

# Dell™ OpenManage™ Server Administrator Version 6.2 Benutzerhandbuch

[Einführung](#)

[Setup und Administration](#)

[Server Administrator verwenden](#)

[Dienste des Server Administrator](#)

[Arbeiten mit dem Remote Access Controller](#)

[Server Administrator-Protokolle](#)

[Warnungsmaßnahmen einstellen](#)

[Fehlerbehebung](#)

[Häufig gestellte Fragen](#)

---

## Anmerkungen und Vorsichtshinweise

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

 **VORSICHTSHINWEIS:** Ein VORSICHTSHINWEIS warnt vor möglichen Beschädigungen der Hardware oder vor Datenverlust und zeigt auf, wie derartige Probleme vermieden werden können.

---

**Irrtümer und technische Änderungen vorbehalten.  
© 2009 Dell Inc. Alle Rechte vorbehalten.**

Die Vervielfältigung oder Wiedergabe dieser Materialien in jeglicher Weise ohne vorherige schriftliche Genehmigung von Dell Inc. ist strengstens untersagt.

In diesem Text verwendete Marken: *Dell*, das *DELL*-Logo, *PowerEdge*, *PowerVault* und *OpenManage* sind Marken von Dell Inc.; *Microsoft*, *Windows*, *Internet Explorer*, *Active Directory*, *Windows Server* und *Windows NT* sind entweder Marken oder eingetragene Marken der Microsoft Corporation in den Vereinigten Staaten und/oder anderen Ländern; *Java* ist eine Marke oder eingetragene Marke von Sun Microsystems, Inc. in den USA und anderen Ländern; *Novell* und *SUSE* sind eingetragene Marken von Novell, Inc. in den Vereinigten Staaten und anderen Ländern; *Intel* und *Pentium* sind eingetragene Marken und *Intel386* ist eine Marke der Intel Corporation; *Red Hat* und *Red Hat Enterprise Linux* sind eingetragene Marken von Red Hat, Inc. in den Vereinigten Staaten und anderen Ländern; *UNIX* ist eine eingetragene Marke von The Open Group in den Vereinigten Staaten und anderen Ländern.

Server Administrator enthält Software, die von der Apache Software Foundation ([www.apache.org](http://www.apache.org)) entwickelt wurde. Server Administrator setzt die OverLIB JavaScript-Bibliothek ein. Diese Bibliothek ist unter [www.bosrup.com](http://www.bosrup.com) verfügbar.

Alle anderen in dieser Dokumentation genannten Marken und Handelsbezeichnungen sind Eigentum der entsprechenden Hersteller und Firmen. Dell Inc. erhebt keinen Anspruch auf Markenzeichen und Handelsbezeichnungen mit Ausnahme der eigenen.

Dezember 2009

[Zurück zum Inhaltsverzeichnis](#)

## Warnungsmaßnahmen einstellen

Dell™ OpenManage™ Server Administrator Version 6.2 Benutzerhandbuch

- [Einstellung von Warnungsmaßnahmen für Systeme, auf denen unterstützte Red Hat Enterprise Linux und SUSE Linux Enterprise Server-Betriebssysteme ausgeführt werden.](#)
- [Einstellen von Warnungsmaßnahmen bei Microsoft Windows Server 2003 und Windows Server 2008](#)
- [Einstellen von Warnungsmaßnahmen \(Anwendungsprogramm ausführen\) in Windows Server 2008](#)
- [Warnungsmeldungen der BMC/iDRAC- Plattformereignisfilter](#)
- [Service-Namen verstehen](#)

---

### Einstellung von Warnungsmaßnahmen für Systeme, auf denen unterstützte Red Hat Enterprise Linux und SUSE Linux Enterprise Server-Betriebssysteme ausgeführt werden.

Wenn Warnungsmaßnahmen für ein Ereignis eingestellt werden, kann die Maßnahme für **Warnung auf dem Server anzeigen** angegeben werden. Um diese Maßnahme auszuführen, schreibt Server Administrator eine Meldung an `/dev/Konsole`. Wenn auf Server Administrator-System X Window System ausgeführt wird, wird diese Meldung standardmäßig nicht angezeigt. Um eine Alarmmeldung auf einem Red Hat® Enterprise Linux®-System zu sehen, wenn X Window System ausgeführt wird, müssen Sie `xconsole` oder `xterm -C` starten, bevor das Ereignis eintritt. Um eine Alarmmeldung auf einem SUSE® Linux Enterprise-Server-System zu sehen, wenn X Window System ausgeführt wird, müssen Sie `xterm -C` starten, bevor das Ereignis eintritt.

Wenn Warnungsmaßnahmen für ein Ereignis eingestellt werden, kann die Maßnahme für **Broadcast-Meldung** angegeben werden. Um diese Maßnahme durchzuführen, führt der Server Administrator den Befehl `wall` aus, wodurch die Meldung an alle angemeldeten Benutzer gesendet wird, deren Meldungsberechtigung auf **Ja** eingestellt ist. Wenn auf Server Administrator-System X Window System ausgeführt wird, wird diese Meldung standardmäßig nicht angezeigt. Um die Broadcast-Meldung unter X Window System anzuzeigen, muss ein Terminal wie z. B. `xterm` oder `gnome-terminal` gestartet werden, bevor das Ereignis eintritt.

Wenn Warnungsmaßnahmen für ein Ereignis eingestellt werden, kann die Maßnahme für **Anwendungsprogramm ausführen** angegeben werden. Für die Anwendungen, die der Server Administrator ausführen kann, gelten Einschränkungen. Folgen Sie diesen Richtlinien, um eine ordnungsgemäße Ausführung zu gewährleisten:

- 1 Geben Sie keine X Window System-basierten Anwendungen an, da Server Administrator solche Anwendungen nicht ordnungsgemäß ausführen kann.
- 1 Geben Sie keine Anwendungen an, bei denen Eingaben durch den Benutzer erforderlich sind, da Server Administrator solche Anwendungen nicht ordnungsgemäß ausführen kann.
- 1 Leiten Sie `stdout` und `stderr` bei der Angabe der Anwendung in eine Datei um, sodass Ausgaben oder Fehlermeldungen angezeigt werden.
- 1 Wenn mehrere Anwendungen (oder Befehle) für eine Warnung ausgeführt werden sollen, erstellen Sie ein Skript, das diese Aufgabe übernimmt, und setzen Sie den vollständigen Pfad zum Skript im Feld **Absoluter Pfad zur Anwendung** ein.

Beispiel 1:

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

Der Befehl in Beispiel 1 führt die Anwendung `ps` aus, leitet `stdout` in die Datei `/tmp/psout.txt` um und leitet `stderr` in dieselbe Datei wie `stdout` um.

Beispiel 2:

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

Der Befehl in Beispiel 2 führt die Mail-Anwendung aus, um die Meldung in der Datei `/tmp/alertmsg.txt` mit dem Betreff **Serverwarnung** an den Red Hat Enterprise Linux-Benutzer oder SUSE LINUX Enterprise Server-Benutzer und Administrator zu senden. Die Datei `/tmp/alertmsg.txt` muss vom Benutzer erstellt werden, bevor das Ereignis eintritt. `stdout` und `stderr` können außerdem in die Datei `/tmp/mailout.txt` umgeleitet werden, falls ein Fehler eintritt.

---

### Einstellen von Warnungsmaßnahmen bei Microsoft Windows Server 2003 und Windows Server 2008

Beim Festlegen von Warnungsmaßnahmen werden Visual Basic-Skripts nicht automatisch von der Funktion "Anwendungsprogramm ausführen" interpretiert, obwohl Sie eine `.cmd`-, `.com`-, `.bat`- oder `.exe`-Datei ausführen können, indem Sie einfach nur die Datei als Warnungsmaßnahme angeben.

Um dieses Problem zu beheben, rufen Sie zuerst den Befehlsverarbeiter `cmd.exe` zum Starten des Skripts auf. Beispiel: Der Warnungsmaßnahmenwert zum Ausführen einer Anwendung kann folgendermaßen eingestellt werden:

```
c:\winnt\system32\cmd.exe /c d:\Beispiel\Beispiel1.vbs
```

Dabei ist `d:\Beispiel\Beispiel1.vbs` der vollständige Pfad zur Skriptdatei.

Stellen Sie keinen Pfad zu einer interaktiven Anwendung (eine Anwendung mit einer grafischen Benutzeroberfläche oder die Anwendereingaben erfordert) im Feld "Absoluter Pfad zur Anwendung" ein. Die interaktive Anwendung kann sich bei manchen Betriebssystemen auf unerwartete Weise verhalten.



**ANMERKUNG:** Es sollte der vollständige Pfad sowohl zur Datei "cmd.exe" als auch zur Skriptdatei angegeben werden.

## Einstellen von Warnungsmaßnahmen (Anwendungsprogramm ausführen) in Windows Server 2008

Aus Sicherheitsgründen ist Microsoft Windows Server 2008 so konfiguriert, dass keine interaktiven Dienste möglich sind. Wenn ein Dienst als interaktiver Dienst auf Microsoft Windows Server 2008 installiert ist, protokolliert das Betriebssystem eine Fehlermeldung über den als interaktiv markierten Dienst in das Windows-Systemprotokoll.

Wenn Sie Server Administrator zum Konfigurieren von Warnungsmaßnahmen für ein Ereignis verwenden, können Sie die Maßnahme "execute an application" ("Ausführen einer Anwendung") festlegen. Damit interaktive Anwendungen für eine Warnungsmaßnahme ordnungsgemäß ausgeführt werden können, muss der DSM SA-Datenverwaltungsservice (Dell Systems Management Server Administrator) als interaktiver Dienst konfiguriert werden. Zu Beispielen interaktiver Anwendungen zählen Anwendungen mit einer grafischen Benutzeroberfläche (GUI) oder Anwendungen, die den Benutzer auf die eine oder andere Weise zu einer Eingabe auffordern, wie z. B. des Befehls "pause" in einer Batch-Datei.

Wenn Server Administrator auf Microsoft Windows Server 2008 installiert wird, wird der DSM SA-Datenverwaltungsservice als nicht interaktiver Dienst installiert, was bedeutet, dass er so konfiguriert wird, dass er standardmäßig nicht mit dem Desktop interagieren darf. Dies bedeutet, dass interaktive Anwendungen nicht ordnungsgemäß ausgeführt werden können, wenn sie für eine Warnungsmaßnahme ausgeführt werden. Wenn in dieser Situation eine interaktive Anwendung für eine Warnungsmaßnahme ausgeführt wird, wird die Anwendung unterbrochen und wartet auf eine Eingabe. Die Schnittstelle/Eingabeaufforderung der Anwendung ist für Sie nicht sichtbar und bleibt selbst dann unsichtbar, nachdem der Dienst der Ermittlung interaktiver Dienste gestartet wurde. Das Register **Processes (Abläufe)** im **Task Manager** zeigt einen Anwendungsablauf-Eintrag für jede Ausführung der interaktiven Anwendung an.

Wenn Sie eine interaktive Anwendung für eine Warnungsmaßnahme auf Microsoft Windows Server 2008 ausführen müssen, müssen Sie den DSM SA-Datenverwaltungsservice so konfigurieren, dass er mit dem Desktop interagieren darf.

So erlauben Sie die Interaktion mit dem Desktop:

1. Klicken Sie mit der rechten Maustaste auf den DSM SA- Datenverwaltungsservice im **Fenster Services control (Dienststeuerung)** und wählen Sie **Properties (Eigenschaften)** aus.
2. Aktivieren Sie im Register **Log On (Anmelden)** die Option "Allow service to interact with desktop" ("Interaktion des Diensts mit Desktop zulassen") und klicken Sie auf **OK**.
3. Starten Sie den DSM SA-Datenverwaltungsservice neu, damit die Änderung wirksam wird.

Wenn der DSM SA-Datenverwaltungsservice mit dieser Änderung neu gestartet wird, protokolliert der Dienststeuerungsmanager die folgende Meldung in das Systemprotokoll: "The DSM SA-Datenverwaltungsservice is marked as an interactive service. However, the system is configured to not allow interactive services. This service may not function properly." ("Der DSM SA-Datenverwaltungsservice ist als interaktiver Dienst markiert. Das System ist jedoch dahingehend konfiguriert, dass es keine interaktiven Dienste zulässt. Dieser Dienst wird eventuell nicht richtig funktionieren.") Durch diese Änderung wird dem DSM SA-Datenverwaltungsservice erlaubt, interaktive Anwendungen für eine Warnungsmaßnahme ordnungsgemäß auszuführen. Stellen Sie außerdem sicher, dass der Dienst der Ermittlung interaktiver Dienste ausgeführt wird, damit Sie die Schnittstelle/Eingabeaufforderung sehen können, die von der interaktiven Anwendung angezeigt wird. Sobald diese Änderungen vorgenommen wurden, wird das Dialogfeld **Interactive services dialog detection (Ermittlung eines Dialogs interaktiver Dienste)** durch das Betriebssystem angezeigt, um Zugriff auf die interaktive Anwendungsschnittstelle/Eingabeaufforderung zu bieten.

## Warnungsmeldungen der BMC/iDRAC- Plattformereignisfilter

Eine Liste aller möglichen Plattformereignisfilter-(PEF-)Meldungen und die Beschreibung des jeweiligen Ereignisses finden Sie in [Tabelle 7-1](#).

**Tabelle 7-1. PEF-Warnungsereignisse**

Ereignis	Beschreibung
Lüftersondenfehler	Der Lüfter läuft zu langsam oder gar nicht.
Spannungssonden-Fehler	Die Spannung reicht für einen ordnungsgemäßen Betrieb nicht aus.
Diskreter Spannungssondenfehler	Die Spannung reicht für einen ordnungsgemäßen Betrieb nicht aus.
Temperatursondenwarnung	Die Temperatur geht auf den oberen bzw. unteren Grenzwert zu.
Temperatursondenfehler	Die Temperatur ist für einen ordnungsgemäßen Betrieb zu hoch oder zu niedrig.
Gehäuseeingriff festgestellt	Das Systemgehäuse wurde geöffnet.
Redundanz (Netzteil oder Lüfter) herabgesetzt	Redundanz der Lüfter bzw. Netzteile wurde herabgesetzt.
Redundanz (Netzteil oder Lüfter) verloren	Keine Redundanz mehr für die Lüfter bzw. Netzteile des Systems vorhanden.
Prozessorwarnung	Ein Prozessor läuft unter seiner Spitzenleistung bzw. Taktrate.
Prozessorfehler	Ein Prozessor ist fehlerhaft.
PPS/VRM/DCtoDC-Warnung	Das Netzteil, das Spannungsreglermodul oder der DC/DC-Konverter steht vor einem Ausfall.
Netzteil/VRM/D2D-Fehler	Das Netzteil, das Spannungsreglermodul oder DC/DC-Konverter ist fehlerhaft.
Hardwareprotokoll ist voll oder wurde geleert	Ein leeres oder volles Hardwareprotokoll erfordert die Aufmerksamkeit des Administrators.
Automatische Systemwiederherstellung	Das System hängt bzw. reagiert nicht, und es werden von der automatischen Systemwiederherstellung konfigurierte Maßnahmen getroffen.
Systemstromsondenwarnung	Die Leistungsaufnahme nähert sich dem Fehlerschwellenwert.
Systemstromsondenfehler	Die Leistungsaufnahme hat die höchstzulässige Stufe überschritten, was zu einem Fehler führte.
Wechselbarer Flash Datenträger vorhanden	Der wechselbare Flash-Datenträger ist vorhanden.
Wechselbarer Flash Datenträgerfehler	Für den wechselbaren Flash-Datenträger steht ein Fehlerzustand an.

