicken Sie auf **Dienste**.
4. Scrollen Sie durch die Liste der Dienste, bis Sie **SNMP-Dienste** finden, klicken Sie mit der rechten Maustaste auf **SNMP-Dienst** und dann auf **Eigenschaften**.

Das Fenster **Eigenschaften von SNMP-Dienst** wird angezeigt.

5. Klicken Sie auf das Register **Sicherheit**.

6. Wählen Sie **SNMP-Pakete von jedem Host annehmen** oder fügen Sie den IT Assistant-Host der Liste **SNMP-Pakete von diesen Hosts annehmen** hinzu.

SNMP-Community-Namen ändern

Durch die Konfiguration der SNMP-Community-Namen wird festgelegt, welche Systeme das System über SNMP verwalten können. Der von Management Station verwendete SNMP-Community-Name muss mit einem SNMP-Community-Namen übereinstimmen, der auf dem Dell OpenManage-Softwaresystem konfiguriert wurde, damit die Verwaltungsanwendungen Systemverwaltungsinformationen von der Dell OpenManage-Software abrufen können.

1. Öffnen Sie das Fenster **Computerverwaltung**.

2. Erweitern Sie das Symbol **Computerverwaltung** im Fenster, falls erforderlich.

3. Erweitern Sie das Symbol **Dienste und Anwendungen** und klicken Sie auf **Dienste**.

4. Scrollen Sie durch die Liste der Dienste, bis Sie **SNMP-Dienste** finden, klicken Sie mit der rechten Maustaste auf **SNMP-Dienst** und dann auf **Eigenschaften**.

   Das Fenster **Eigenschaften von SNMP-Dienst** wird angezeigt.

5. Klicken Sie auf das Register **Sicherheit**, um einen Community-Namen hinzuzufügen oder zu ändern.

   a. Um einen Community-Namen hinzuzufügen, klicken Sie auf **Hinzufügen** unter der Liste **Akzeptierte Community-Namen**.

      Das Fenster **Konfiguration von SNMP-Dienst** wird angezeigt.

   b. Geben Sie den Community-Namen der Management Station (der Standard ist öffentlich) im Textfeld **Community-Name** ein und klicken Sie auf **Hinzufügen**.

      Das Fenster **Eigenschaften von SNMP-Dienst** wird angezeigt.

   c. Zum Ändern eines Community-Namens wählen Sie einen Community-Namen aus der Liste **Akzeptierte Community-Namen** aus und klicken Sie auf **Bearbeiten**.

      Das Fenster **Konfiguration von SNMP-Dienst** wird angezeigt.

   d. Bearbeiten Sie den Community-Namen der Management Station im Textfeld **Community-Name** und klicken Sie auf **OK**.

      Das Fenster **Eigenschaften von SNMP-Dienst** wird angezeigt.

6. Klicken Sie auf **OK** zum Speichern der Änderungen.

SNMP-Set-Vorgänge aktivieren

SNMP-Set-Vorgänge müssen auf dem Dell OpenManage-Softwaresystem aktiviert sein, damit Dell OpenManage-Softwareattribute mittels IT Assistant geändert werden können. Um Remote-Herunterfahren eines Systems von IT Assistant zu aktivieren, muss der SNMP Set-Betrieb aktiviert sein.

ANMERKUNG: Ein Neustart des Systems für Änderungsverwaltungsfunktionen erfordert keine SNMP Set-Vorgänge.

1. Öffnen Sie das Fenster **Computerverwaltung**.

2. Erweitern Sie das Symbol **Computerverwaltung** im Fenster, falls erforderlich.

3. Erweitern Sie das Symbol **Dienste und Anwendungen** und klicken Sie auf **Dienste**.

4. Scrollen Sie durch die Liste der Dienste, bis Sie **SNMP-Dienste** finden, klicken Sie mit der rechten Maustaste auf **SNMP-Dienst** und dann auf **Eigenschaften.**

   Das Fenster **Eigenschaften von SNMP-Dienst** wird angezeigt.

5. Klicken Sie auf das Register **Sicherheit**, um die Zugriffsrechte für eine Community zu ändern.

6. Wählen Sie einen Community-Namen aus der Liste **Akzeptierte Community-Namen** und klicken Sie auf **Bearbeiten.**

   Das Fenster **Konfiguration von SNMP-Dienst** wird angezeigt.

7. Legen Sie die **Community-Rechte LESEN SCHREIBEN** oder **LESEN ERSTELLEN** fest und klicken Sie auf **OK**.

   Das Fenster **Eigenschaften von SNMP-Dienst** wird angezeigt.