## Service-Namen verstehen

Die ausführbare Service-Datei und die Anzeigenamen der folgenden Services haben sich geändert:

Tabelle 7-2. **Service-Namen**

Zweck	Service-Name	Vorhergehende Version (älter als 5.0)	Aktuelle Version
<b>Web-Server</b>	Anzeigenname	Sicherer Anschluss Server	DSM SA-Verbindungsdienst
	Name der ausführbaren Datei	Omaaws [32 64]	dsm_om_connsvc
			dsm_om_connsvc
<b>Planung oder Benachrichtigung</b>	Anzeigenname	OM Common Services	DSM SA-Freigabedienste
	Name der ausführbaren Datei	Omsad [32 64]	dsm_om_shrsvc
			dsm_om_shrsvc

---

[Zurück zum Inhaltsverzeichnis](#)

[Zurück zum Inhaltsverzeichnis](#)

## Fehlerbehebung

Dell™ OpenManage™ Server Administrator Version 6.2 Benutzerhandbuch

- [Anmeldefehler-Szenarien](#)
- [Reparieren einer fehlerhaften Server Administrator-Installation auf einem unterstützten Windows-Betriebssystem](#)
- [OpenManage Server Administrator-Dienste](#)

---

### Anmeldefehler-Szenarien

Eine Anmeldung beim Managed System kann in folgenden Situationen fehlschlagen:

1. Eingabe einer **ungültigen/falschen IP-Adresse**.
1. Eingabe **falscher Anmeldeinformationen** (Benutzername und Kennwort).
1. Das Managed System ist nicht eingeschaltet.
1. Das Managed System ist aufgrund einer ungültigen IP-Adresse oder eines DNS-Fehlers nicht erreichbar.
1. Das Managed System weist ein nicht vertrauenswürdigen Zertifikat auf und Sie wählen auf der Anmeldeseite nicht **Ignore Certificate Warning (Zertifikatswarnung ignorieren)** aus.
1. Die Server Administrator-Dienste sind auf dem VMware ESXi 3.5-System nicht aktiviert. Im *Installationshandbuch zu Dell OpenManage Server Administrator* finden Sie Informationen darüber, wie Server Administrator-Dienste auf dem VMware ESXi 3.5-System aktiviert werden.
1. Der SFCBD-Dienst (small footprint CIM broker daemon) des VMware ESXi 3.5-Systems wird nicht ausgeführt.
1. Der Web Server-Verwaltungsdienst auf dem verwalteten System wird nicht ausgeführt.
1. Sie geben die IP-Adresse des verwalteten Systems und nicht den Hostnamen ein und markieren das Kontrollkästchen **Zertifikatswarnung ignorieren** nicht.
1. Die WinRM-Autorisierungsfunktion (Remoteaktivierung) ist auf dem verwalteten System nicht konfiguriert. Informationen zu dieser Funktion finden Sie im *Installationshandbuch zu Dell OpenManage Server Administrator*.

---

### Reparieren einer fehlerhaften Server Administrator-Installation auf einem unterstützten Windows-Betriebssystem

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

So erzwingen Sie eine Neuinstallation:

1. Bringen Sie in Erfahrung, welche Version von Server Administrator zuvor installiert wurde.
2. Laden Sie das Installationspaket für diese Version von der Dell™ Support- Website unter [support.dell.com](http://support.dell.com) herunter.
3. Machen Sie **SysMgmt.msi** vom Verzeichnis **srvadmin\windows\SystemManagement** ausfindig.
4. An der Befehlseingabeaufforderung geben Sie den folgenden Befehl ein, um eine Neuinstallation zu erzwingen.  

```
msiexec /i SysMgmt.msi REINSTALL=ALL REINSTALLMODE=vamus
```
5. Wählen Sie **Benutzerdefiniertes Setup** und alle Funktionen, die ursprünglich installiert wurden. Wenn Sie nicht sicher sind, welche Funktionen installiert wurden, wählen Sie alle Funktionen aus und führen Sie die Installation aus.

 **ANMERKUNG:** Wenn Sie Server Administrator in einem Nichtstandardverzeichnis installiert haben, stellen Sie sicher, dass es auch in **Benutzerdefiniertes Setup** geändert wird.

6. Sobald die Anwendung installiert ist, können Sie Server Administrator mithilfe von Software deinstallieren.

---

### OpenManage Server Administrator-Dienste

Diese Tabelle führt die von Server Administrator verwendeten Dienste zur Bereitstellung von Systemverwaltungsinformationen sowie die Folgen eines Ausfalls dieser Dienste auf.

--	--	--	--	--

Service-Name	Beschreibung	Fehlerwirkung	Wiederherstellungsmechanismus	Severity
Windows: DSM SA Verbindungsdiens Linux: dsm_om_connsvc  (Dieser Dienst wird mit dem Server Administrator Web Server installiert.)	Bietet Remote-/lokalen Zugriff auf Server Administrator von beliebigen Systemen mit einem unterstützten Internet-Browser und einer unterstützten Netzwerkverbindung aus.	Benutzer können sich nicht bei Server Administrator anmelden und über die Web-Benutzeroberfläche beliebige Funktionen ausführen. CLI kann jedoch nach wie vor verwendet werden.	Neustart-Service	Kritisch
<b>Allgemeiner Service</b>				
Windows: DSM SA freigegeben  Dienste Linux: dsm_om_shrsvc  (Dieser Dienst wird auf dem Managed System ausgeführt.)	Legt beim Start eine Bestandsaufnahme der Systemsoftware an, über die SNMP- und CIM-Anbieter von Server Administrator eine Remote-Softwareaktualisierung mithilfe der Dell System Management Console und des Dell IT Assistant (ITA) durchführen.	Softwareaktualisierungen sind nicht mit dem ITA möglich. Jedoch können die Aktualisierungen lokal und außerhalb von Server Administrator mithilfe einzelner Dell Update-Pakete durchgeführt werden. Aktualisierungen können nach wie vor mit Hilfsprogrammen von Drittanbietern (z. B. MSSMS, Altiris und Novell ZENworks) durchgeführt werden.	Neustart-Service	Warnung
<b>Instrumentation Service</b>				
DSM SA-Datenmanager Linux: dsm_sa_datamgrd  (im Service dataeng gehostet)  (Dieser Dienst wird auf dem Managed System ausgeführt.)	Überwacht das System, bietet schnellen Zugriff auf detaillierte Fehler- und Leistungsinformationen und erlaubt Remote-Verwaltung auf überwachten Systemen, einschließlich Herunterfahren, Start und Sicherheit.	Benutzer können die Einzelheiten der Hardware-Ebene auf der GUI/CLI ohne diese ausführenden Dienste nicht konfigurieren/ ansehen.	Neustart-Service	Kritisch
DSM SA-Ereignismanager Linux: dsm_sa_eventmgrd  (im Service dataeng gehostet)  (Dieser Dienst wird auf dem Managed System ausgeführt.)	Bietet einen Service zur Ereignisprotokollierung von Betriebssystemen und Dateien für die Systemverwaltung und wird auch von Ereignisprotokollanalytikern verwendet.	Wenn dieser Service beendet wird, werden die Funktionen der Ereignisprotokollierung nicht einwandfrei funktionieren.	Neustart-Service	Warnung
Linux: dsm_sa_snmpd  (im Service dataeng gehostet)  (Dieser Dienst wird auf dem Managed System ausgeführt.)	Data Engine-SNMP von Linux  Schnittstelle	SNMP Get/Set/Trap-Anforderung funktioniert nicht auf einer Management Station.	Neustart-Service	Kritisch
<b>Storage Management-Dienst</b>				
Windows: mr2kserv (Dieser Dienst wird auf dem Managed System ausgeführt.)	Der Speicherverwaltungsservice gibt Auskunft über die Speicherverwaltung und erweiterte Funktionen zur Konfiguration eines lokalen oder Remote-Speichers, der mit einem System verbunden ist.	Benutzer kann keine Speicherfunktionen für alle unterstützten RAID- und Nicht-RAID-Controller ausführen.	Neustart-Service	Kritisch

[Zurück zum Inhaltsverzeichnis](#)

## Häufig gestellte Fragen

### Dell™ OpenManage™ Server Administrator Version 6.2 Benutzerhandbuch

In diesem Abschnitt werden die häufig gestellten Fragen zu OpenManage™ Server Administrator aufgelistet:



**ANMERKUNG:** Diese Fragen beziehen sich nicht ausschließlich auf die vorliegende Version von Server Administrator.

1. **Welche Berechtigungsebene muss ein Benutzer mindestens haben, um Server Administrator zu installieren?**

Um Server Administrator installieren zu können, müssen Sie mindestens über die Berechtigungsebene des **Administrators** verfügen. Hauptbenutzer und reguläre Benutzer haben keine Berechtigung, Server Administrator zu installieren.

2. **Ist ein Upgrade-Pfad erforderlich, um Server Administrator zu installieren?**

Für Systeme der Version 4.3 ist kein Upgrade-Pfad erforderlich. Für Systeme, die eine ältere Version als 4.3 aufweisen, müssen Sie zuerst ein Upgrade auf Version 4.3 durchführen und im Anschluss daran ein Upgrade auf Version 5.x (wobei x für die Version von Server Administrator steht, auf die erweitert werden soll).

3. **Wie kann ich feststellen, welches die aktuellste Version von Server Administrator ist, die für mein System erhältlich ist?**

Melden Sie sich bei [support.dell.com](http://support.dell.com) → **Product Support (Produktsupport)** → **Manuals (Handbücher)** → **Software** → **Systems Management** → **Dell OpenManage Server Administrator** an.

Die neuste Dokumentationsversion zeigt die Version von OpenManage Server Administrator an, die Ihnen zur Verfügung steht.

4. **Wie kann ich feststellen, welche Version von Server Administrator auf meinem System ausgeführt wird?**

Nachdem Sie sich bei Server Administrator angemeldet haben, wechseln Sie zu **Properties (Eigenschaften)** → **Summary (Zusammenfassung)**. Die auf Ihrem System installierte Version von Server Administrator wird in der Spalte **Systemverwaltung** angezeigt.

5. **Gibt es noch andere Schnittstellen außer 1311, die Benutzer verwenden können?**

Ja, Sie können Ihren bevorzugten https-Anschluss einrichten. Navigieren Sie zu **Voreinstellungen** → **Allgemeine Einstellungen** → **Web Server** → **HTTPS-Anschluss**

Klicken Sie statt auf **Standardeinstellung verwenden** auf die Optionsschaltfläche **Verwenden, um Ihren bevorzugten Anschluss festzulegen**.

Die Änderung der Schnittstellenummer zu einer ungültigen bzw. einer bereits belegten Schnittstellenummer kann andere Anwendungen oder Browser beim Zugriff auf den Server Administrator auf dem verwalteten System behindern. Eine Liste der Standardschnittstellen erhalten Sie im *Dell OpenManage-Installations- und Sicherheitsbenutzerhandbuch*.

6. **Kann ich Server Administrator auf Fedora, College Linux, Mint, Ubuntu, Sabayon oder PCLinux installieren?**

Nein, Server Administrator unterstützt keines dieser Betriebssysteme.

7. **Kann Server Administrator beim Auftreten eines Problems E-Mails senden?**

Nein, Server Administrator ist nicht dafür eingerichtet, bei Problemen E-Mails auszusenden.

8. **Ist SNMP für die ITA-Ermittlung, die Bestandsaufnahme und Software- Aktualisierungen auf PowerEdge™-Systemen erforderlich? Kann CIM für Ermittlung, Bestandsaufnahme und Aktualisierungen alleine verwendet werden oder ist SNMP erforderlich?**

*ITA-Kommunikation mit Linux-Systemen:*

SNMP ist auf dem Linux-System für Ermittlung, Statusabfrage und Bestandsaufnahme erforderlich.

Dell-Softwareaktualisierungen werden über eine SSH-Sitzung und ein sicheres FTP vorgenommen. Für diese separate Maßnahme sind Berechtigungen/Anmeldeinformationen auf Stammebene erforderlich, die dann eingegeben werden müssen, wenn die Maßnahme eingerichtet oder angefordert wird. Anmeldeinformationen aus dem Ermittlungsbereich werden nicht vorausgesetzt.

*ITA-Kommunikation mit Windows-Systemen:*

Für Server (Systeme, die Windows Server-Betriebssysteme ausführen), kann das System entweder mit SNMP oder CIM oder beidem zur Ermittlung durch ITA konfiguriert werden. Bestandsaufnahme erfordert CIM.

Softwareaktualisierungen, wie bei Linux, stehen nicht mit Ermittlung, Abfrage und den verwendeten Protokollen in Verbindung.

Unter Verwendung der Anmeldeinformationen auf Administratorebene, die zum Zeitpunkt der Aktualisierungsplanung oder -ausführung angefordert werden, wird eine administrative (Laufwerk-) Freigabe auf ein Laufwerk des Zielsystems eingerichtet, und Dateien werden von einem beliebigen Speicherort (eventuell eine andere Netzwerkfreigabe) auf das Zielsystem kopiert. Daraufhin werden WMI-Funktionen aufgerufen, um die Softwareaktualisierung auszuführen.

Für Clients/Workstations wird Server Administrator nicht installiert. Die CIM-Ermittlung wird daher verwendet, wenn das Zielsystem die OpenManage Client Instrumentation ausführt.

Für viele andere Geräte, wie z. B. Netzwerkdrucker, kommuniziert SNMP weiterhin standardmäßig mit dem Gerät bzw. ermittelt es in erster Linie.

Geräte wie EMC-Speicher haben proprietäre Protokolle. Bestimmte Informationen zu dieser Umgebung können über die Schnittstellen gesammelt werden, die in den Tabellen der OpenManage-Dokumentation aufgeführt sind.

**9. Gibt es Pläne für SNMP-v3-Unterstützung?**

Nein, in dieser Version ist keine SNMP-v3-Unterstützung geplant.

**10. Verursacht ein Unterstreichungszeichen im Domainname Probleme bei der Anmeldung bei Server Admin?**

Ja, ein Unterstreichungszeichen im Domainname ist ungültig. Auch alle anderen Sonderzeichen (außer dem Bindestrich) sind ungültig. Es sind ausschließlich Buchstaben und Zahlen zu verwenden, bei denen nicht zwischen Groß- und Kleinschreibung unterschieden wird.

**11. Welchen Einfluss hat das Markieren/Aufheben der Markierung von 'Active Directory' auf der Anmeldungsseite auf Berechtigungssebenen?**

Wenn Sie das Kontrollkästchen Active Directory nicht auswählen, haben Sie nur den Zugriff, der im Microsoft Active Directory konfiguriert ist. Sie können sich nicht mit der Dell Extended Schema Solution bei Microsoft® Active Directory anmelden. Diese Lösung ermöglicht Ihnen, Zugriff auf Server Administrator zu gewähren. Sie können damit Server Administrator-Benutzer und -Berechtigungen zu bestehenden Benutzern in Ihrer Active Directory-Software hinzufügen bzw. steuern. Weitere Informationen finden Sie unter "Microsoft Active Directory verwenden" im *Installationshandbuch zu Dell OpenManage Server Administrator*.

---

[Zurück zum Inhaltsverzeichnis](#)

[Zurück zum Inhaltsverzeichnis](#)

## Dienste des Server Administrator

Dell™ OpenManage™ Server Administrator Version 6.2 Benutzerhandbuch

- [Systemverwaltung](#)
- [System-/Servermodul-Strukturobjekte verwalten](#)
- [Server Administrator-Homepage- Systemstrukturobjekte](#)
- [Voreinstellungen verwalten: Konfigurationsoptionen der Startseite](#)

---

## Übersicht

Der Dell™ OpenManage™ Server Administrator Instrumentation Service überwacht den Funktionszustand eines Systems und gewährt schnellen Zugriff auf detaillierte Fehler- und Leistungsinformationen, die von marktüblichen Systemverwaltungsagenten gesammelt werden. Die Berichts- und Ansichtsfunktionen ermöglichen den Abruf des Gesamtfunktionszustands für jedes der Gehäuse, aus denen das System besteht. Auf der Subsystemebene kann man Informationen über Spannungen, Temperaturen, Lüftergeschwindigkeit und Speicherfunktion an den wichtigsten Punkten des Systems anzeigen. Eine detaillierte Beschreibung aller Einzelheiten zu den relevanten Betriebskosten (COO) des Systems ist in einer Zusammenfassung einsehbar. Die Versionsinformationen für BIOS, Firmware, Betriebssystem und installierte Systems Management Software können einfach abgerufen werden.

Ferner können System-Administratoren den Instrumentation Service zur Ausführung der folgenden wesentlichen Tasks verwenden:

- 1 Festlegung der Höchst- und Mindestwerte für bestimmte kritische Komponenten. Diese Werte, Schwellenwerte genannt, bestimmen den Bereich, in dem ein Warnungsereignis für die betreffende Komponente auftritt (Mindest- und Höchstausfallwerte werden vom Hersteller des Systems festgelegt).
- 1 Festlegung der Systemreaktion bei Auftreten eines Warnungs- oder Ausfallereignisses. Benutzer können die Maßnahmen konfigurieren, die ein System als Reaktion auf Benachrichtigungen über Warnungs- und Ausfallereignisse ergreift. Andererseits können Benutzer mit permanenter Überwachung festlegen, dass keine Maßnahmen zu ergreifen sind, und sich auf das menschliche Urteil über die beste Reaktion auf ein Ereignis verlassen.
- 1 Bestücken aller der benutzerfestlegbaren Werte für das System, z. B. Systemname, Telefonnummer des primären Systembenutzers, Abschreibungsmethode, ob das System gemietet oder gekauft ist, usw.

 **ANMERKUNG:** Sie müssen den SNMP-Dienst (einfaches Netzwerkverwaltungsprotokoll) konfigurieren, um SNMP-Pakete sowohl für verwaltete Systeme als auch für Netzwerk-Management Stations akzeptieren zu können, die Microsoft® Windows Server® 2003 ausführen. Näheres erfahren Sie im Abschnitt "[SNMP-Agenten für Systeme konfigurieren, auf denen unterstützte Windows-Betriebssysteme ausgeführt werden](#)".

---

## Systemverwaltung

Die Startseite von Server Administrator wird automatisch auf der Ansicht des **Systemobjekts** der Systemstrukturansicht geöffnet. Die Standardeinstellung für das **Systemobjekt** öffnet die **Zustandskomponenten** im Register **Eigenschaften**.

Die Startseite **Preferences (Einstellungen)** zeigt standardmäßig auf das Fenster **Access Configuration (Zugriffskonfiguration)** im Register **Preferences (Einstellungen)**.

Auf der Startseite **Voreinstellungen** können Sie den Zugriff auf Benutzer mit Benutzer- und Hauptbenutzerberechtigungen einschränken, das SNMP-Kennwort festlegen und Benutzer- und DSM SA-Verbindungsdienst-Einstellungen konfigurieren.

 **ANMERKUNG:** Kontextbezogene Onlinehilfe ist verfügbar für jedes Fenster der Homepage des Server Administrators. Durch Klicken auf **Hilfe** auf der allgemeinen Navigationsleiste wird ein unabhängiges Hilfefenster geöffnet, das detaillierte Informationen über das betrachtete Fenster enthält. Die Onlinehilfe ist darauf ausgelegt, Sie durch die spezifischen Maßnahmen zu leiten, die zur Ausführung aller Aspekte des Server Administrator-Dienstes erforderlich sind. Onlinehilfe ist verfügbar für alle Fenster, die angesehen werden können, basierend auf den Software- und Hardwaregruppen, die der Server Administrator auf dem System feststellt, und dem Benutzer-Zugriffsrecht.

 **ANMERKUNG:** Admin- oder Hauptbenutzer-Berechtigungen sind zur Ansicht vieler der konfigurierbaren Systemstrukturobjekte, Systemkomponenten, Maßnahmenregister oder Datenbereichsfunktionen erforderlich. Darüber hinaus haben nur Benutzer, die mit Administrator-Rechten angemeldet sind, Zugriff auf kritische Systemfunktionen wie die Herunterfahren-Funktion im Register **Herunterfahren**.

---

## System-/Servermodul-Strukturobjekte verwalten

Die Systemstruktur von Server Administrator zeigt alle sichtbaren Systemobjekte basierend auf den Software- und Hardwaregruppen an, die Server Administrator auf dem verwalteten System feststellt, und auf den Zugriffsrechten der Benutzer. Die Systemkomponenten sind nach Komponententyp kategorisiert. Beim Erweitern des Hauptobjekts- "[Modulares Gehäuse](#)"- "[System-/Servermodul](#)"-sind die Hauptkategorien an Systemkomponenten, die möglicherweise angezeigt werden, "[Hauptsystemgehäuse/Hauptsystem](#)", "[Software](#)" und "[Lagerung](#)."

Wenn der Storage Management Service installiert ist, erweitert sich abhängig vom Controller und Speicher, die am System angeschlossen sind, das Speicherstrukturobjekt, um verschiedene Objekte anzuzeigen.

Detaillierte Informationen zur Storage Management Service-Komponente finden Sie im *Benutzerhandbuch zu Dell OpenManage Server Administrator Storage Management* auf der Dell Support-Website unter [support.dell.com/manuals](http://support.dell.com/manuals).

---

## Server Administrator-Homepage- Systemstrukturobjekte

## Nicht unterstützte Funktionen von OpenManage Server Administrator

Wegen der Einschränkungen des Betriebssystems VMware ESXi Version 3.5 und 4.0 sind einige der vormals verfügbaren Funktionen von OpenManage Server Administrator bei dieser Version nicht mehr verfügbar. Dies sind:

### Nicht unterstützte Funktionen auf ESXi 3.5

- 1 Warnungsverwaltung - Warnungsmaßnahmen
- 1 Warnungsverwaltung - SNMP-Traps
- 1 BIOS-Setup - Startreihenfolge (*xx1x-Systeme*)
- 1 BIOS-Setup - TPM-Sicherheit (Trusted Platform Module)
- 1 Netzwerkschnittstelle - Verwaltungsstatus
- 1 Netzwerkschnittstelle - DMA
- 1 Netzwerkschnittstelle - IP-Adresse
- 1 Netzwerkschnittstelle - MAC-Adresse
- 1 Netzwerkschnittstelle - Maximale Übertragungseinheit
- 1 Netzwerkschnittstelle - Betriebsstatus
- 1 Energieverwaltung - Profile (*xx1x-Systeme*)
- 1 Voreinstellungen - SNMP-Konfiguration
- 1 Prozessoren - Leistungsfähigkeit - DBS (Demand Based Switching) (*xx1x-Systeme*)
- 1 Remote-Herunterfahren - Ein-/Ausschalten mit vorherigem Herunterfahren des BS
- 1 Zu Details - Details zu den Server Administrator-Komponenten, die nicht unter dem Register Details aufgeführt sind

### Nicht unterstützte Funktionen auf ESXi 4.0

- 1 Warnungsverwaltung - Warnungsmaßnahmen
- 1 Netzwerkschnittstelle - Verwaltungsstatus
- 1 Netzwerkschnittstelle - DMA
- 1 Netzwerkschnittstelle - IP-Adresse
- 1 Netzwerkschnittstelle - Maximale Übertragungseinheit
- 1 Netzwerkschnittstelle - Betriebsstatus
- 1 Voreinstellungen - SNMP-Konfiguration
- 1 Remote-Herunterfahren - Ein-/Ausschalten mit vorherigem Herunterfahren des BS
- 1 Zu Details - Details zu den Server Administrator-Komponenten, die nicht unter dem Register Details aufgeführt sind

 **ANMERKUNG:** Server Administrator zeigt das Datum stets im Format <MM/TT/JJJJ> an.

 **ANMERKUNG:** Admin- oder Hauptbenutzer-Zugriffsrechte sind zur Ansicht vieler der konfigurierbaren Systemstrukturobjekte, Systemkomponenten, Maßnahmenregister oder Datenbereichsfunktionen erforderlich. Darüber hinaus haben nur Benutzer, die mit Administrator-Rechten angemeldet sind, Zugriff auf kritische Systemfunktionen wie die Herunterfahren-Funktion im Register **Herunterfahren**.

## Modulares Gehäuse

 **ANMERKUNG:** Für die Zwecke von Server Administrator bezieht sich "modulares Gehäuse" auf ein System, das möglicherweise ein oder mehrere modulare Systeme enthält, die in der Systemstruktur als ein separates Servermodul angezeigt werden. Wie ein eigenständiges Servermodul enthält ein modulares Gehäuse alle wichtigen Komponenten eines Systems. Der einzige Unterschied besteht darin, dass es in einem größeren Container Steckplätze für mindestens zwei Servermodule gibt. Jedes Modul ist ein genauso komplettes System wie ein Servermodul.

Um die Gehäuseinformationen des modularen Systems und die CMC-Informationen (Chassis Management Controller) anzuzeigen, klicken Sie auf das Objekt **Modular Enclosure (modulares Gehäuse)**.

#### Eigenschaften

##### Unterregister: Informationen

Im Register **Eigenschaften** können Sie Folgendes durchführen:

- 1 Die Gehäuseinformationen für das modulare System anzeigen, das überwacht wird.
- 1 Detaillierte CMC-Informationen für das modulare System anzeigen, das überwacht wird.

### Chassis Management Controller (CMC) aufrufen und verwenden

So stellen Sie eine Verknüpfung zum Fenster **Log in (Anmelden)** des Chassis Management Controllers über die Startseite des Server Administrator her:

1. Klicken Sie auf das Objekt **Modular Enclosure (modulares Gehäuse)**.
2. Klicken Sie auf das Register **CMC Information (CMC-Informationen)** und dann auf **Launch the CMC Web Interface (CMC-Web-Schnittstelle starten)**. Das CMC-Fenster **Log in (Anmelden)** wird angezeigt.

Sie können Ihr modulares Gehäuse nach dem Herstellen einer Verbindung zum CMC überwachen und verwalten.

## System-/Servermodul

Das Objekt **System-/Servermodul** enthält drei Hauptsystemkomponentengruppen: "[Hauptsystemgehäuse/Hauptsystem](#)", "[Software](#)" und "[Lagerung](#)". Die Startseite von Server Administrator zeigt standardmäßig das **System**-Objekt der Systemstruktur an. Die meisten Verwaltungsfunktionen können vom Maßnahmenfenster des Objekts **System-/Servermodul** getätigt werden. Das Maßnahmenfenster des Objekts **System-/Servermodul** weist abhängig von den Berechtigungen der Benutzergruppe folgende Register auf: **Eigenschaften**, **Herunterfahren**, **Protokolle**, **Warnungsverwaltung** und **Sitzungsverwaltung**.

-  **ANMERKUNG:** Die Aktualisierungsfunktion wird bei Server Administrator Version 2.0 oder niedriger unterstützt. Die Dell™ Server Update Utility und Dell Update Packages können von der Dell Support-Webseite unter [support.dell.com](http://support.dell.com) heruntergeladen werden. Diese werden auf den Betriebssystemen Microsoft Windows®, Red Hat® Enterprise Linux® und SUSE® Linux Enterprise Server unterstützt.
-  **ANMERKUNG:** Das Server-Aktualisierungsdienstprogramm von Dell oder Aktualisierungspakete von Dell müssen von dem System gestartet werden, das Sie aktualisieren möchten.

### Eigenschaften

Unterregister: [Funktionszustand](#) | [Zusammenfassung](#) | [Bestandsinformationen](#) | [Autom. Wiederherstellung](#)

Im Register **Eigenschaften** können Sie Folgendes durchführen:

- 1 Den aktuellen Warnungsfunktionszustand für Hardware- und Softwarekomponenten im Objekt **Hauptsystemgehäuse/Hauptsystem** und das Objekt **Speicher** anzeigen.
  - 1 Die detaillierten Zusammenfassungen für alle Komponenten im überwachten System anzeigen.
  - 1 Die Bestandsinformationen für das überwachte System anzeigen und konfigurieren.
  - 1 Die automatischen Systemwiederherstellungsmaßnahmen (OS-Watchdog-Zeitgeber) für das überwachte System anzeigen und einstellen.
-  **ANMERKUNG:** Automatische Systemwiederherstellungsoptionen sind möglicherweise nicht verfügbar, da der Watchdog-Zeitgeber des Betriebssystems in BIOS aktiviert ist. Um die automatischen Wiederherstellungsoptionen zu konfigurieren, muss der Watchdog-Zeitgeber des Betriebssystems deaktiviert sein.
  -  **ANMERKUNG:** Automatische Systemwiederherstellungsmaßnahmen werden eventuell nicht genau pro eingestellter Zeitüberschreitungperiode (in Sekunden) ausgeführt, wenn der Watchdog ein System identifiziert, das nicht antwortet. Der Maßnahmen-Ausführungszeitraum erstreckt sich von  $n-h+1$  bis  $n+1$  Sekunden, wobei  $n$  die Zeitüberschreitungperiode und  $h$  das Heartbeat-Intervall darstellt. Der Wert des Heartbeat-Intervalls beträgt 7 Sekunden, wenn  $n < 30$  ist, und 15 Sekunden, wenn  $n > 30$  ist.
  -  **ANMERKUNG:** Die Funktionalität der Watchdog-Zeitgeberfunktion kann in einem Fall, wo ein nicht behebbares Speicherereignis im System DRAM Bank\_1 auftritt, nicht garantiert werden. Wenn an diesem Ort ein nicht behebbares Speicherereignis auftritt, ist es möglich, dass der BIOS-Code-Resident an dieser Stelle beschädigt wird. Da die Watchdog-Funktion einen Aufruf zu BIOS verwendet, um das Herunterfahren- oder Neustartverhalten zu beeinflussen, läuft die Funktion eventuell nicht richtig. Wenn dies eintritt, müssen Sie das System manuell neu starten.

### Herunterfahren

Unterregister: [Remote-Herunterfahren](#) | [Temperaturbedingtes Herunterfahren](#) | [Web Server herunterfahren](#)

Im Register **Herunterfahren** können Sie Folgendes durchführen:

- 1 Die Optionen zum Herunterfahren und Remote-Herunterfahren des Betriebssystems konfigurieren.
  - 1 Die Schweregradstufe des temperaturbedingten Herunterfahrens, dass das System herunterfährt, wenn ein Temperatursensor eine Warnung oder einen Fehlerwert zurückgibt, einstellen.
-  **ANMERKUNG:** Ein temperaturbedingtes Herunterfahren erfolgt nur dann, wenn die vom Sensor gemeldete Temperatur über dem Temperaturschwellenwert liegt. Ein temperaturbedingtes Herunterfahren erfolgt nicht, wenn die vom Sensor gemeldete Temperatur unter dem Temperaturschwellenwert liegt.
- 1 Fahren Sie den DSM SA-Verbindungsdienst (Web Server) herunter.
-  **ANMERKUNG:** Server Administrator ist auch dann noch verfügbar und verwendet die Befehlszeilenoberfläche (CLI), wenn der DSM SA-Verbindungsdienst heruntergefahren ist. Die CLI-Funktionen erfordern nicht, dass der DSM SA-Verbindungsdienst ausgeführt wird.

### Protokolle

Unterregister: [Hardware](#) | [Warnung](#) | [Befehl](#)

Im Register **Protokolle** können Sie Folgendes durchführen:

- 1 Das Protokoll für die integrierte Systemverwaltung (ESM) oder das Systemereignisprotokoll (SEL) auf einer Liste aller mit den Hardwarekomponenten des Systems verbundenen Ereignissen anzeigen. Das Statusanzeigesymbol neben dem Protokoll-Namen wird sich von normalem Status (  ) zu nichtkritischem Status (  ) ändern, wenn die Protokolldatei 80-Prozent Kapazität erreicht. Auf Dell™ PowerEdge™ x8xx-, x9xx- und xx1x-Systemen wechselt das Statusanzeigesymbol neben dem Protokollnamen auf einen kritischen Status (  ), wenn die Protokolldatei 100-Prozent Kapazität erreicht.

 **ANMERKUNG:** Es wird empfohlen, dass Sie das Hardwareprotokoll löschen, wenn es 80-Prozent-Kapazität erreicht. Wenn dem Protokoll erlaubt wird, 100-Prozent Kapazität zu erreichen, werden die neuesten Ereignisse aus Protokoll entfernt und verworfen.

- 1 Das Warnungsprotokoll auf einer Liste aller vom Server Administrator-Instrumentation Service in Reaktion auf Sensorstatusänderungen erzeugten Ereignissen und anderer überwachter Parameter anzeigen.

 **ANMERKUNG:** Im *Server Administrator-Meldungs-Referenzhandbuch* finden Sie eine vollständige Erklärung jeder einzelnen Warnungsereignis-ID, eine entsprechende Beschreibung, den Schweregrad und die Ursache.

- 1 Das Befehlsprotokoll für eine Liste mit jedem entweder von der **Server Administrator**-Startseite oder von der Befehlszeilenoberfläche ausgeführten Befehl anzeigen.

 **ANMERKUNG:** Unter "[Server Administrator-Protokolle](#)" erhalten Sie vollständige Anleitungen zu Ansicht, Drucken, Speichern und Senden von Protokollen per E-Mail.

## Warnungsverwaltung

### Unterregister: Warnungsmaßnahmen | Plattförmereignisse | SNMP-Traps

Im Register **Warnungsverwaltung** können Sie Folgendes durchführen:

- 1 Die aktuellen Warnungsmaßnahmen-Einstellungen sehen und die Warnungsmaßnahmen festlegen, die ausgeführt werden sollen, wenn ein Systemkomponentensensor einen Warnungs- oder Ausfallwert sendet.
- 1 Die aktuellen Plattförmereignisfilter-Einstellungen sehen und die Plattförmereignisfilter-Maßnahmen festlegen, die ausgeführt werden sollen, wenn ein Systemkomponentensensor einen Warnungs- oder Ausfallwert sendet. Sie können auch über die Option **Ziel konfigurieren** ein Ziel auswählen (IPv4- oder IPv6-Adresse), an das eine Warnung über ein Plattförmereignis gesendet werden soll.

 **ANMERKUNG:** Server Administrator wird die Scope-ID der IPv6-Adresse nicht in seiner grafischen Benutzeroberfläche anzeigen.

- 1 Prüfen Sie die derzeitigen SNMP-Trap-Warnungsgrenzwerte und setzen Sie die Warnungsgrenzwerte für instrumentierte Systemkomponenten. Die ausgewählten Traps werden ausgelöst, wenn das System ein entsprechendes Ereignis bei dem ausgewählten Schweregrad erzeugt.

 **ANMERKUNG:** Im Fenster Warnungsmaßnahmen sind alle **Warnungsmaßnahmen** für alle potenziellen Systemkomponentensensoren aufgelistet, auch wenn diese in Ihrem System gar nicht vorhanden sind. Das Setzen von Warnungsmaßnahmen für Systemkomponentensensoren, die auf dem System nicht vorhanden sind, hat keine Auswirkungen.

## Sitzungsverwaltung

### Unterregister: Sitzung

Im Register **Sitzungsverwaltung** können Sie Folgendes durchführen:

- 1 Sitzungsinformationen für die aktuellen Benutzer ansehen, die sich im Server Administrator angemeldet haben.
- 1 Benutzersitzungen beenden.

 **ANMERKUNG:** Nur Benutzer mit administrativen Berechtigungen können die Seite "Sitzungsverwaltung" sehen und Sitzungen von angemeldeten Benutzern beenden.