8. Klicken Sie auf **OK** zum Speichern der Änderungen.

ANMERKUNG: Beginnend mit Dell OpenManage Server Administrator Version 5.3 sind die SNMP-Satz-Vorgänge standardmäßig in Server Administrator deaktiviert. Server Administrator bietet Support, um SNMP-Satz-Vorgänge zu aktivieren oder zu deaktivieren. Sie können die Server Administrator-Seite **SNMP-Konfiguration** unter **Einstellungen** oder die Server Administrator-Befehlszeilenschnittstelle (CLI) verwenden, um die SNMP-Satz-Vorgänge zu aktivieren oder zu deaktivieren. Weitere Informationen zum Aktivieren oder Deaktivieren von SNMP-Satz-Vorgängen in Server Administrator finden Sie im *Benutzerhandbuch zum Dell OpenManage Server Administrator* oder im *Benutzerhandbuch für die Dell OpenManage Server Administrator Befehlszeilenoberfläche*.

Konfigurieren des Systems zum Senden von SNMP-Traps an eine Management Station

Dell OpenManage-Software erzeugt SNMP-Traps als Reaktion auf Änderungen im Status von Sensoren und anderen überwachten Parametern. Sie müssen ein oder mehrere Trap-Ziele auf dem Dell OpenManage-Softwaresystem konfigurieren, damit SNMP-Traps an eine Management Station gesendet werden können.

1. Öffnen Sie das Fenster **Computerverwaltung**.
2. Erweitern Sie das Symbol **Computerverwaltung** im Fenster, falls erforderlich.
3. Erweitern Sie das Symbol **Dienste und Anwendungen** und klicken Sie auf **Dienste**.
4. Scrollen Sie durch die Liste der Dienste, bis Sie **SNMP-Dienste** finden, klicken Sie mit der rechten Maustaste auf **SNMP-Dienst** und dann auf **Eigenschaften**.

   Das Fenster **Eigenschaften von SNMP-Dienst** wird angezeigt.

5. Klicken Sie auf das Register **Traps**, um eine Community für Traps hinzuzufügen oder um ein Trap-Ziel für eine Trap-Community hinzuzufügen.
   a. Zur Hinzufügung einer Community für Traps geben Sie den **Community-Namen** im Feld Community-Name ein und klicken dann auf **Zur Liste hinzufügen** gleich neben dem Feld **Community- Name.**
   b. Zur Hinzufügung eines Trap-Ziels für eine Trap-Community wählen Sie den Community-Namen aus dem Dropdown-Feld **Community- Name** und klicken Sie auf **Hinzufügen** unter dem Feld **Trap-Ziele**.

      Das Fenster **Konfiguration von SNMP-Dienst** wird angezeigt.

   c. Geben Sie das Trap-Ziel ein und klicken Sie auf **Hinzufügen**.

      Das Fenster **Eigenschaften von SNMP-Dienst** wird angezeigt.

6. Klicken Sie auf **OK** zum Speichern der Änderungen.

Konfigurieren von SNMP-Agenten auf Systemen, auf denen unterstützte Red Hat Enterprise Linux-Betriebssysteme ausgeführt werden

Server Administrator verwendet die SNMP-Dienste, die vom **ucd-snmp**- oder **net-snmp**-Agenten bereitgestellt werden. Sie können den SNMP-Agenten zur Änderung des Community-Namens, zur Aktivierung von Set-Vorgängen und zum Senden von Traps an eine Verwaltungsstation konfigurieren. Zur Konfiguration des SNMP-Agenten für die korrekte Interaktion mit Verwaltungsanwendungen, wie dem IT Assistant, führen Sie die im folgenden beschriebenen Verfahren aus.

ANMERKUNG: Konsultieren Sie die Dokumentation des Betriebssystems für zusätzliche Details über die SNMP-Konfiguration.

Konfiguration von SNMP-Agent Access Control

Der Zweig der Verwaltungsinformationsbasis (MIB), der von Server Administrator implementiert wird, wird mit dem OID 1.3.6.1.4.1.674 gekennzeichnet. Management Station-Anwendungen müssen Zugriff auf diesen Zweig der MIB-Struktur aufweisen, um Systeme verwalten zu können, auf denen Server Administrator ausgeführt wird.

Bei unterstützten Red Hat Enterprise Linux-Betriebssystemen erlaubt die standardmäßige SNMP-Agent-Konfiguration Lesezugriff für die *öffentliche* Community nur für den *System*-Zweig MIB-II (gekennzeichnet mit dem OID 1.3.6.1.2.1.1) der MIB-Struktur. Diese Konfiguration erlaubt es nicht, dass Verwaltungsanwendungen Informationen von Server Administrator oder andere Systems Management-Informationen außerhalb des "**System**"-Zweigs MIB-II abrufen oder ändern.

Server Administrator SNMP Agent - Installationsmaßnahmen

Wenn Server Administrator diese Standard-SNMP-Konfiguration während der Installation erkennt, versucht er, die SNMP-Agent-Konfiguration so zu ändern, dass die *öffentliche* Community einen Lesezugriff für die gesamte MIB- Struktur erhält. Server Administrator ändert die SNMP-Agent-Konfigurationsdatei **/etc/snmp/snmpd.conf** auf zwei Arten.

Mit der ersten Änderung wird die Ansicht auf die gesamte MIB-Struktur freigegeben, und zwar durch Hinzufügen der folgenden Zeile, falls diese noch nicht existiert:

```
view all included .1
```

Mit der zweiten Änderung wird die Zeile für den standardmäßigen *Zugriff* abgeändert, so dass die *öffentliche* Community Lesezugriff auf die gesamte MIB-Struktur erhält. Der Server Administrator sucht folgende Zeile:

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

Wenn Server Administrator auf diese Zeile stößt, wird die Zeile wie folgt modifiziert:

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

Diese Änderungen der standardmäßigen SNMP-Agent-Konfiguration erlauben der *öffentlichen* Community den Lesezugriff auf die gesamte MIB-Struktur.

ANMERKUNG: Damit sichergestellt ist, dass der Server Administrator die SNMP-Agent-Konfiguration ändern kann, um korrekten Zugriff auf die Systems Management-Daten zu erteilen, wird empfohlen, etwaige weitere SNMP-Agent-Konfigurationsänderungen erst nach Installation von Server Administrator vorzunehmen.

Server Administrator-SNMP kommuniziert mit dem SNMP-Agenten über das SNMP-Multiplexing-Protokoll (SMUX). Wenn Server Administrator eine Verbindung mit dem SNMP-Agenten hergestellt hat, sendet dieser einen Objektbezeichner an den SNMP-Agenten, um sich als SMUX-Peer zu identifizieren. Da dieser Objektbezeichner mit dem SNMP-Agenten konfiguriert werden muss, fügt Server Administrator der Konfigurationsdatei **/etc/snmp/snmpd.conf** des SNMP-Agenten während der Installation die folgende Zeile hinzu, wenn diese nicht vorhanden ist:

```
smuxpeer .1.3.6.1.4.1.674.10892.1
```

SNMP-Community-Namen ändern

Durch die Konfiguration der SNMP-Community-Namen wird festgelegt, welche Systeme das System über SNMP verwalten können. Der von Systemverwaltungsanwendungen verwendete SNMP-Community-Name muss mit einem SNMP-Community-Namen übereinstimmen, der auf dem Server Administrator-Softwaresystem konfiguriert wurde, damit die Systemverwaltungsanwendungen Verwaltungsinformationen von Server Administrator abrufen können.

Zum Ändern des SNMP-Community-Namens, der zum Abrufen von Verwaltungsinformationen von einem System verwendet wird, auf dem Server Administrator ausgeführt wird, bearbeiten Sie die SNMP-Agent-Konfigurationsdatei **/etc/snmp/snmpd.conf** und führen Sie folgende Schritte aus:

1. Suchen Sie die folgende Zeile:

   ```
   com2sec publicsec default public
   ```

   oder

   ```
   com2sec notConfigUser default public
   ```

2. Bearbeiten Sie diese Zeile und ersetzen Sie `public` durch den neuen SNMP-Community-Namen. Nach der Bearbeitung muss die Zeile wie folgt aussehen:

   ```
   com2sec publicsec default Community-Name
   ```

   oder

   ```
   com2sec notConfigUser default Community-Name
   ```

3. Zur Aktivierung von Änderungen an der SNMP-Konfiguration starten Sie den SNMP-Agenten neu durch Eingabe von:

   ```
   service snmpd restart
   ```

SNMP-Set-Vorgänge aktivieren

SNMP-Set-Vorgänge müssen auf dem System aktiviert sein, auf dem Server Administrator ausgeführt wird, damit Server Administrator-Softwareattribute mittels IT Assistant geändert werden können. Um Remote-Herunterfahren eines Systems von IT Assistant zu aktivieren, muss der SNMP Set-Betrieb aktiviert sein.