## Hauptsystemgehäuse/Hauptsystem

Durch Klicken auf das Objekt **Hauptsystemgehäuse/Hauptsystem** können Sie die wichtigen Hardware- und Softwarekomponenten des Systems verwalten.

Die verfügbaren Komponenten sind:

- o [Batterien](#)
- o [BIOS](#)
- o [Lüfter](#)
- o [Firmware](#)
- o [Hardwareleistung](#)
- o [Eingriff](#)
- o [Speicher](#)
- o [Netzwerk](#)
- o [Ports](#)
- o [Power Management](#)
- o [Netzteile](#)
- o [Prozessoren](#)
- o [Remotegriff](#)
- o [Wechselbarer Flash-Datenträger](#)
- o [Steckplätze](#)
- o [Temperaturen](#)

- o [Spannungen](#)

-  **ANMERKUNG:** Hardwareleistung wird nur auf Dell xx0x-Systemen unterstützt.
-  **ANMERKUNG:** Netzteile ist nicht auf einem Dell PowerEdge 1900-System verfügbar.
-  **ANMERKUNG:** Die Energieverwaltung wird von einer beschränkten Auswahl an Dell xx0x-Systemen unterstützt.

Das System/Servermodul kann ein Hauptsystemgehäuse oder mehrere Gehäuse enthalten. Das Hauptsystemgehäuse/Hauptsystem enthält die wichtigsten Komponenten eines Systems. Das Maßnahmenfenster des Objekts **Hauptsystemgehäuse/Hauptsystem** verfügt über folgende Registerkarte: **Eigenschaften**.

#### Eigenschaften

Unterregister: Funktionszustand | Informationen | Systemkomponenten (FRU) | Vorderseite

Im Register **Eigenschaften** können Sie Folgendes durchführen:

- 1 Den Zustand oder Status von Hardwarekomponenten und Sensoren anzeigen. Neben jeder aufgelisteten Komponente ist das Symbol "System/Servermodul-Komponentenstatusanzeigen" zu sehen. Ein grünes Kontrollhäkchen (  ) zeigt an, dass eine Komponente in Ordnung (normal) ist. Ein gelbes Dreieck mit einem Ausrufezeichen (  ) zeigt an, dass für eine Komponente ein Warnzustand (nicht kritisch) besteht, der sofortige Aufmerksamkeit erfordert. Ein rotes X (  ) zeigt eine Ausfallbedingung (kritisch) für eine Komponente an, die einen sofortigen Eingriff erfordert. Eine Leerstelle (  ) bedeutet, dass der Zustand der Komponente unbekannt ist. Die verfügbaren überwachten Komponenten umfassen:

- o [Lüfter](#)
- o [Hardware-Protokoll](#)
- o [Eingriff](#)
- o [Speicher](#)
- o [Netzwerk](#)
- o [Power Management](#)
- o [Netzteile](#)
- o [Prozessoren](#)
- o [Temperaturen](#)
- o [Spannungen](#)

-  **ANMERKUNG:** Netzstromschalter wird bei beschränkten Systemen unterstützt.
-  **ANMERKUNG:** Batterien wird nur bei Dell PowerEdge x9xx- und Dell xx0x-Systemen unterstützt.
-  **ANMERKUNG:** Netzteile sind nicht auf einem Dell PowerEdge 1900-System verfügbar.
-  **ANMERKUNG:** Die Energieverwaltung wird von einer beschränkten Auswahl an Dell xx0x-Systemen unterstützt.

- 1 Informationen über die Attribute des Hauptsystemgehäuses anzeigen
- 1 Detaillierte Informationen über die in Ihrem System eingebauten vor Ort austauschbaren Einheiten (FRUs) anzeigen (im Unterregister **Systemkomponenten (FRU)**).
- 1 Aktivieren oder deaktivieren Sie die Schaltflächen an der Vorderseite des verwalteten Systems, und zwar den Netzschalter und die Schaltfläche Nicht-maskierbarer Interrupt (NMI) (falls auf dem System vorhanden).

#### Netzstromschalter

Klicken Sie auf das Objekt **Netzstromschalter**, um Schlüsselfunktionen des Netzstrom-Failover-Schalters des Systems anzuzeigen. Das Maßnahmenfenster des Objekts **Netzstromschalter** kann das folgende Register aufweisen, abhängig von den Gruppenzugriffsrechten des Benutzers: **Eigenschaften**.

#### Eigenschaften

Unterregister: Informationen

Im Register **Eigenschaften** können Netzstromredundanz-Informationen angezeigt und Informationen zu Netzstromleitungen angezeigt werden.

#### Batterien

Klicken Sie auf das Objekt **Batterien**, um Informationen über die jeweiligen auf dem System installierten Batterien anzuzeigen. Batterien behalten die Zeit und das Datum bei, wenn Ihr System ausgeschaltet wird. Die Batterie speichert die BIOS-Setup-Konfiguration des Systems, wodurch das System effizient neu starten kann. Das Maßnahmenfenster des Objekts **Batterien** kann die folgenden Register aufweisen, abhängig von den Gruppenzugriffsberechtigungen des Benutzers: **Eigenschaften** und **Warnungsverwaltung**.

#### Eigenschaften

Unterregister: Informationen

Im Register **Eigenschaften** können Sie die aktuellen Messwerte und den Status Ihrer Systembatterien anzeigen.

## Warnungsverwaltung

Unter dem Register **Warnungsverwaltung** können die Warnungen konfiguriert werden, die im Falle einer Batteriewarnung oder eines Kritisch/Fehler-Ereignisses in Kraft treten sollen.

## BIOS

Klicken Sie auf das Objekt **BIOS**, um die Schlüsselfunktionen des BIOS Ihres Systems zu verwalten. Das System-BIOS enthält auf einem Flash-Speicherchipatz gespeicherte Programme, die den Datenaustausch zwischen dem Mikroprozessor und Peripheriegeräten, z. B. Tastatur und Videoadapter, und verschiedenen anderen Funktionen, wie z. B. Systemmeldungen, steuern. Das Maßnahmenfenster des Objekts **BIOS** kann, abhängig von den Gruppenberechtigungen des Benutzers, die folgenden Registerkarten aufweisen: **Eigenschaften** und **Setup**.

### Eigenschaften

#### Unterregister: Informationen

Im Register **Eigenschaften** können Sie BIOS-Informationen anzeigen.

### Setup

#### Unterregister: BIOS

Im Register **Setup** kann der Zustand jedes BIOS-Setup-Objektes eingestellt werden.

Sie können den Zustand von vielen BIOS-Setup-Funktionen modifizieren, einschließlich, aber nicht beschränkt auf, serielle Schnittstelle, Netzwerkschnittstellen-Controller-Karten, Startsequenz, Festplattenlaufwerksequenz, für den Benutzer zugreifbare USB-Schnittstellen, CPU Virtualization Technology, CPU HyperThreading, Wechselstromwiederherstellungs-Modus, integrierter SATA-Controller, Konsolenumleitung und Failsafe-Baudrate der Konsolenumleitung. Sie können auch ein internes USB-Gerät, Trusted Platform Module-Einstellungen (TPM-Einstellungen), Einstellungen des optischen Laufwerk-Controllers, den Watchdog-Zeitgeber der automatischen Systemwiederherstellung (ASR), einen integrierten Hypervisor und zusätzliche LAN-Netzwerkschnittstellen bei Hauptplatineninformationen konfigurieren.

Abhängig von der spezifischen Systemkonfiguration werden eventuell zusätzliche Setup-Elemente angezeigt. Jedoch können einige BIOS-Setup-Optionen auf dem F2 BIOS-Setup-Bildschirm gezeigt werden, die in Server Administrator nicht zugreifbar sind.

 **ANMERKUNG:** Die NIC-Konfigurationsinformationen innerhalb des Server Administrator **BIOS-Setup** sind für integrierte NICs eventuell ungenau. Das Verwenden des **BIOS-Setup-Bildschirms**, um NICs zu aktivieren oder deaktivieren, führt eventuell zu unerwarteten Ergebnissen. Es wird empfohlen, dass Sie alle Konfigurationen für integrierte NICs über den betreffenden **System-Setup-Bildschirm** ausführen, der während des Systemstarts durch Drücken von <F2> aufgerufen werden kann.

 **ANMERKUNG:** Das BIOS-Setup-Register für Ihr System zeigt nur die BIOS-Funktionen an, die auf Ihrem System unterstützt werden.

## Lüfter

Klicken Sie auf das Objekt **Lüfter**, um Ihre Systemlüfter zu verwalten. Server Administrator überwacht den Status jedes Systemlüfters durch Messung der Lüfterumdrehungen pro Minute. Lüftersonden melden die Lüfterdrehzahlen an den Server Administrator-Instrumentation Service. Wenn Sie **Lüfter** in der Gerätestruktur wählen, werden Details im Datenbereich im rechten Teil der Server Administrator-Homepage angezeigt. Das Maßnahmenfenster des Objekts **Lüfter** kann die folgenden Register aufweisen, abhängig von den Gruppenzugriffsberechtigungen des Benutzers: **Eigenschaften** und **Warnungsverwaltung**.

### Eigenschaften

#### Unterregister: Lüftersonden

Im Register **Eigenschaften** können Sie Folgendes durchführen:

- 1 Lesen Sie die Strommesswerte Ihrer System-Lüftersonden ab und geben Sie Minimal- und Maximalwerte für die Lüftersonden-Warnung ein.

 **ANMERKUNG:** Manche Lüftersondenfelder weichen ab, je nachdem, welche Firmware Ihr System hat: Manche Schwellenwerte können in BMC-Systemen nicht geändert werden.

- 1 Lüftersteuerungsoptionen auswählen.

### Warnungsverwaltung

#### Unterregister: Warnungsmaßnahmen | SNMP-Traps

Im Register **Warnungsverwaltung** können Sie Folgendes durchführen:

- 1 Die aktuellen Warnungsmaßnahmen-Einstellungen sehen und die Warnungsmaßnahmen festlegen, die ausgeführt werden sollen, wenn ein Lüfter einen Warnungs- oder Ausfallwert sendet.
- 1 Prüfen Sie die derzeitigen SNMP-Trap-Warnungsgrenzwerte und setzen Sie die Warnungsgrenzwerte für Lüfter. Die ausgewählten Traps werden ausgelöst, wenn das System ein entsprechendes Ereignis bei dem ausgewählten Schweregrad erzeugt.

## Firmware

Klicken Sie auf das Objekt **Firmware**, um Ihre Systemlüfter zu verwalten. Firmware besteht aus Programmen oder Daten, die in den ROM geschrieben wurden. Die Firmware kann ein Gerät starten und betreiben. Jeder Controller enthält Firmware, die die Controller-Funktionalität bereitstellt. Das Maßnahmenfenster des **Firmware-Objekts** kann, abhängig von den Gruppenzugriffsrechten des Benutzers, das folgende Register aufweisen: **Eigenschaften**.

### Eigenschaften

#### Unterregister: Informationen

Im Register **Eigenschaften** können Sie die Firmware-Informationen für das System anzeigen.

## Hardwareleistung

Klicken Sie auf das Objekt **Hardwareleistung**, um den Status und die Ursache für den Abfall der Systemleistung anzuzeigen. Das Maßnahmenfenster des Objekts **Hardwareleistung** kann das folgende Register aufweisen, abhängig von den Gruppenzugriffsrechten des Benutzers: **Eigenschaften**.

[Tabelle 4-1](#) listet die möglichen Werte für den Status und die Ursache einer Sonde auf:

**Tabelle 4-1. Mögliche Werte für den Status und die Ursache einer Sonde**

Statuswerte	Ursachenwerte
Degraded	Benutzerkonfiguration
	Unzureichende Stromkapazität
	Unbekannter Grund
Normal	-

### Eigenschaften

#### Unterregister: Informationen

Im Register **Eigenschaften** können Sie die Details zur Verschlechterung der Systemleistung sehen.

## Eingriff

Klicken Sie auf das Objekt **Eingriff**, um den Gehäuseeingriffsstatus Ihres Systems zu verwalten. Server Administrator überwacht den Gehäuseeingriffsstatus als Sicherheitsmaßnahme zur Vermeidung unbefugten Zugriffs auf die kritischen Komponenten des Systems. Gehäuseeingriff zeigt an, dass jemand die Abdeckung des Systemgehäuses öffnet oder bereits geöffnet hat. Das Maßnahmenfenster des Objekts **Eingriff** kann die folgenden Register aufweisen, abhängig von den Gruppenzugriffsberechtigungen des Benutzers: **Eigenschaften** und **Warnungsverwaltung**.

### Eigenschaften

#### Unterregister: Eingriff

Im Register **Eigenschaften** können Sie den Gehäuseeingriffsstatus anzeigen.

### Warnungsverwaltung

#### Unterregister: Warnungsmaßnahmen | SNMP-Traps

Im Register **Warnungsverwaltung** können Sie Folgendes durchführen:

- 1 Die aktuellen Warnungsmaßnahmen-Einstellungen anzeigen und die Warnungsmaßnahmen festlegen, die ausgeführt werden sollen, wenn der Eingriffssensor einen Warnungs- oder Ausfallwert sendet.
- 1 Aktuelle SNMP-Trap-Warnungsgrenzwerte anzeigen und die Warnungsgrenzwerte für den Eingriffssensor setzen. Die ausgewählten Traps werden ausgelöst, wenn das System ein entsprechendes Ereignis bei dem ausgewählten Schweregrad erzeugt.

## Speicher

Klicken Sie auf das Objekt **Speicher**, um die Speichergeräte des Systems zu verwalten. Server Administrator überwacht den Speichergerätestatus für jedes im überwachten System vorhandene Speichermodul. Speichergerät-Vorausfallsensoren überwachen die Speichermodule durch Zählen der ECC-Speicherkorrekturen. Server Administrator überwacht darüber hinaus die Speicherredundanzinformationen, wenn das betreffende System diese Funktion unterstützt. Das Maßnahmenfenster des Objekts **Speicher** kann die folgenden Register aufweisen, abhängig von den Gruppenzugriffsberechtigungen des Benutzers: **Eigenschaften** und **Warnungsverwaltung**.

### Eigenschaften

#### Unterregister: Speicher

Im Register **Eigenschaften** können Speicherattribute, Einzelheiten über Speichergeräte und Gerätestatus des Speichers angezeigt werden.

 **ANMERKUNG:** Wenn ein System mit aktiviertem Spare Bank-Speicher in einen "Redundanz verloren"-Zustand übergeht, ist es eventuell nicht offensichtlich, welches Speichermodul die Ursache ist. Wenn Sie nicht bestimmen können, welches DIMM ersetzt werden soll, sehen Sie den Protokolleintrag *Wechsel zu Ersatzspeicherbank festgestellt* im ESM-Systemprotokoll nach, um herauszufinden, welches Speichermodul versagte.

### Warnungsverwaltung

#### Unterregister: Warnungsmaßnahmen | SNMP-Traps

Im Register **Warnungsverwaltung** können Sie Folgendes durchführen:

- 1 Die aktuellen Warnungsmaßnahmen-Einstellungen anzeigen und die Warnungsmaßnahmen festlegen, die ausgeführt werden sollen, wenn ein Speichermodul einen Warnungs- oder Ausfallwert sendet.
- 1 Aktuelle SNMP-Trap-Warnungsgrenzwerte anzeigen und die Warnungsgrenzwerte für Speichermodule setzen. Die ausgewählten Traps werden ausgelöst, wenn das System ein entsprechendes Ereignis bei dem ausgewählten Schweregrad erzeugt.

## Netzwerk

Klicken Sie auf das Objekt **Netzwerk**, um die NICs des Systems zu verwalten. Der Server Administrator überwacht den Status jeder NIC im System, um eine kontinuierliche Remote-Verbindung sicherzustellen. Das Maßnahmenfenster des Objekts **Netzwerk** kann das folgende Register aufweisen, abhängig von den Gruppenzugriffsrechten des Benutzers: **Eigenschaften**.

### Eigenschaften

#### Unterregister: Informationen

Im Register **Eigenschaften** können Sie Informationen über die im System installierten NICs anzeigen.



**ANMERKUNG:** Im Abschnitt IPv6-Adressen zeigt Server Administrator neben der link-lokalen Adresse nur zwei Adressen an.

## Ports

Klicken Sie auf das Objekt **Schnittstellen**, um die externen Anschlüsse des Systems zu verwalten. Server Administrator überwacht den Status jedes im System vorhandenen externen Anschlusses. Das Maßnahmenfenster des Objekts **Schnittstellen** kann das folgende Register aufweisen, abhängig von den Gruppenzugriffsrechten des Benutzers: **Eigenschaften**.

### Eigenschaften

#### Unterregister: Informationen

Im Register **Eigenschaften** können Sie die Informationen über die im System vorhandenen externen Anschlüsse anzeigen.

## Power Management

### Überwachung

#### Unterregister: Verbrauchsstatistik

Unter dem Register Verbrauch können Sie die Leistungsaufnahmeinformationen zum System in Watt and BTU/h anzeigen und verwalten.