ANMERKUNG: Ein Neustart des Systems für Änderungsverwaltungsfunktionen erfordert keine SNMP Set-Vorgänge.

Zur Aktivierung von SNMP-Set-Vorgängen auf dem System, auf dem Server Administrator ausgeführt wird, bearbeiten Sie die SNMP-Agent-Konfigurationsdatei **/etc/snmp/snmpd.conf** und führen folgende Schritte aus:

1. Suchen Sie die folgende Zeile:

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

   oder

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

2. Bearbeiten Sie diese Zeile und ersetzen Sie das erste `none` durch `all`. Nach der Bearbeitung muss die Zeile wie folgt aussehen:

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

oder

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

3. Zur Aktivierung von Änderungen an der SNMP-Konfiguration starten Sie den SNMP-Agenten neu durch Eingabe von:

```
service snmpd restart
```

Konfigurieren des Systems zum Senden von Traps an eine Management Station

Server Administrator erstellt SNMP-Traps als Reaktion auf Änderungen im Status von Sensoren und anderen überwachten Parametern. Sie müssen ein oder mehrere Trap-Ziele auf dem System konfigurieren, auf dem Server Administrator ausgeführt wird, damit SNMP-Traps an eine Management Station gesendet werden können.

Um ein System, auf dem Server Administrator ausgeführt wird, so zu konfigurieren, dass Traps an eine Management Station gesendet werden, bearbeiten Sie die SNMP-Agent-Konfigurationsdatei **/etc/snmp/snmpd.conf** und führen Sie folgende Schritte aus:

1. Fügen Sie folgende Zeile zur Datei hinzu:

```
trapsink IP-Adresse Community-Name
```

wobei *IP-Adresse* die IP-Adresse der Management Station und *Community-Name* der SNMP-Community-Name ist.

2. Zur Aktivierung von Änderungen an der SNMP-Konfiguration starten Sie den SNMP-Agenten neu durch Eingabe von:

```
service snmpd restart
```

Firewall-Konfiguration auf Systemen, auf denen unterstützte Red Hat Enterprise Linux-Betriebssysteme ausgeführt werden

Wenn beim Installieren von Red Hat Enterprise Linux die Firewall-Sicherheit aktiviert wird, wird die SNMP-Schnittstelle an allen externen Netzwerkschnittstellen standardmäßig geschlossen. Damit SNMP-Verwaltungsanwendungen, wie z. B. IT Assistant, Informationen vom Server Administrator ermitteln und empfangen können, muss die SNMP-Schnittstelle auf mindestens einer externen Netzwerkschnittstelle geöffnet sein. Wenn der Server Administrator ermittelt, dass keine SNMP-Schnittstelle der Firewall aller externen Netzwerkschnittstellen geöffnet ist, zeigt der Server Administrator eine Warnmeldung an und trägt eine Meldung in das Systemprotokoll ein.

Um den SNMP-Anschluss zu öffnen, muss die Firewall deaktiviert, eine gesamte externe Netzwerkschnittstelle der Firewall geöffnet oder der SNMP-Anschluss von mindestens einer externen Netzwerkschnittstelle der Firewall geöffnet werden. Diese Maßnahme kann vor oder nach dem Start des Server Administrators durchgeführt werden.

Um den SNMP-Anschluss mittels einer der zuvor beschriebenen Methoden zu öffnen, führen Sie folgende Schritte durch:

1. Geben Sie bei der Befehlsaufforderung von Red Hat Enterprise Linux den Befehl setup ein und drücken Sie <Eingabe>, um das Textmodus- Setup-Dienstprogramm zu starten.

   ANMERKUNG: Dieser Befehl steht nur dann zur Verfügung, wenn das Betriebssystem mit Standardeinstellungen installiert worden ist.

   Das Menü **Hilfsprogramm auswählen** wird eingeblendet.

2. Wählen Sie **Firewall-Konfiguration** mit dem Nach-Unten-Pfeil aus und drücken Sie <Eingabe>.

   Der Bildschirm **Firewall-Konfiguration** wird geöffnet.

3. Wählen Sie die **Sicherheitsstufe** aus. Die ausgewählte **Sicherheitsstufe** wird mit einem Sternchen markiert.

   ANMERKUNG: Drücken Sie die Taste <F1>, um weitere Informationen über die Sicherheitsstufen der Firewall zu erhalten. Die Standard-SNMP-Anschlussnummer ist **161**. Wenn Sie die X Windows-GUI verwenden, kann es sein, dass bei neueren Versionen des Red Hat Enterprise Linux-Betriebssystems durch Drücken von <F1> nicht die Informationen über die Firewall-Sicherheitsstufen angezeigt werden.

   a. Zur Deaktivierung der Firewall wählen Sie **Keine Firewall** oder **Deaktiviert** aus und gehen dann zu Schritt Schritt 7 weiter.

   b. Um eine komplette Netzwerkschnittstelle oder die SNMP- Schnittstelle zu öffnen, wählen Sie **Hoch, Mittel** oder **Aktiviert** aus.

d. Wählen Sie **Anpassen** und drücken Sie <Eingabe>.

   Der Bildschirm **Firewall-Konfiguration - Anpassen** wird geöffnet.

5. Wählen Sie aus, ob eine gesamte Netzwerkschnittstelle oder nur ein SNMP-Anschluss jeder Netzwerkschnittstelle geöffnet werden soll.

   a. Um eine komplette Netzwerkschnittstelle zu öffnen, wählen Sie eine der **vertrauenswürdigen Komponenten** und drücken Sie die Leertaste. Ein Sternchen im Feld links neben dem Komponentennamen zeigt an, dass die gesamte Schnittstelle geöffnet wird.

   b. Um einen SNMP-Anschluss jeder Netzwerkschnittstelle zu öffnen, wählen Sie **Weitere Anschlüsse** und geben Sie `snmp:udp` ein.

6. Wählen Sie **OK** und drücken Sie <Eingabe>.

   Der Bildschirm **Firewall-Konfiguration** wird geöffnet.

7. Wählen Sie **OK** und drücken Sie <Eingabe>.

   Das Menü **Hilfsprogramm auswählen** wird eingeblendet.

8. Wählen Sie **Beenden** und drücken Sie <Eingabe>.

Konfigurieren von SNMP-Agenten auf Systemen, auf denen unterstützte SUSE Linux Enterprise Server-Betriebssysteme ausgeführt werden

Server Administrator verwendet die SNMP-Dienste, die vom ucd-snmp- oder net-snmp-Agenten bereitgestellt werden. Sie können den SNMP Agenten so konfigurieren, dass der SNMP-Zugang von Remote-Hosts aktiviert ist, der Community-Name geändert werden kann, Set-Vorgänge aktiviert sind und Traps an eine Management Station gesendet werden. Zur Konfiguration des SNMP-Agenten für die korrekte Interaktion mit Systemverwaltungsanwendungen wie dem IT Assistant führen Sie die im Folgenden beschriebenen Verfahren aus.

ANMERKUNG: Beim SUSE Linux Enterprise Server (Version 10) befindet sich die SNMP-Agent-Konfigurationsdatei unter **/etc/snmp/snmpd.conf**.

ANMERKUNG: Konsultieren Sie die Dokumentation des Betriebssystems für zusätzliche Details über die SNMP-Konfiguration.

SNMP-Installationsmaßnahme für Server Administrator

Server Administrator-SNMP kommuniziert mit dem SNMP-Agenten über das SNMP-Multiplexing-Protokoll (SMUX). Wenn Server Administrator eine Verbindung mit dem SNMP-Agenten hergestellt hat, sendet dieser einen Objektbezeichner an den SNMP-Agenten, um sich als SMUX-Peer zu identifizieren. Da dieser Objektbezeichner mit dem SNMP-Agenten konfiguriert werden muss, fügt Server Administrator der Konfigurationsdatei **/etc/snmpd/.conf** oder **/etc/snmp/snmpd.conf** des SNMP-Agenten während der Installation die folgende Zeile hinzu, wenn diese nicht vorhanden ist:

```
smuxpeer .1.3.6.1.4.1.674.10892.1
```

SNMP-Zugang von Remote-Hosts aktivieren

Die Standard-SNMP Agent-Konfiguration auf SUSE Linux Enterprise Server-Betriebssystemen erteilt nur schreibgeschützten Zugriff auf die komplette MIB-Struktur an die *öffentliche* Community vom lokalen Host. Diese Konfiguration lässt keine SNMP-Verwaltungsanwendungen wie IT Assistant, die auf anderen Hosts ausgeführt werden, für eine einwandfreie Erkennung und Verwaltung von Server Administrator-Systemen zu. Wenn diese Konfiguration während der Installation von Server Administrator erkannt wird, wird eine Meldung in der Betriebssystem-Protokolldatei **/var/log/messages** aufgezeichnet, um anzuzeigen, dass sich der SNMP-Zugang auf den lokalen Host beschränkt. Sie müssen den SNMP-Agenten konfigurieren, um den SNMP-Zugang von Remote-Hosts zu aktivieren, wenn Sie das System mit SNMP Verwaltungsanwendungen von Remote-Hosts aus verwalten möchten.