**BTU/h=Watt X 3,413** (Wert zur nächsten ganzen Zahl abgerundet)

Server Administrator überwacht den Stromverbrauchstatus, die Stromstärke und Details zur Stromstatistik.

Sie können auch den Sofort-Headroom des Systems sowie den Spitzen-Headroom des Systems anzeigen. Die Werte werden sowohl in Watt als auch in BTU/h (British Thermal Unit) angezeigt. Stromschwellenwerte können sowohl in Watt als auch in BTU/h festgelegt werden.

Über das Register Statistik können Sie die Stromverfolgungsstatistik zum System anzeigen und zurücksetzen, wie z. B. für Energieverbrauch, Spitzenleistung des Systems und Spitzenstromstärke des Systems.

### Verwaltung

#### Unterregister: Budget | Profile

Über das Register Budget können Sie die Strominventarattribute wie Spannungslosigkeit des Systems und den maximalen potenziellen Systemstrom in Watt und BTU/h anzeigen. Sie können die Strombudget-Option auch dazu verwenden, die Stromobergrenze für Ihr System festzulegen und zu aktivieren.

Über das Register Profile können Sie ein Stromprofil auswählen, um die Systemleistung zu maximieren und Energie einzusparen.

### Warnungsverwaltung

#### Unterregister: Warnungsmaßnahmen | SNMP-Traps

Verwenden Sie das Register Warnungsmaßnahmen, um Systemwarnungsmaßnahmen für verschiedene Systemereignisse wie Systemstromsondenwarnungen und Spitzenleistung des Systems festzulegen.

Verwenden Sie das Register SNMP-Traps zum Konfigurieren von SNMP-Traps für das System.

Bestimmte Energieverwaltungs-Funktionen stehen eventuell nur auf Systemen zur Verfügung, die mit dem Energieverwaltungs-Bus (PMBus) aktiviert wurden.

## Netzteile

Klicken Sie auf das Objekt **Netzteile**, um die Netzteile des Systems zu verwalten. Server Administrator überwacht den Status der Netzteile, einschließlich der Redundanz, um sicherzustellen, dass jedes im System vorhandene Netzteil korrekt funktioniert. Das Maßnahmenfenster des Objekts **Netzteile** kann die folgenden Register aufweisen, abhängig von den Gruppenzugriffsberechtigungen des Benutzers: **Eigenschaften** und **Warnungsverwaltung**.

### Eigenschaften

#### Unterregister: Elemente

Im Register **Eigenschaften** können Sie Folgendes durchführen:

- Informationen über die Attribute der Netzteilredundanz anzeigen.

· Den Status individueller Netzteilelemente überprüfen, einschließlich Nennwattleistung Eingabe und maximale Wattleistung Ausgabe. Das Attribut der Nennwattleistung Eingabe wird nur auf PMBus-Systemen angezeigt, die mit xx7x beginnen.

## Warnungsverwaltung

### Unterregister: Warnungsmaßnahmen | SNMP-Traps

Im Register **Warnungsverwaltung** können Sie Folgendes durchführen:

- 1 Die aktuellen Warnungsmaßnahmen-Einstellungen anzeigen und die Warnungsmaßnahmen festlegen, die ausgeführt werden sollen, wenn ein Systemstrom einen Warnungs- oder Ausfallwert sendet.
- 1 Plattförmereignis-Warnungsziele für IPv6-Adressen konfigurieren.
- 1 Aktuelle SNMP-Trap-Warnungsgrenzwerte anzeigen und die Warnungsgrenzwerte für die Stromleistung des Systems setzen. Die ausgewählten Traps werden ausgelöst, wenn das System bei dem ausgewählten Schweregrad ein entsprechendes Ereignis erzeugt.

 **ANMERKUNG:** Der Trap für die Spitzenleistung des Systems erzeugt nur Ereignisse für Schweregrade in Bezug auf Informationen.

## Prozessoren

Klicken Sie auf das Objekt **Prozessoren**, um die Mikroprozessoren des Systems zu verwalten. Ein Prozessor ist der primäre Rechenchip im Inneren eines Systems, der die Auswertung und Ausführung von arithmetischen und logischen Funktionen steuert. Das Maßnahmenfenster des Objekts **Prozessoren** kann, abhängig von den Gruppenzugriffsberechtigungen des Benutzers, die folgenden Register aufweisen: **Eigenschaften** und **Warnungsverwaltung**.

### Eigenschaften

#### Unterregister: Informationen

Im Register **Eigenschaften** können Sie Informationen über den/die Mikroprozessor(en) des Systems anzeigen und auf detaillierte Informationen des Cache zugreifen.

## Warnungsverwaltung

### Unterregister: Warnungsmaßnahmen | SNMP-Traps

Im Register **Warnungsverwaltung** können Sie Folgendes durchführen:

- 1 Die aktuellen Warnungsmaßnahmen-Einstellungen sehen und die Warnungsmaßnahmen festlegen, die ausgeführt werden sollen, wenn ein Prozessor einen Warnungs- oder Ausfallwert sendet.
- 1 Aktuelle SNMP-Trap-Warnungsgrenzwerte anzeigen und die Warnungsgrenzwerte für Prozessoren setzen. Die ausgewählten Traps werden ausgelöst, wenn das System ein entsprechendes Ereignis bei dem ausgewählten Schweregrad erzeugt.

## Remotezugriff

Klicken Sie auf das Objekt **Remote-Zugriff**, um die BMC-Funktionen (Baseboard-Verwaltungs-Controller) oder iDRAC- (Integrated Dell Remote Access Controller) und Remote Access Controller-Funktionen zu verwalten.

Durch die Auswahl des Registers Remote-Zugriff können Sie die BMC/iDRAC-Funktionen, wie z. B. allgemeine Informationen zu BMC/iDRAC, verwalten. Sie können auch die Konfiguration des BMC/iDRAC in einem LAN-Netzwerk, die serielle Schnittstelle für den BMC/iDRAC, Terminalmoduseinstellungen für die serielle Schnittstelle, BMC/iDRAC seriell über LAN und BMC/iDRAC-Benutzer verwalten.

 **ANMERKUNG:** BMC wird bei den Dell PowerEdge x8xx- und x9xx-Systemen unterstützt. iDRAC wird nur auf den Dell xx0x- und xx1x-Systemen unterstützt.

 **ANMERKUNG:** Wenn eine andere Anwendung als Server Administrator zur Konfiguration des BMC/iDRAC verwendet wird, während Server Administrator läuft, dann kann es vorkommen, dass die BMC/iDRAC-Konfigurationsdaten, die von Server Administrator angezeigt werden, nicht mit dem BMC/iDRAC übereinstimmen. Es wird deshalb empfohlen, Server Administrator zur Konfiguration des BMC/iDRAC zu verwenden, während Server Administrator läuft.

DRAC ermöglicht Ihnen, auf die Remote System Management-Fähigkeiten des Systems zuzugreifen. Der Server Administrator DRAC gewährt Remote-Zugriff auf nicht arbeitsfähige Systeme, auf Warnungsmeldungen, wenn ein System außer Betrieb ist, und die Möglichkeit, ein System neu zu starten.

Das Maßnahmenfenster des Objekts **Remote-Zugriff** kann die folgenden Register aufweisen, abhängig von den Gruppenzugriffsberechtigungen des Benutzers: **Eigenschaften**, **Konfiguration** und **Benutzer**.

### Eigenschaften

#### Unterregister: Informationen

Im Register **Eigenschaften** können Sie allgemeine Informationen über das Remote-Zugriffsgerät anzeigen. Sie können auch die Attribute der IPv4- und IPv6-Adressen anzeigen.

Klicken Sie auf **Wieder auf Standardeinstellung stellen**, um alle Attribute wieder auf ihre Standardeinstellungen zurückzusetzen.

## Konfiguration

### Unterregister: LAN | Serielle Schnittstelle | Seriell über LAN | Zusätzliche Konfiguration

Wenn BMC/iDRAC konfiguriert ist, können Sie im Register **Konfiguration** den BMC/iDRAC für ein LAN-Netzwerk, die serielle Schnittstelle für den BMC/iDRAC oder den BMC/iDRAC seriell über LAN konfigurieren.

Wenn DRAC konfiguriert ist, können Sie unter dem Register **Konfiguration** Folgendes ausführen:

- 1 Netzwerkeigenschaften konfigurieren.

 **ANMERKUNG:** Die Felder **NIC aktivieren**, **NIC-Auswahl** und **Verschlüsselungsschlüssel** werden nur auf Dell PowerEdge x9xx-Systemen angezeigt.

Unter dem Register **Zusätzliche Konfiguration** können Sie IPv4/IPv6-Eigenschaften entweder aktivieren oder deaktivieren.

 **ANMERKUNG:** Das Aktivieren/Deaktivieren von IPv4/IPv6 ist nur in einer Dual-Stack-Umgebung möglich (wo sowohl die IPv4- als auch die IPv6-Stacks geladen sind).

## Benutzer

### Unterregister: Benutzer

Im Register **Benutzer** kann die Benutzerkonfiguration für Remote-Zugriff geändert werden. Informationen über Remote Access Controller-Benutzer können hinzugefügt, konfiguriert und angesehen werden.

 **ANMERKUNG:** Auf Dell PowerEdge x9xx-Systemen:

- 1 Zehn Benutzer-IDs werden angezeigt. Wenn eine DRAC-Karte installiert wird, werden sechzehn Benutzer-IDs angezeigt.
- 1 Seriell über LAN Nutzlast-Spalte wird angezeigt.

## Wechselbarer Flash-Datenträger

Klicken Sie auf das Objekt **Removable Flash Media (wechselbarer Flash-Datenträger)**, um den Funktionszustand und Redundanzstatus interner SD-Module und vFlash-Datenträger anzuzeigen. Das Maßnahmenfenster des wechselbaren Flash-Datenträgers verfügt über das Register **Properties (Eigenschaften)**.

### Eigenschaften

#### Unterregister: Informationen

Unter dem Register **Properties (Eigenschaften)** können Sie Informationen zu den wechselbaren Flash-Datenträgern und internen SD-Modulen anzeigen. Dies schließt Details zum Konnektornamen, seinem Zustand sowie seiner Speichergröße an.

### Warnungsverwaltung

#### Unterregister: Warnungsmaßnahmen | SNMP-Traps

Im Register **Warnungsverwaltung** können Sie Folgendes durchführen:

- 1 Die aktuellen Warnungsmaßnahmen-Einstellungen anzeigen und die Warnungsmaßnahmen festlegen, die ausgeführt werden sollen, falls die wechselbare Flash-Datenträgersonde einen Warnungs- oder Ausfallwert zurückgibt.
- 1 Die derzeitigen SNMP-Trap-Warnungsgrenzwerte anzeigen und die Warnungsgrenzwerte für wechselbare Flash-Datenträgersonden einstellen. Die ausgewählten Traps werden ausgelöst, wenn das System ein entsprechendes Ereignis bei dem ausgewählten Schweregrad erzeugt.

Die Warnungsverwaltung ist internen SD-Modulen und vFlash gemeinsam. Durch das Konfigurieren von Warnungsmaßnahmen/SNMP/PEF für das eine wird die Konfiguration automatisch auch für das andere ausgeführt.

## Steckplätze

Klicken Sie auf das Objekt **Steckplätze**, um die Anschlüsse oder Sockel auf der Hauptplatine zu verwalten, die gedruckte Leiterplatten, z. B. Erweiterungskarten, aufnehmen. Das Objektmaßnahmenfenster **Slots (Steckplätze)** enthält das Register **Properties (Eigenschaften)**.

### Eigenschaften

#### Unterregister: Informationen

Im Register **Eigenschaften** können Sie Informationen über jeden Steckplatz und installierten Adapter anzeigen.

## Temperaturen

Klicken Sie auf das Objekt **Temperaturen**, um die Systemtemperatur zu verwalten und so Hitzeschäden an den internen Komponenten zu verhindern. Server Administrator überwacht die Temperatur an verschiedenen Stellen im Systemgehäuse, um sicherzustellen, dass die Temperaturen im Gehäuse nicht zu stark ansteigen. Das Maßnahmenfenster des Objekts **Temperaturen** kann, abhängig von den Gruppenzugriffsberechtigungen des Benutzers, die folgenden Register aufweisen: **Eigenschaften** und **Warnungsverwaltung**.

### Eigenschaften

#### Unterregister: Temperatursonden

Im Register **Eigenschaften** können Sie die Strommesswerte und den Status der Temperatursonden des Systems sehen und Minimum- und Maximumwerte für den Schwellenwert der Temperatursonden-Warnung angeben.

 **ANMERKUNG:** Manche Temperatursondenfelder weichen ab, je nachdem, welche Firmware Ihr System hat: BMC oder ESM. Manche Schwellenwerte können in BMC-Systemen nicht geändert werden. Beim Zuweisen von Sondenschwellenwerten rundet Server Administrator die von Ihnen eingegebenen Mindest- oder Maximalwerte manchmal zu den am nächsten zuweisbaren Werten.

### Warnungsverwaltung

#### Unterregister: Warnungsmaßnahmen | SNMP-Traps

Im Register **Warnungsverwaltung** können Sie Folgendes durchführen:

- 1 Die aktuellen Warnungsmaßnahmen-Einstellungen anzeigen und die Warnungsmaßnahmen festlegen, die ausgeführt werden sollen, wenn eine Temperatursonde einen Warnungs- oder Ausfallwert sendet.
- 1 Die derzeitigen SNMP-Trap-Warnungsgrenzwerte anzeigen und die Warnungsgrenzwerte für Temperatursonden setzen. Die ausgewählten Traps werden ausgelöst, wenn das System ein entsprechendes Ereignis bei dem ausgewählten Schweregrad erzeugt.

 **ANMERKUNG:** Minimale und maximale Grenzwerte der Temperatursonde für das externe Gehäuse können nur in Ganzzahlen angegeben werden. Wenn ein Benutzer versucht, den minimalen oder maximalen Grenzwert der Temperatursonde auf einen Dezimalwert zu setzen, wird nur die Ganzzahl vor dem Komma als Grenzwerteinstellung gespeichert.

## Spannungen

Klicken Sie auf das Objekt **Spannungen**, um die Spannungsniveaus im System zu regeln. Server Administrator überwacht die Spannungen in kritischen Komponenten an verschiedenen Gehäusestellen im überwachten System. Das Maßnahmenfenster des Objekts **Spannungen** kann die folgenden Register aufweisen, abhängig von den Gruppenzugriffsberechtigungen des Benutzers: **Eigenschaften** und **Warnungsverwaltung**.

### Eigenschaften

#### Unterregister: Spannungssonden

Im Register **Eigenschaften** können Sie die Strommesswerte und den Status der Spannungssonden Ihres Systems ablesen und die Minimal- und Maximalwerte, d. h. die Schwellenwerte für die Spannungssonden-Warnung, konfigurieren.

 **ANMERKUNG:** Manche Spannungssondenfelder weichen ab, je nachdem, welche Firmware Ihr System hat: BMC oder ESM. Manche Schwellenwerte können in BMC-Systemen nicht geändert werden.

### Warnungsverwaltung

#### Unterregister: Warnungsmaßnahmen | SNMP-Traps

Im Register **Warnungsverwaltung** können Sie Folgendes durchführen:

- 1 Die aktuellen Warnungsmaßnahmen-Einstellungen sehen und die Warnungsmaßnahmen festlegen, die ausgeführt werden sollen, wenn ein Systemspannungssensor einen Warnungs- oder Ausfallwert sendet.
- 1 Die aktuellen SNMP-Trap-Warnungsgrenzwerte anzeigen und die Warnungsgrenzwerte für Spannungssensoren setzen. Die ausgewählten Traps werden ausgelöst, wenn das System ein entsprechendes Ereignis bei dem ausgewählten Schweregrad erzeugt.

## Software

Klicken Sie auf das Objekt **Software**, um detaillierte Versionsinformationen über die wichtigsten Softwarekomponenten des verwalteten Systems anzuzeigen, z. B. das Betriebssystem und die Systemverwaltungssoftware. Das Maßnahmenfenster des Objekts **Software** hat folgende Register, abhängig von den Gruppenzugriffsberechtigungen des Benutzers: **Eigenschaften**.

### Eigenschaften

#### Unterregister: Zusammenfassung

Im Register **Eigenschaften** können Sie eine Zusammenfassung über Betriebssystem und Systemverwaltungssoftware des verwalteten Systems anzeigen.

## Betriebssystem

Klicken Sie auf das Objekt **Betriebssystem**, um grundlegende Informationen über das jeweilige Betriebssystem anzuzeigen. Das Maßnahmenfenster des Objekts **Betriebssystem** kann die folgenden Register aufweisen, abhängig von den Gruppenzugriffsberechtigungen des Benutzers: **Eigenschaften**.

### Eigenschaften

#### Unterregister: Informationen

Im Register **Eigenschaften** können Sie grundlegende Informationen über das jeweilige Betriebssystem anzeigen.