ANMERKUNG: Aus Sicherheitsgründen ist es ratsam, den SNMP-Zugriff auf bestimmte Remote-Hosts soweit wie möglich einzuschränken.

Um den SNMP- Zugang von einem bestimmten Remote-Host zu einem System zu aktivieren, das Server Administrator ausführt, bearbeiten Sie die SNMP-Agenten-Konfigurationsdatei **/etc/snmpd.conf** oder **/etc/snmp/snmpd.conf** und führen folgende Schritte durch:

1. Suchen Sie die folgende Zeile:

   ```
   rocommunity public 127.0.0.1
   ```

2. Bearbeiten oder kopieren Sie diese Zeile und ersetzen Sie 127.0.0.1 mit der IP-Adresse des Remote-Hosts. Nach der Bearbeitung muss die Zeile wie folgt aussehen:

   ```
   rocommunity public IP_Adresse
   ```

   ANMERKUNG: Sie können SNMP-Zugriff von mehrfachen spezifischen Remote-Hosts aktivieren, indem Sie eine `rocommunity`-Direktive für jeden Remote-Host hinzufügen.

3. Zur Aktivierung von Änderungen an der SNMP-Konfiguration starten Sie den SNMP-Agenten neu durch Eingabe von:

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

Um den SNMP- Zugang von allen Remote-Hosts zu einem System zu aktivieren, das Server Administrator ausführt, bearbeiten Sie die SNMP-Agenten-Konfigurationsdatei **/etc/snmpd.conf** oder **/etc/snmp/snmpd.conf** und führen folgende Schritte durch:

1. Suchen Sie die folgende Zeile:

   ```
   rocommunity public 127.0.0.1
   ```

2. Bearbeiten Sie diese Zeile, indem Sie 127.0.0.1 entfernen. Nach der Bearbeitung muss die Zeile wie folgt aussehen:

   ```
   rocommunity public
   ```

3. Zur Aktivierung von Änderungen der SNMP-Konfiguration starten Sie den SNMP-Agenten neu durch Eingabe von:

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

SNMP-Community-Namen ändern

Die Konfiguration des SNMP-Community-Namens bestimmt, welche Systeme das System über SNMP verwalten kann. Der von Verwaltungsanwendungen verwendete SNMP-Community-Name muss mit einem SNMP-Community-Namen übereinstimmen, der auf dem Server Administrator-System konfiguriert wurde, damit die Verwaltungsanwendungen Verwaltungsinformationen von Server Administrator abrufen können.

Zum Ändern des standardmäßigen SNMP-Community-Namens, der zum Abrufen von Verwaltungsinformationen von einem System verwendet wird, auf dem Server Administrator ausgeführt wird, bearbeiten Sie die SNMP-Agent-Konfigurationsdatei **/etc/snmpd.conf** oder **/etc/snmp/snmpd.conf** und führen Sie folgende Schritte aus:

1. Suchen Sie die folgende Zeile:

   ```
   rocommunity public 127.0.0.1
   ```

2. Bearbeiten Sie diese Zeile, indem Sie public durch den neuen SNMP- Community-Namen ersetzen. Nach der Bearbeitung muss die Zeile wie folgt aussehen:

   ```
   rocommunity Community-Name 127.0.0.1
   ```

3. Zur Aktivierung von Änderungen an der SNMP-Konfiguration starten Sie den SNMP-Agenten neu durch Eingabe von:

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

Aktivieren von SNMP-Set-Vorgängen

SNMP-Set-Vorgänge müssen auf dem System aktiviert sein, auf dem Server Administrator ausgeführt wird, damit Server Administrator-Attribute mittels IT Assistant geändert werden können. Um Remote-Herunterfahren eines Systems von IT Assistant zu aktivieren, muss der SNMP Set-Betrieb aktiviert sein.

ANMERKUNG: Ein Neustart des Systems für Änderungsverwaltungsfunktionen erfordert keine SNMP Set-Vorgänge.

Um SNMP-Satz-Vorgänge auf dem System zu aktivieren, das Server Administrator ausführt, bearbeiten Sie die SNMP-Agent-Konfigurationsdatei, **/etc/snmpd.conf** oder **/etc/snmp/snmpd.conf**, und führen Sie die folgenden Schritte aus:

1. Suchen Sie die folgende Zeile:

   ```
   rocommunity public 127.0.0.1
   ```

2. Bearbeiten Sie diese Zeile, indem Sie rocommunity durch rwcommunity ersetzen. Nach der Bearbeitung muss die Zeile wie folgt aussehen:

   ```
   rwcommunity public 127.0.0.1
   ```

3. Zur Aktivierung von Änderungen an der SNMP-Konfiguration starten Sie den SNMP-Agenten neu durch Eingabe von:

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

Konfigurieren des Systems zum Senden von Traps an eine Management Station

Server Administrator erstellt SNMP-Traps als Reaktion auf Änderungen im Status von Sensoren und anderen überwachten Parametern. Sie müssen ein oder mehrere Trap-Ziele auf dem System konfigurieren, auf dem Server Administrator ausgeführt wird, damit SNMP-Traps an eine Management Station gesendet werden können.

Um Ihr System, das Server Administrator ausführt, so zu konfigurieren, dass Traps an eine Management Station gesendet werden, bearbeiten Sie die SNMP-Agenten-Konfigurationsdatei **/etc/snmpd.conf** oder **/etc/snmp/snmpd.conf** und führen folgende Schritte durch:

1. Fügen Sie folgende Zeile zur Datei hinzu:

   ```
   trapsink IP-Adresse Community-Name
   ```

   wobei IP-Adresse die IP-Adresse der Management Station und Community-Name der SNMP-Community-Name ist.

2. Zur Aktivierung von Änderungen an der SNMP-Konfiguration starten Sie den SNMP-Agenten neu durch Eingabe von:

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

Secure Port-Server- und Sicherheits-Setup

Dieser Abschnitt behandelt die folgenden Themen:

- Benutzer- und Server-Einstellungen vornehmen
- X.509-Zertifikatsverwaltung

Benutzer- und Server-Einstellungen vornehmen

Sie können die Einstellungen für Benutzer und sicheren Port Server für Server Administrator und IT Assistant von der entsprechenden Webseite **Einstellungen** festlegen. Klicken Sie auf **Allgemeine Einstellungen** und entweder auf das Register **Benutzer** oder das Register **Web Server**.

ANMERKUNG: Zum Festlegen oder Zurücksetzen von Benutzer- oder Server-Einstellungen müssen Sie mit Administrator-Rechten angemeldet sein.

Führen Sie folgende Schritte durch, um die Benutzereinstellungen festzulegen:

1. Klicken Sie auf **Einstellungen** auf der allgemeinen Navigationsleiste.

   Die Startseite **Einstellungen** wird eingeblendet.

2. Klicken Sie auf **Allgemeine Einstellungen**.

3. Um einen vorausgewählten E-Mail-Empfänger hinzuzufügen, geben Sie die E-Mail-Adresse des festgelegten Dienstkontakts im Feld **Senden an:** ein und klicken auf **Änderungen übernehmen**.

   ANMERKUNG: Durch Klicken auf **E-Mail** wird eine E-Mail-Nachricht, an die eine HTML-Datei des Fensters angehängt ist, an die vorgegebene E-Mail-Adresse gesendet, und zwar von jedem Fenster aus.

4. Zum Ändern der Darstellung der Startseite wählen Sie einen anderen Wert in den Feldern **Skin** oder **Schema** und klicken Sie auf **Änderungen übernehmen**.

Führen Sie folgende Schritte durch, um die Secure Port-Server-Einstellungen festzulegen.

1. Klicken Sie auf **Einstellungen** auf der allgemeinen Navigationsleiste.

   Die Startseite **Einstellungen** wird eingeblendet.

2. Klicken Sie auf **Allgemeine Einstellungen** und auf das Register **Web- Server**.

3. Im Fenster **Servereinstellungen** stellen Sie die Optionen nach den Erfordernissen ein.

   - Mit der Funktion **Sitzungszeitüberschreitung** kann die Zeit begrenzt werden, in der eine Sitzung aktiv bleiben kann. Wählen Sie die Optionsschaltfläche **Aktivieren**, um eine Zeitüberschreitung zuzulassen, wenn für eine bestimmte Zeit (in Minuten) keine Benutzermaßnahme stattfindet. Benutzer, deren Sitzungszeit überschritten wurde, müssen sich erneut anmelden. Wählen Sie das Optionsschaltfläche **Deaktivieren**, um die Sitzungszeitüberschreitungsfunktion für Server Administrator zu deaktivieren.
   - Das Feld **HTTPS-Anschluss** bestimmt den sicheren Anschluss für den Server Administrator. Der sichere Standardanschluss für Server Administrator ist 1311.