## Lagerung

Server Administrator enthält den Storage Management-Service:

Der Storage Management Service enthält Funktionen für die Konfiguration der Speichergeräte. In den meisten Fällen wird der Storage Management Service mit dem typischen Setup installiert. Der Speicherverwaltungsservice ist auf Systemen mit den Betriebssystemen Microsoft Windows, Red Hat Enterprise Linux und SUSE® Linux Enterprise Server verfügbar.

Wenn Storage Management Service installiert ist, klicken Sie auf das Objekt **Speichermedien**, um den Status und die Einstellungen für verschiedene angeschlossene Array-Speichergeräte, Datenträger, Systemfestplatten usw. anzuzeigen.

Beim Storage Management Service hat das Maßnahmenfenster des Objekts **Speichermedien**, je nach Gruppenzugriffsberechtigungen des Benutzers, folgende Register: **Eigenschaften**.

### Eigenschaften

#### Unterregister: Funktionszustand

Im Register **Eigenschaften** können Sie den Funktionszustand oder Status angeschlossener Speicherkomponenten und Sensoren wie Array-Subsysteme, Betriebssystem-Festplatten und Datenträger anzeigen.

## Voreinstellungen verwalten: Konfigurationsoptionen der Startseite

Im linken Fenster der Einstellungen-Startseite (in der die Systemstruktur auf der Startseite von Server Administrator angezeigt wird) werden alle verfügbaren Konfigurationsoptionen im Systemstrukturfenster angezeigt. Die angezeigten Optionen basieren auf der Systemverwaltungssoftware, die auf dem verwalteten System installiert ist.

S. [Tabelle 4-2](#) für verfügbare Konfigurationsoptionen der Einstellungen-Startseite.

**Tabelle 4-2. Konfigurationsoptionen der Voreinstellungen-Homepage verwalten**

	*****	Allgemeine Einstellungen
	*****	Server Administrator

## Allgemeine Einstellungen

Klicken Sie auf das Objekt **Allgemeine Einstellungen**, um Benutzer- und DSM SA Verbindungsdienst-Einstellungen (Web Server) für ausgewählte Server Administrator-Funktionen einzurichten. Das Maßnahmenfenster des Objekts **Allgemeine Einstellungen** kann, abhängig von den Gruppenzugriffsrechten des Benutzers, die folgenden Register aufweisen: **Benutzer** und **Web-Server**.

### Benutzer

#### Unterregister: Eigenschaften

Im Register **Benutzer** können Sie Benutzereinstellungen setzen, z. B. die Homepage-Darstellung und die Standard-E-Mail-Adresse für die Schaltfläche **E-Mail**.

### Web-Server

#### Unterregister: Eigenschaften | X.509-Zertifikat

Im Register **Web Server** können Sie Folgendes durchführen:

- 1 DSM SA-Verbindungsdiensteinstellungen festlegen. S. "[Dell Systems Management Server Administration-Verbindungsdienst und Sicherheits-Setup](#)" für Anleitungen zum Konfigurieren von Servereinstellungen.
- 1 Konfigurieren Sie die SMTP-Serveradresse und die Bind-IP-Adresse im IPv6-Adressierungsmodus.
- 1 Führen Sie die X.509-Zertifikatsverwaltung durch, indem Sie ein neues X.509-Zertifikat erzeugen, ein vorhandenes X.509-Zertifikat wiederverwenden oder ein Stammzertifikat oder eine Zertifikatskette von einer Zertifizierungsstelle (CA) importieren. Weitere Informationen zur Zertifikatsverwaltung finden Sie unter "[X.509-Zertifikatsverwaltung](#)".

## Server Administrator

Klicken Sie auf das **Server Administrator**-Objekt, um den Zugriff von Benutzern mit Benutzer- oder Hauptbenutzerrechten zu aktivieren oder deaktivieren und das SNMP-Stammkennwort zu konfigurieren. Das Maßnahmenfenster des Objekts **Server Administrator** kann das folgende Register aufweisen, abhängig von den Gruppenzugriffsrechten des Benutzers: **Einstellungen**.

### Einstellungen

#### Unterregister: Zugriffskonfiguration | SNMP-Konfiguration

Im Register **Einstellungen** können Sie Folgendes durchführen:

- 1 Zugriff von Benutzern mit Benutzer- oder Hauptbenutzerrechten aktivieren oder deaktivieren.
- 1 Das SNMP-Stammkennwort konfigurieren.



**ANMERKUNG:** Die Standardeinstellung des SNMP-Konfigurationsbenutzers ist `root` und das Kennwort ist `calvin`.

- 1 SNMP-Satzvorgänge konfigurieren.



**ANMERKUNG:** Nachdem die SNMP-Satzvorgänge konfiguriert sind, müssen die Dienste neu gestartet werden, um die Änderungen wirksam zu machen. Auf Systemen, auf denen unterstützte Microsoft Windows-Betriebssysteme ausgeführt werden, muss der Windows SNMP-Dienst neu gestartet werden. Auf Systemen, auf denen unterstützte Red Hat Enterprise Linux- und SUSE Linux Enterprise Server-Betriebssysteme ausgeführt werden, müssen Server Administrator-Dienste neu gestartet werden, indem der Neustartbefehl `srvadmin-services.sh` ausgeführt wird.

---

[Zurück zum Inhaltsverzeichnis](#)

[Zurück zum Inhaltsverzeichnis](#)

## Einführung

### Dell™ OpenManage™ Server Administrator Version 6.2 Benutzerhandbuch

- [Übersicht](#)
- [Was ist neu bei Version 6.2](#)
- [Verfügbarkeit auf unterstützten Betriebssystemen](#)
- [Server Administrator-Startseite](#)
- [Weitere nützliche Dokumente](#)
- [Anfordern von technischer Unterstützung](#)

---

## Übersicht

Dell™ OpenManage™ Server Administrator bietet eine umfassende Eins-zu-Eins-Systemverwaltungslösung in zwei Formen: als eine integrierte Webbrowser-basierte grafische Benutzeroberfläche (GUI) und als eine Befehlszeilenschnittstelle (CLI) über das Betriebssystem. Server Administrator ist so ausgelegt, dass Systemadministratoren Systeme sowohl lokal als auch extern auf einem Netzwerk verwalten können. Server Administrator ermöglicht es Systemadministratoren, sich auf die Verwaltung des gesamten Netzwerks zu konzentrieren. Dazu wird eine umfassende 1:1-Systemverwaltung zur Verfügung gestellt.

Für Server Administrator kann ein System ein eigenständiges System, ein System mit verbundenen Netzwerkspeichereinheiten in einem separaten Gehäuse oder ein modulares System sein, das aus einem oder mehreren Servermodulen in einem modularen Gehäuse besteht.

Server Administrator enthält Informationen über:

- 1 Systeme, die korrekt arbeiten und Systeme mit Problemen
- 1 Systeme, die Remote-Wiederherstellungsverfahren erfordern.

Server Administrator bietet einfach verwendbare Verwaltung und Administration von lokalen und Remote-Systemen durch ein umfassendes Angebot von integrierten Verwaltungsdiensten. Server Administrator ist die einzige Installation auf dem verwalteten System und ist sowohl lokal als auch extern über die Homepage von Server Administrator zugänglich. Auf Systeme, die im Remote-Zugriff überwacht werden, haben Sie über Einwahl-, 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).

## Installation

Sie können Server Administrator unter Verwendung der *DVD Dell Systems Management Tools and Documentation* installieren. Die DVD bietet ein Setup-Programm zum Installieren, Erweitern und Deinstallieren der Softwarekomponenten von Server Administrator, Managed System und Management Station. Zusätzlich können Sie Server Administrator mittels einer unbeaufsichtigten Installation über ein Netzwerk auf mehreren Systemen installieren.

Das Installationsprogramm von Dell™ OpenManage™ stellt Installationsscripts und RPM-Pakete bereit, um Dell OpenManage Server Administrator und andere Managed System-Softwarekomponenten auf dem verwalteten System zu installieren oder zu deinstallieren. Weitere Informationen finden Sie im *Installationshandbuch zu Dell OpenManage Server Administrator* und im *Installationshandbuch zur Dell OpenManage Management Station-Software*. Sie finden diese Dokumente auch auf der Dell Support-Website unter [support.dell.com/manuals](http://support.dell.com/manuals).

Bei einem modularen System muss Server Administrator auf jedem Servermodul im Gehäuse installiert werden.

## Aktualisieren individueller Systemkomponenten

Um individuelle Systemkomponenten zu aktualisieren, verwenden Sie komponentenspezifische Dell Update Packages. Verwenden Sie die *DVD Dell Server Updates*, um den vollständigen Versionsbericht anzuzeigen und das gesamte System zu aktualisieren. Server Update Utility ist eine DVD-ROM-basierte Anwendung zur Identifizierung und Anwendung von Aktualisierungen auf Ihr System. Die Server Update Utility-Anwendung kann von [support.dell.com](http://support.dell.com) heruntergeladen werden.

Das *Server Update Utility-Benutzerhandbuch* bietet Informationen zum Erhalten und Verwenden des Server-Aktualisierungsdienstprogramms (SUU), um Dell-Systeme zu aktualisieren oder die Aktualisierungen einzusehen, die für alle im Repository aufgelisteten Systeme vorhanden sind.

## Storage Management-Dienst

Der Storage Management Service enthält Speicherverwaltungsinformationen in einer integrierten Grafiksicht.

Detaillierte Informationen zum Storage Management Service finden Sie im *Benutzerhandbuch zu Dell OpenManage Server Administrator Storage Management* auf der Dell Support-Website unter [support.dell.com/manuals](http://support.dell.com/manuals).

## Instrumentation Service

Der Instrumentation Service gewährt schnellen Zugang zu detaillierten Fehler- und Leistungsinformationen, die von industriestandardmäßigen Systemverwaltungsagenten gesammelt werden, und erlaubt die Remote-Verwaltung überwachter Systeme, einschließlich des Herunter- und Hochfahrens des Systems und der Sicherheit.

## Remote-Access-Controller

Der Remote Access Controller bietet eine vollständige Remote System Management-Lösung für Systeme, die mit der DRAC-Lösung (Dell Remote Access Controller) oder der BMC/IDRAC-Lösung (Baseboard-Verwaltungs-Controller/Integrierter Dell Remote Access Controller) ausgestattet sind. Der Remote Access Controller gestattet externen Zugriff auf ein nicht funktionierendes System, wodurch es schnellstmöglich wieder in einen funktionierenden Zustand versetzt werden kann. Der Remote Access Controller leistet ebenfalls Warnungsbenachrichtigung, wenn ein System ausgefallen ist, und ermöglicht den externen Neustart eines Systems. Darüber hinaus protokolliert der Remote Access Controller die wahrscheinliche Ursache von Systemabstürzen und speichert den letzten Absturzbildschirm.

## Protokolle

Server Administrator zeigt Protokolle von an das System gegebene bzw. vom System erhaltene Befehle, überwachte Hardwareereignisse, POST-Ereignisse und Systemwarnungen an. Sie können die Protokolle auf der Homepage anzeigen, drucken oder als Berichte speichern und sie als E-Mail an einen festgelegten Service-Kontakt senden.

---

## Was ist neu bei Version 6.2

Die Versionshöhepunkte von OpenManage Server Administrator 6.2 sind:

- 1 Unterstützung für die Berichterstattung des Funktionszustands interner SD-Module und vFlash-Datenträger auf Dell-Systemen der neuen Generation.
- 1 Unterstützung für das Konfigurieren der Startreihenfolge und das Hinzufügen/Entfernen von Geräten aus der Startliste.
- 1 Unterstützung für das Konfigurieren von e-SATA-Schnittstelle und Prozessor-C1-E.
- 1 Unterstützung für Microsoft® Windows® 7.
- 1 Unterstützung für den zentralen Server Administrator Web Server für Linux.
- 1 Unterstützung für Betriebssystem in türkischer Sprache.
- 1 Unterstützung für Schlüsselsignierungsalgorithmus.

 **ANMERKUNG:** Eine Liste der unterstützten Betriebssysteme finden Sie in der *Dell Systems Software Support Matrix* auf der Dell Support-Website unter [support.dell.com/manuals](http://support.dell.com/manuals).

 **ANMERKUNG:** In der Onlinehilfe zu Server Administrator finden Sie weitere Informationen zu den in dieser Version vorgestellten Funktionen.

---

## Verfügbarkeit von Systemverwaltungsstandards

### Übersicht

Dell™ OpenManage™ Server Administrator unterstützt die folgenden wichtigen Systemverwaltungsprotokolle:

- 1 HTTPS (HyperText Transfer Protocol Secure )
- 1 CIM (Common Information Model, gemeinsames Informationsmodell)
- 1 SNMP (Simple Network Management Protocol, einfaches Netzwerkverwaltungsprotokoll)

Wenn Ihr System SNMP unterstützt, müssen Sie den Dienst auf Ihrem Betriebssystem installieren und aktivieren. Wenn SNMP-Dienste auf Ihrem Betriebssystem verfügbar sind, installiert das Server Administrator-Installationsprogramm die unterstützenden Agenten für SNMP.

HTTPS wird auf allen Betriebssystemen unterstützt. Unterstützung für CIM und SNMP ist betriebssystemabhängig und in einigen Fällen auch abhängig von der Version des Betriebssystems.

Informationen zu SNMP-Sicherheitsbedenken finden Sie in der **Infodatei** zu Dell OpenManage Server Administrator (im Lieferumfang der Server Administrator-Anwendung enthalten) oder auf der Dell Support-Website unter [support.dell.com/manuals](http://support.dell.com/manuals). Sie müssen Aktualisierungen von den Master-SNMP-Agenten Ihres Betriebssystems anwenden, um sicherzustellen, dass die SNMP-Subagenten von Dell sicher sind.

---

## Verfügbarkeit auf unterstützten Betriebssystemen

Auf unterstützten Microsoft® Windows®-Betriebssystemen unterstützt Server Administrator zwei Systemverwaltungsstandards: CIM/WMI (Windows Management Instrumentation) und SNMP, während Server Administrator auf unterstützten Red Hat® Enterprise Linux®- und SUSE® Linux Enterprise Server-Betriebssystemen den SNMP-Systemverwaltungsstandard unterstützt.

Server Administrator fügt diesen Systemverwaltungsstandards bedeutende Sicherheit hinzu. Alle Attributeinstellungsvorgänge (z. B. Ändern des Werts einer Systemkennnummer) müssen mit Dell OpenManage IT Assistant ausgeführt werden, während eine Anmeldung mit der erforderlichen Berechtigung vorliegt.

---

## Verfügbarkeit auf unterstützten Betriebssystemen

[Tabelle 1-1](#) zeigt die Systemverwaltungsstandards, die für jedes unterstützte Betriebssystem zur Verfügung stehen.

**Tabelle 1-1. Verfügbarkeit von Systemverwaltungsstandards**

Betriebssystem	SNMP	CIM
Familie Windows Server® 2008 und Familie Windows Server 2003	Auf dem Installationsmedium des Betriebssystems verfügbar	Immer installiert
Red Hat Enterprise Linux	Verfügbar im <b>net-snmp</b> -Paket über den Betriebssystem-Installationsdatenträger	Nicht verfügbar
SUSE Linux Enterprise Server	Verfügbar im <b>net-snmp</b> -Paket über den Betriebssystem-Installationsdatenträger	Nicht verfügbar
VMware ESX 3.5 und 4.0	Verfügbar über das vom Betriebssystem installierte net-snmp-Paket	Verfügbarer
VMware ESXi 4.0	SNMP-Trap-Support verfügbar  <b>ANMERKUNG:</b> Während ESXi die SNMP-Traps unterstützt, unterstützt es nicht die Hardwarebestandsaufnahme über SNMP.	Verfügbarer

## Server Administrator-Startseite

Die Startseite von Server Administrator bietet einfach einrichtbare und leicht anwendbare, Web-Browser-basierte Systemverwaltungs-Tasks vom verwalteten System oder von einem Remote-Host über ein LAN, einen DFÜ-Dienst oder ein drahtloses Netzwerk. Wenn der Dell Systems Management Server Administrator-Verbindungsdienst (DSM SA-Verbindungsdienst) installiert und auf dem verwalteten System konfiguriert ist, können Sie Remote-Verwaltungsfunktionen von jedem System mit Internet-Browser und Verbindung ausführen. Zusätzlich enthält die Startseite von Server Administrator eine ausführliche, kontextabhängige Online-Hilfe.