   ANMERKUNG: Die Änderung der Anschlussnummer auf eine ungültige bzw. eine bereits belegte Anschlussnummer kann andere Anwendungen oder Browser beim Zugriff auf den Server Administrator auf dem verwalteten System behindern.

   - Das Feld **Zu bindende IP-Adresse** legt die IP-Adresse(n) für das Managed System fest, mit der sich der Server Administrator zu Beginn einer Sitzung verbindet. Wählen Sie die Optionsschaltfläche **Alle** zum Binden an alle für das System in Frage kommenden IP-Adressen. Wählen Sie die Optionsschaltfläche **Spezifisch** zum Binden an eine bestimmte IP-Adresse.

   ANMERKUNG: Benutzer mit Administrator-Berechtigungen können Server Administrator nicht verwenden, wenn sie im Remote-Zugriff bei dem System angemeldet sind.

   ANMERKUNG: Wenn der Wert für **IP-Adresse binden an** auf einen anderen Wert als **Alle** geändert wird, kann dies dazu führen, dass andere Anwendungen oder Browser im Remote-Zugriff nicht mehr auf den Server Administrator auf dem verwalteten System zugreifen können.

   - Die Felder **SMTP-Servername** und **DNS-Suffix für SMTP-Server** bestimmen das Suffix für das Simple Mail Transfer Protocol (SMTP) und den Domänennamenserver (DNS) einer Firma oder Organisation. Um für Server Administrator das Versenden von E-Mails zu aktivieren, müssen die IP-Adresse und das DNS-Suffix des SMTP-Servers für die Firma bzw. Organisation in die entsprechenden Felder eingeben werden.

   ANMERKUNG: Aus Sicherheitsgründen gestattet Ihre Firma eventuell nicht, dass E-Mails über den SMTP-Server an Empfänger außerhalb gesendet werden.

   - Im Feld **Befehlsprotokollumfang** wird der maximale Umfang (in MB) für die Befehlsprotokolldatei festgelegt.
   - Das Feld **Support-Link** enthält die Webadresse für das Geschäftsunternehmen, das die Unterstützung für das Managed System leistet.
   - Das Feld **Benutzerdefinierte Begrenzungszeichen** bestimmt das Zeichen, das zur Trennung der Datenfelder der Dateien verwendet wird, die durch die Schaltfläche **Exportieren** erstellt werden. Das Zeichen **;** ist das standardmäßige Begrenzungszeichen. Andere Optionen sind **!**, **@**, **#**, **$**, **%**, **^**, *****, **~**, **?**, **:**, **|** und **,**.

- Wenn Sie alle Einstellungen im Fenster **Servereinstellungen** vorgenommen haben, klicken Sie auf **Änderungen übernehmen**.

X.509-Zertifikatsverwaltung

Web-Zertifikate sind erforderlich zum Schutz der Identität eines Remote-Systems und damit sichergestellt werden kann, dass mit dem Remote-System ausgetauschte Informationen von anderen weder gesehen noch geändert werden können. Zur Gewährleistung der Systemsicherheit wird empfohlen, entweder ein neues X.509-Zertifikat zu erstellen, ein bestehendes wieder zu verwenden oder ein Stammzertifikat oder eine Stammzertifikatkette von einer Zertifizierungsstelle (CA) zu importieren.

ANMERKUNG: Für die Zertifikatsverwaltung müssen Sie mit Administrator-Zugriffsrechten angemeldet sein.

Sie können X.509-Zertifikate für Server Administrator und IT Assistant von der entsprechenden Webseite **Einstellungen** verwalten. Klicken Sie auf **Allgemeine Einstellungen**, dann auf das Register **Web Server** und anschließend auf **X.509-Zertifikat**. Verwenden Sie das X.509-Zertifikathilfsprogramm, um entweder ein neues X.509-Zertifikat zu erstellen, ein bestehendes wieder zu verwenden oder ein Stammzertifikat oder eine Stammzertifikatskette von einer CA zu importieren. Zu den Zertifizierungsstellen gehören Verisign, Entrust und Thawte.

Empfohlene Verfahren für die X.509-Zertifikatverwaltung

Um die Sicherheit des Systems während der Verwendung von Server Administrator nicht zu gefährden, sollten Sie Folgendes beachten:

- **Eindeutiger Host-Name**: Alle Systeme, auf denen Server Administrator installiert ist, sollten einen eindeutigen Host-Namen tragen.
- **Ändern von 'localhost' zu eindeutig**: Allen Systemen mit dem Host-Namen 'localhost' sollte ein eindeutiger Host-Name zugewiesen werden.

Zurück zum Inhaltsverzeichnis