## Weitere nützliche Dokumente

Auf der Dell Support-Website unter [support.dell.com/manuals](http://support.dell.com/manuals) sind außer dem vorliegenden *Benutzerhandbuch* auch folgende Dokumente zu finden:

- Die *Dell Systems Software Support-Matrix* bietet Informationen über die verschiedenen Dell-Systeme, die von diesen Systemen unterstützten Betriebssysteme und die Dell OpenManage-Komponenten, die auf diesen Systemen installiert werden können.
- Das *Installationshandbuch zu Dell OpenManage Server Administrator* enthält Anleitungen zur Installation von Dell OpenManage Server Administrator.
- Das *Installationshandbuch zur Dell OpenManage Management Station-Software* enthält Anleitungen zur Installation der Dell OpenManage Management Station-Software, die das Baseboard Management-Dienstprogramm, DRAC Tools und das Active Directory Snap-In enthält.
- Das *Dell OpenManage Server Administrator SNMP-Referenzhandbuch* enthält die SNMP-Verwaltungsinformationen-Datenbank (MIB). Die SNMP -MIB definiert Variablen, die die Standard-MIB erweitern, sodass sie die Fähigkeiten von Systemverwaltungsagenten einschließt.
- Das *Dell OpenManage Server Administrator CIM-Benutzerhandbuch* dokumentiert den Allgemeines Informationsmodell-Anbieter (CIM-Anbieter), eine Erweiterung der standardmäßigen Verwaltungsobjektformat-Datei (MOF-Datei). Das CIM-Anbieter-MOF dokumentiert unterstützte Klassen von Verwaltungsobjekten.
- Das *Dell OpenManage Server Administrator Meldungs-Referenzhandbuch* enthält die Meldungen, die im Warnungsprotokoll auf der Homepage des Server Administrators oder auf der Ereignisanzeige des Betriebssystems angezeigt werden. Das Handbuch erklärt Text, Schweregrad und Ursache jeder Instrumentation Service-Warnmeldung, die von Server Administrator ausgegeben wird.
- Das *Benutzerhandbuch für die Dell OpenManage Server Administrator Befehlszeilenschnittstelle* dokumentiert die gesamte Befehlszeilenschnittstelle (CLI) des Server Administrators, einschließlich einer Erklärung der CLI -Befehle, um den Systemstatus anzuzeigen, auf Protokolle zuzugreifen, Berichte zu erstellen, verschiedene Komponentenparameter zu konfigurieren und kritische Schwellenwerte festzulegen.
- Das *Benutzerhandbuch zum integrierten Dell Remote Access Controller* gibt detaillierte Auskunft über das Konfigurieren und Verwenden des iDRAC.
- Das *Dell Gehäuseverwaltungscontroller-Benutzerhandbuch* gibt detaillierte Auskunft über die Installation, Konfiguration und Verwendung des CMC.
- Das *Dell Online Diagnostics-Benutzerhandbuch* bietet umfassende Informationen über die Installation und Verwendung von Online Diagnostics auf Ihrem System.
- Das *Dell OpenManage Baseboard Management Controller Utilities-Benutzerhandbuch* enthält zusätzliche Informationen über die Verwendung von Server Administrator zur Konfiguration und Verwaltung des System-BMC.
- Das *Dell OpenManage Server Administrator Storage Management-Benutzerhandbuch* ist ein umfassendes Nachschlagewerk für die Konfiguration und Verwaltung lokaler und externer Speicherkomponenten, die an ein System angeschlossen sind.
- Das *Benutzerhandbuch zum Dell Remote Access Controller / Racadm* finden Sie Informationen zur Verwendung des racadm-Befehlszeilen-Dienstprogramms.
- Das *Dell Remote Access Controller 5-Benutzerhandbuch* bietet vollständige Informationen zur Installation und Konfiguration eines DRAC 5-Controllers und zur Verwendung des DRAC 5 für den Remote-Zugriff auf ein nichtbetriebsfähiges System.
- Das *Dell Update Packages-Benutzerhandbuch* enthält Informationen über Erhalten und Verwenden von Dell Update Packages als ein Teil Ihrer Systemaktualisierungsstrategie.
- Das *Dell OpenManage Server Update Utility-Benutzerhandbuch* bietet Informationen zum Erhalten und Verwenden des Server-Aktualisierungsdienstprogramms (SUU), um Dell-Systeme zu aktualisieren oder die Aktualisierungen einzusehen, die für alle im Repository aufgelisteten Systeme vorhanden sind.
- Das *Benutzerhandbuch der Dell Management Console* enthält Informationen zur Installation, Konfiguration und Nutzung der Dell Management Console. Dell Management Console ist eine webbasierte Systemverwaltungssoftware, mit der Sie Geräte in Ihrem Netzwerk ermitteln und inventarisieren können. Die Software bietet zudem erweiterte Funktionen, wie Zustands- und Leistungsüberwachung von vernetzten Geräten und Patch-Verwaltungsfunktionen

für Dell Systeme.

- 1 Das *Benutzerhandbuch zum Dell Life Cycle Controller* enthält Informationen zum Einrichten und Verwenden des Unified Server Configurator, um System- und Speicherwaltungs-Tasks über die gesamte Lebensdauer des Systems durchführen zu können. Sie können den Unified Server Configurator auch dazu verwenden, ein Betriebssystem bereitzustellen, ein redundantes Array unabhängiger Festplatten (RAID) zu konfigurieren und Diagnosen durchzuführen, um das System und die angeschlossene Hardware zu überprüfen. Die Fähigkeiten der Remote-Dienste ermöglichen die automatisierte Systemplattformermittlung durch Verwaltungskonsolen und verbessern die Bereitstellungsfähigkeiten für Betriebssysteme im Remote-Zugriff. Diese Funktionen nutzen die webdienstbasierte Hardwareverwaltungsschnittstelle der Lifecycle Controller-Firmware.
- 1 Das *Glossar*, das Informationen zu den in diesem Dokument verwendeten Begriffen bietet.

---

## Anfordern von technischer Unterstützung

Wenn Sie ein in diesem Handbuch beschriebenes Verfahren nicht verstehen, oder wenn Ihr Produkt nicht die erwartete Leistung erbringt, sind Hilfsprogramme vorhanden, um Ihnen zu helfen. Weitere Informationen zu diesen Hilfsprogrammen finden Sie unter "Wie Sie Hilfe bekommen" im *Hardware-Benutzerhandbuch* Ihres Systems.

Außerdem ist Dell Enterprise-Ausbildung und -Zertifizierung verfügbar; weitere Informationen finden Sie unter [www.dell.com/training](http://www.dell.com/training). Diese Dienstleistungen stehen unter Umständen nicht an allen Standorten zur Verfügung.

---

[Zurück zum Inhaltsverzeichnis](#)

[Zurück zum Inhaltsverzeichnis](#)

## Server Administrator-Protokolle

Dell™ OpenManage™ Server Administrator Version 6.2 Benutzerhandbuch

- [Übersicht](#)
- [Integrierte Funktionen](#)
- [Server Administrator-Protokolle](#)

---

### Übersicht

Server Administrator ermöglicht die Anzeige und Verwaltung von Hardware-, Warnungs- und Befehlsprotokollen. Alle Benutzer können entweder von der Homepage von Server Administrator oder von seiner Befehlszeilenschnittstelle auf Protokolle zugreifen und Berichte drucken. Benutzer müssen mit Administrator-Berechtigungen angemeldet sein, um Protokolle zu löschen, oder sie müssen mit Admin- oder Hauptbenutzer-Berechtigungen angemeldet sein, um E-Mail-Protokolle an ihren festgelegten Dienstkontakt zu senden.

Informationen zum Anzeigen von Protokollen und dem Erstellen von Reporten von der Befehlszeile finden Sie hier: *Dell™ OpenManage™ Server Administrator-Befehlszeilenoberfläche: Benutzerhandbuch*.

Beim Anzeigen der Server Administrator-Protokolle können Sie auf der allgemeinen Navigationsleiste auf **Hilfe** klicken, um detaillierte Informationen über das Fenster zu erhalten, das gerade zu sehen ist. Server Administrator-Protokollhilfe ist in allen Fenstern verfügbar, die dem Benutzer zugänglich sind, basierend auf den entsprechenden Zugriffsrechten und den spezifischen Hardware- und Softwaregruppen, die Server Administrator auf dem verwalteten System feststellt.

---

### Integrierte Funktionen

Klicken Sie auf eine Spaltenüberschrift, um den Inhalt der Spalte zu sortieren oder die Sortierreihenfolge zu ändern. Außerdem enthält jedes Protokollfenster mehrere Task-Schaltflächen, die zur Verwaltung und Unterstützung des Systems verwendet werden können.

### Protokollfenster-Task-Schaltflächen

- 1 Klicken Sie auf **Drucken**, um eine Kopie des Protokolls auf dem Standarddrucker auszugeben.
- 1 Klicken Sie auf **Exportieren**, um eine Textdatei mit den Protokoll Daten (in der die Werte aller Datenfelder durch ein benutzerdefiniertes Begrenzungszeichen getrennt sind) an einem von Ihnen festgelegten Ort zu speichern.
- 1 Klicken Sie auf **E-Mail**, um eine E-Mail-Nachricht zu erstellen, die den Inhalt des Protokolls als Anhang mitsendet.
- 1 Klicken Sie auf **Protokoll löschen**, um alle Ereignisse aus dem Protokoll zu löschen.
- 1 Klicken Sie auf **Speichern unter**, um den Protokollinhalt in einer ZIP-Datei zu speichern.
- 1 Klicken Sie auf **Aktualisieren**, um den Protokollinhalt wieder in den Datenbereich des Maßnahmenfensters zu laden.

Unter "[Task-Schaltflächen](#)" erhalten Sie weitere Informationen über die Task-Schaltflächen.

---

### Server Administrator-Protokolle

Server Administrator enthält die folgenden Protokolle:

- 1 "[Hardware-Protokoll](#)"
- 1 "[Warnungsprotokoll](#)"
- 1 "[Befehlsprotokoll](#)"

### Hardware-Protokoll

Verwenden Sie das Hardware-Protokoll zur Suche nach potenziellen Problemen bei den Hardwarekomponenten des Systems. Auf Dell PowerEdge™ x8xx-, x9xx- und xx1x-Systemen ändert sich die Hardwareprotokoll-Statusanzeige zum kritischen Status (  ), wenn die Protokolldatei 100-Prozent-Kapazität erreicht. Es gibt zwei verfügbare Hardwareprotokolle, abhängig vom System: das ESM-Protokoll (Embedded System Management-Protokoll) und das SEL-Protokoll (Systemereignisprotokoll). Das ESM- und das SEL-Protokoll bestehen jeweils aus einem Satz von integrierten Anweisungen, die Hardwarestatusmeldungen an die Systemverwaltungssoftware senden können. Jede in den Protokollen verzeichnete Komponente hat ein

Statusanzeigensymbol neben der Bezeichnung. Ein grünes Kontrollhäkchen (  ) zeigt an, dass eine Komponente in Ordnung (normal) ist. Ein gelbes Dreieck mit einem Ausrufezeichen (  ) zeigt an, dass für eine Komponente ein Warnzustand (nicht kritisch) besteht, der sofortige Aufmerksamkeit erfordert.

Ein rotes X (  ) zeigt eine kritische Bedingung (Ausfall) für eine Komponente an, die einen sofortigen Eingriff erfordert. Eine Leerstelle (  ) bedeutet, dass der Zustand der Komponente unbekannt ist.

Zum Zugriff auf das Hardware-Protokoll klicken Sie auf **System**, dann auf das **Register Protokolle** und auf **Hardware**.

In den ESM- und SEL-Protokollen enthaltene Informationen umfassen:

- 1 Den Schweregrad des Ereignisses
- 1 Datum und Uhrzeit, zu der das Ereignis erfasst wurde
- 1 Eine Beschreibung des Ereignisses

## Aufrechterhalten des Hardwareprotokolls

Das Statusanzeigesymbol neben dem Protokollnamen auf der Server Administrator-Homepage wird sich von normalem Status (  ) zu nicht-kritischem Status (  ) ändern, wenn die Protokolldatei 80-Prozent Kapazität erreicht. Löschen Sie das Hardwareprotokoll, wenn es 80-Prozent-Kapazität erreicht. Wenn dem Protokoll erlaubt wird, 100-Prozent-Kapazität zu erreichen, werden die spätesten Ereignisse vom Protokoll abgelegt.

## Warnungsprotokoll

 **ANMERKUNG:** Wenn das Warnungsprotokoll ungültige XML-Daten anzeigt (wenn zum Beispiel die für die Auswahl generierten XML-Daten nicht gut formatiert sind), dann klicken Sie auf **Protokoll löschen** und lassen die Protokolldaten noch einmal anzeigen.

Mit dem Warnungsprotokoll können verschiedene Systemereignisse überwacht werden. Server Administrator erzeugt Ereignisse als Reaktion auf Änderungen im Status von Sensoren und anderen überwachten Parametern. Jedes Statusänderungsereignis, das im Warnungsprotokoll aufgezeichnet wird, besteht aus einem eindeutigen Bezeichner, genannt Ereignis-ID, für die spezifische Ereigniskategorie und einer Ereignismeldung, die das Ereignis beschreibt. Ereignis-ID und -Meldung beschreiben den Schweregrad und die Ursache des Ereignisses eindeutig und enthalten weitere relevante Informationen wie z. B. die Stelle des Ereignisses und den vorherigen Status der überwachten Komponente.

Zum Zugriff auf das Warnungsprotokoll klicken Sie auf **System**, dann auf das Register **Protokolle** und auf **Warnung**.

Im Warnungsprotokoll enthaltene Informationen umfassen:

- 1 Den Schweregrad des Ereignisses
- 1 Die Ereignis-ID
- 1 Datum und Uhrzeit, zu der das Ereignis erfasst wurde
- 1 Die Kategorie des Ereignisses
- 1 Eine Beschreibung des Ereignisses

 **ANMERKUNG:** Die Protokollhistorie kann später zur Behebung von Störungen oder für Diagnosezwecke erforderlich werden. Es wird deshalb empfohlen, die Protokolldateien zu speichern.

Im *Server Administrator-Meldungs-Referenzhandbuch* erhalten Sie detaillierte Informationen über Warnungsmeldungen.

## Befehlsprotokoll

 **ANMERKUNG:** Wenn das Befehlsprotokoll ungültige XML-Daten anzeigt (wenn zum Beispiel die für die Auswahl generierten XML-Daten nicht gut formatiert sind), dann klicken Sie auf **Protokoll löschen** und lassen die Protokolldaten noch einmal anzeigen.

Verwenden Sie das Befehlsprotokoll zur Überwachung aller vom Server Administrator ausgegebenen Befehle. Das Befehlsprotokoll verzeichnet An- und Abmeldungen, Systemverwaltungssoftware-Initialisierung und von der Systemverwaltungssoftware eingeleitetes Herunterfahren, und berichtet den Zeitpunkt, zu dem das Protokoll zuletzt gelöscht wurde. Die Größe der Befehlsprotokolldatei kann laut Ihrer Anforderung angegeben werden.

Zum Zugriff auf das Befehlsprotokoll klicken Sie auf **System**, dann auf das Register **Protokolle** und auf **Befehl**.

Im Befehlsprotokoll enthaltene Informationen umfassen:

- 1 Datum und Uhrzeit, zu der der Befehl gegeben wurde
- 1 Benutzer, der derzeit auf der Server Administrator-Homepage oder der CLI angemeldet ist
- 1 Eine Beschreibung des Befehls und seiner zugehörigen Werte

 **ANMERKUNG:** Die Protokollhistorie kann später zur Behebung von Störungen oder für Diagnosezwecke erforderlich werden. Es wird deshalb empfohlen, die Protokolldateien zu speichern.

---

[Zurück zum Inhaltsverzeichnis](#)

## Arbeiten mit dem Remote Access Controller

Dell™ OpenManage™ Server Administrator Version 6.2 Benutzerhandbuch

- [Übersicht](#)
- [Anzeigen grundlegender Informationen](#)
- [Konfigurieren des Remote-Zugriffsgeräts zur Verwendung einer LAN-Verbindung](#)
- [Konfigurieren des Remote-Zugriffsgeräts zur Verwendung der Verbindung einer seriellen Schnittstelle](#)
- [Konfigurieren des Remote-Zugriffsgeräts zur Verwendung einer Seriell-über-LAN-Verbindung](#)
- [Zusätzliche Konfiguration für iDRAC](#)
- [Konfigurieren der Benutzer von Remote- Zugriffsgeräten](#)
- [Plattformereignisfilter-Warnungen einstellen](#)

**ANMERKUNG:** Der Baseboard Management Controller (BMC) wird auf Dell™ PowerEdge™ x8xx- und x9xx-Systemen unterstützt, der iDRAC (Integrated Dell Remote Access Controller) auf Dell xx0x- und xx1x-Systemen.

### Übersicht

Dieses Kapitel bietet Informationen zum Zugreifen auf die Remote-Zugriffs-Funktionen von BMC/iDRAC und DRAC und zu deren Verwendung.

Der Dell BMC/iDRAC (Baseboard Management Controller/Integrated Dell Remote Access Controller) überwacht das System auf kritische Ereignisse, indem er mit verschiedenen Sensoren auf der Systemplatine kommuniziert und Warnungen und Protokollereignisse sendet, wenn bestimmte Parameter die voreingestellten Schwellenwerte überschreiten. Der BMC/iDRAC unterstützt die Industriestandards bei Intelligent Platform Management Interfaces (IPMI), sodass Sie Systeme im Remote-Zugriff konfigurieren, überwachen oder wiederherstellen können.

Der DRAC ist eine Hardware- und Softwarelösung zur Systemverwaltung und ermöglicht die Remote-Verwaltung, die Wiederherstellung eines abgestürzten Systems sowie die Stromsteuerungsfunktionen für Dell-Systeme.

Durch die Kommunikation mit dem BMC/iDRAC (Baseboard Management Controller/Integrated Dell Remote Access Controller) des Systems kann der DRAC für das Senden von E-Mail-Warnungen mit Warn- oder Fehlermeldungen zu Spannung, Temperatur und Lüftergeschwindigkeit konfiguriert werden. Der DRAC protokolliert außerdem Ereignisdaten und den letzten Bildschirm vor dem Absturz (nur für Systeme, die das Betriebssystem Microsoft® Windows® ausführen), um Ihnen bei der Diagnose der möglichen Ursachen eines Systemfehlers behilflich zu sein.

Der Remote Access Controller gestattet externen Zugriff auf ein nicht funktionierendes System, wodurch es schnellstmöglich wieder in einen funktionierenden Zustand versetzt werden kann. Der Remote Access Controller leistet ebenfalls Warnungsbearbeitung, wenn ein System ausgefallen ist, und ermöglicht den externen Neustart eines Systems. Darüber hinaus protokolliert der Remote Access Controller die wahrscheinliche Ursache von Systemabstürzen und speichert den letzten Absturzbildschirm.

Sie können sich beim Remote Access Controller anmelden, entweder über die Server Administrator-Homepage oder durch direktes Zugreifen auf die IP-Adresse des Controllers mit einem unterstützten Browser.

Bei der Verwendung des Remote Access Controller können Sie auf der allgemeinen Navigationsleiste auf **Hilfe** klicken, um detaillierte Informationen über das Fenster zu erhalten, in dem Sie sich gerade befinden. Remote Access Controller-Hilfe ist in allen Fenstern verfügbar, die dem Benutzer zugänglich sind, basierend auf den entsprechenden Zugriffsrechten und den spezifischen Hardware- und Softwaregruppen, die der Server Administrator auf dem verwalteten System feststellt.

**ANMERKUNG:** Weitere Informationen über den BMC erhalten Sie im *Dell OpenManage™ Baseboard-Verwaltungs-Controller: Dienstprogramm-Benutzerhandbuch*.

**ANMERKUNG:** Weitere Informationen über die Verwendung von DRAC 4 erhalten Sie im *Dell Remote Access Controller 4: Benutzerhandbuch* und weitere Informationen über die Verwendung von DRAC 5 erhalten Sie im *Dell Remote Access Controller 5: Benutzerhandbuch*.

**ANMERKUNG:** Das *Dell Integrated Remote Access Controller-Benutzerhandbuch* enthält ausführliche Informationen über die Konfiguration und Verwendung des iDRAC.

[Tabelle 5-1](#) listet die Feldnamen der Benutzeroberfläche und das zutreffende System auf, wenn Server Administrator auf dem System installiert ist.

**Tabelle 5-1. Systemverfügbarkeit für die folgenden Feldnamen der Benutzeroberfläche**

Feldname der Benutzeroberfläche	Zutreffendes System
Modulares Gehäuse	Modulares System
Servermodul	Modulares System
Hauptsystem	Modulares System
System	Nicht modulares System
Hauptsystemgehäuse	Nicht modulares System

Die *Dell Systems Software Support Matrix* bietet weitere Informationen zur Systemunterstützung für Remote-Zugriffsgeräte.

Der Server Administrator ermöglicht den bandinternen Remote-Zugriff auf Ereignisprotokoll-, Stromsteuerungs- und Sensorstatusdaten, und er ermöglicht das Konfigurieren des BMC/iDRAC. Sie können den BMC/iDRAC und den DRAC über die grafische Benutzeroberfläche von Server Administrator verwalten, indem Sie auf das Objekt **Remote-Zugriff** klicken, welches eine Unterkomponente der Gruppe **Hauptsystemgehäuse/Hauptsystem** ist. Sie können folgende Aufgaben ausführen:

- 1 Grundlegende Informationen anzeigen
- 1 Das Remote-Zugriffsgerät auf einer LAN-Verbindung konfigurieren
- 1 Das Remote-Zugriffsgerät auf einer Seriell-über-LAN-Verbindung konfigurieren

- 1 Das Remote-Zugriffsgerät auf der Verbindung einer seriellen Schnittstelle konfigurieren
- 1 Zusätzliche Eigenschaften des Remote-Zugriffsgeräts konfigurieren
- 1 Benutzer auf dem Remote-Zugriffsgerät konfigurieren
- 1 Plattformereignisfilter-Warnungen einrichten

Sie können BMC/iDRAC- oder DRAC-Informationen basierend auf der Hardware ansehen, die die Remote-Zugriffsfähigkeiten für das System bietet.

Berichterstattung und Konfiguration von BMC/iDRAC und DRAC können auch mithilfe des CLI-Befehls `omreport/omconfig chassis remoteaccess` verwaltet werden.

Außerdem können Sie den Server Administrator Instrumentation Service für die Verwaltung der Parameter und Warnungsziele des Plattformereignisfilters (PEF) verwenden.

 **ANMERKUNG:** Sie können BMC-Daten nur auf Dell PowerEdge x8xx- und x9xx-Systemen ansehen.

---

## Anzeigen grundlegender Informationen

Sie können grundlegende Informationen zu BMC/iDRAC, zur IPv4-Adresse und zum DRAC anzeigen. Sie haben auch die Möglichkeit, die BMC-Einstellungen auf ihre Standardwerte zurückzusetzen. Führen Sie dazu folgende Schritte durch:

 **ANMERKUNG:** Um die BMC-Einstellungen einzustellen, müssen Sie mit Admin-Zugriffsrechten angemeldet sein.

1. Klicken Sie auf das Objekt **Modulares Gehäuse** → **System/Servermodul** → **Hauptsystemgehäuse/Hauptsystem** → **Remote- Zugriff**.

Die Seite **Remote-Zugriff** zeigt folgende Basisinformationen für den System-BMC:

### Remote-Zugriffsgerät

- 1 Gerätetyp
- 1 IPMI-Version
- 1 System-GUID
- 1 Anzahl von möglichen aktiven Sitzungen
- 1 Anzahl von aktuellen aktiven Sitzungen
- 1 LAN aktiviert
- 1 SOL aktiviert
- 1 MAC-Adresse

### IPv4-Adresse

- 1 IP-Adressen-Quelle
- 1 IP-Adresse
- 1 IP-Subnetz
- 1 IP-Gateway

### IPv6-Adresse

- 1 IP-Adressen-Quelle
- 1 IPv6-Adresse 1
- 1 Standard-Gateway
- 1 IPv6-Adresse 2
- 1 Lokale Adresse verbinden
- 1 DNS-Adressenquelle
- 1 Bevorzugter DNS-Server
- 1 Alternativer DNS-Server

 **ANMERKUNG:** Details zu den IPv4- und IPv6-Adressen können nur angezeigt werden, wenn Sie die IPv4- und IPv6-Adresseneigenschaften auf der Registerkarte **Remote-Zugriff** unter **Zusätzliche Konfiguration** aktivieren.

---

## Konfigurieren des Remote-Zugriffsgeräts zur Verwendung einer LAN-Verbindung

 **ANMERKUNG:** Die **LAN-Konfiguration**-Felder werden schreibgeschützt angezeigt, wenn sie für Inband-Benutzer als *deaktiviert* konfiguriert sind.

Sie können das Remote-Zugriffsgerät für die Kommunikation über eine LAN-Verbindung konfigurieren. Führen Sie dazu folgende Schritte durch:

1. Klicken Sie auf das Objekt **Modulares Gehäuse**→ **System/Servermodul**→ **Hauptsystemgehäuse/Hauptsystem**→ **Remote- Zugriff**.
2. Klicken Sie auf das Register **Konfiguration**.
3. Klicken Sie auf **LAN**.

Das Fenster **LAN-Konfiguration** wird angezeigt.

 **ANMERKUNG:** BMC/iDRAC-Verwaltungsverkehr funktioniert nicht richtig, wenn das LAN auf der Hauptplatine (LOM) mit Netzwerkadapter-Add-In-Karten geteamt wird.

4. Konfigurieren Sie folgende NIC-Konfigurationsdaten:

- 1 NIC aktivieren (Diese Option ist auf Dell PowerEdge x9xx-Systemen verfügbar und wenn DRAC installiert ist. Wählen Sie diese Option für das NIC-Teaming aus. In Dell PowerEdge x9xx-Systemen können Sie NICs für zusätzliche Redundanz als Team definieren.)

 **ANMERKUNG:** Die DRAC enthält einen integrierten 10BASE-T/100BASE-T Ethernet-NIC und unterstützt TCP/IP. Der NIC hat die Standardadresse 192.168.20.1 und den Standard-Gateway 192.168.20.1.

 **ANMERKUNG:** Wenn der DRAC auf die gleiche IP-Adresse wie ein anderer NIC auf dem gleichen Netzwerk eingestellt ist, tritt ein IP-Adressenkonflikt auf. Der DRAC antwortet nicht mehr auf Netzwerkbefehle, bis die IP-Adresse auf dem DRAC geändert wird. Der DRAC muss selbst dann zurückgesetzt werden, wenn der IP-Adressenkonflikt durch Änderung der IP-Adresse des anderen NIC aufgelöst wird.

 **ANMERKUNG:** Eine Änderung der IP-Adresse des DRAC bewirkt, dass der DRAC zurückgesetzt wird. Wenn SNMP den DRAC abfragt, bevor er initialisiert wird, wird eine Temperaturwarnmeldung protokolliert, da die korrekte Temperatur erst nach der Initialisierung des DRAC übertragen wird.

- 1 NIC-Auswahl

 **ANMERKUNG:** Die **NIC-Auswahl** kann auf modularen Systemen nicht konfiguriert werden.

- 1 IPMI-über-LAN aktivieren
- 1 IP-Adressen-Quelle
- 1 IP-Adresse
- 1 Subnetzmaske
- 1 Gateway-Adresse
- 1 Beschränkung der Kanalberechtigungsebene
- 1 Neuer Verschlüsselungsschlüssel (Diese Option ist auf Dell PowerEdge x9xx-Systemen verfügbar.)

5. Konfigurieren Sie die folgenden optionalen VLAN-Konfigurationsdetails:

 **ANMERKUNG:** VLAN-Konfiguration ist nicht anwendbar für Systeme mit iDRAC.

- 1 VLAN-ID aktivieren
- 1 VLAN-ID
- 1 Priorität

6. Konfigurieren Sie die folgenden IPv4-Eigenschaften:

- 1 IP-Adressen-Quelle
- 1 IP-Adresse
- 1 Subnetzmaske
- 1 Gateway-Adresse

7. Konfigurieren Sie die folgenden IPv6-Eigenschaften:

- 1 IP-Adressen-Quelle
- 1 IP-Adresse
- 1 Präfixlänge
- 1 Standard-Gateway
- 1 DNS-Adressenquelle
- 1 Bevorzugter DNS-Server
- 1 Alternativer DNS-Server

 **ANMERKUNG:** Details zu den IPv4- und IPv6-Adressen können nur konfiguriert werden, wenn Sie die IPv4- und IPv6-Eigenschaften unter **Zusätzliche Konfiguration** aktivieren.

8. Klicken Sie auf **Änderungen anwenden**.
- 

## Konfigurieren des Remote-Zugriffsgeräts zur Verwendung der Verbindung einer seriellen Schnittstelle

Sie können den BMC für die Kommunikation über eine serielle Schnittstellenverbindung konfigurieren. Führen Sie dazu folgende Schritte durch:

1. Klicken Sie auf das Objekt **Modulares Gehäuse**→ **System/Servermodul**→ **Hauptsystemgehäuse/Hauptsystem**→ **Remote- Zugriff**.
2. Klicken Sie auf das Register **Konfiguration**.
3. Klicken Sie auf **Serielle Schnittstelle**.

Das Fenster **Konfiguration der seriellen Schnittstelle** wird angezeigt.

4. Konfigurieren Sie folgende Details:

- 1 Verbindungsmoduseinstellung
- 1 Baudrate
- 1 Ablaufsteuerung
- 1 Beschränkung der Kanalberechtigungsebene

5. Klicken Sie auf **Änderungen anwenden**.

6. Klicken Sie auf **Terminalmoduseinstellungen**.

Im Fenster **Terminalmoduseinstellungen** können Sie die Terminalmoduseinstellungen für die serielle Schnittstelle konfigurieren.

Der Terminalmodus wird für Intelligent Plattform Schnittstellenmanagement (IPMI)-Meldungen über die serielle Schnittstelle unter Verwendung von druckbaren ASCII-Zeichen benutzt. Der Terminalmodus unterstützt auch eine begrenzte Zahl an Textbefehlen für die Unterstützung von alten textbasierten Umgebungen. Diese Umgebung ist so gestaltet, dass ein einfaches Terminal oder ein Terminalemulator verwendet werden kann.

7. Legen Sie folgende benutzerspezifische Daten fest, um die Kompatibilität mit ihren bestehenden Terminals zu erhöhen:

- 1 Zeilenbearbeitung
- 1 Löschrücksteuerung
- 1 Echo-Steuerung
- 1 Handshaking-Steuerung
- 1 Neue Zeilenreihenfolge
- 1 Neue Zeilenreihenfolge eingeben

8. Klicken Sie auf **Änderungen übernehmen**.

9. Klicken Sie auf **Zurück zum Fenster Konfiguration der seriellen Schnittstelle**, um zum Fenster **Konfiguration der seriellen Schnittstelle** zu wechseln.
- 

## Konfigurieren des Remote-Zugriffsgeräts zur Verwendung einer Seriell-über-LAN-Verbindung

Sie können den BMC/iDRAC für Datenübertragung einer Seriell über LAN (SOL)-Verbindung konfigurieren. Führen Sie dazu folgende Schritte durch:

1. Klicken Sie auf das Objekt **Modulares Gehäuse**→ **System/Servermodul**→ **Hauptsystemgehäuse/Hauptsystem**→ **Remote- Zugriff**.
2. Klicken Sie auf das Register **Konfiguration**.
3. Klicken Sie auf **Seriell über LAN**.

Das Fenster **Seriell über LAN - Konfiguration** wird angezeigt.

4. Konfigurieren Sie folgende Details:

- 1 Seriell über LAN aktivieren
- 1 Baudrate
- 1 Erforderliche Mindestberechtigung

5. Klicken Sie auf **Änderungen anwenden**.
  6. Klicken Sie auf **Erweiterte Einstellungen**, um den BMC weiter zu konfigurieren.
  7. Im Fenster **Seriell über LAN - Konfiguration - Erweiterte Einstellungen** können Sie die folgenden Informationen konfigurieren:
    - 1 ?Intervall der Zeichenakkumulation
    - 1 Schwellenwert der gesendeten Zeichen
  8. Klicken Sie auf **Änderungen anwenden**.
  9. Klicken Sie auf **Zurück zu Seriell über LAN - Konfiguration**, um zum Fenster **Seriell über LAN - Konfiguration** zurückzukehren.
- 

## Zusätzliche Konfiguration für iDRAC

Sie können die IPv4- und IPv6-Eigenschaften unter Verwendung des Registers **Zusätzliche Konfiguration** konfigurieren. Führen Sie dazu folgende Schritte durch:

1. Klicken Sie auf das Objekt **Modulares Gehäuse**→ **System/Servermodul**→ **Hauptsystemgehäuse/Hauptsystem**→ **Remote-Zugriff**.
  2. Klicken Sie auf das Register **Konfiguration**.
  3. Klicken Sie auf **Zusätzliche Konfiguration**.
  4. Konfigurieren Sie die IPv4- und IPv6-Eigenschaften als **Aktiviert** oder **Deaktiviert**.
  5. Klicken Sie auf **Änderungen anwenden**.
- 

## Konfigurieren der Benutzer von Remote- Zugriffsgeräten

Die Benutzer von Remote-Zugriffsgeräten können über die Seite **Remote-Zugriff** konfiguriert werden. So greifen Sie auf die Seite zu:

1. Klicken Sie auf das Objekt **Modulares Gehäuse**→ **System/Servermodul**→ **Hauptsystemgehäuse/Hauptsystem**→ **Remote- Zugriff**.
2. Klicken Sie auf das Register **Benutzer**.

Im Fenster **Remote-Zugriffsbenutzer** werden Informationen über Benutzer angezeigt, die ein BMC/iDRAC-Benutzer konfigurieren kann.
3. Klicken Sie auf **Benutzer-ID**, um einen neuen oder bestehenden BMC/iDRAC-Benutzer zu konfigurieren.

Im Fenster **Benutzerkonfiguration für Remote-Zugriff** können Sie einen bestimmten BMC/iDRAC-Benutzer konfigurieren.
4. Legen Sie folgende allgemeine Informationen fest:
  - 1 Zur Aktivierung eines Benutzers wählen Sie **Benutzer aktivieren**.
  - 1 Geben Sie einen Namen für den Benutzer in das Feld **Benutzername** ein.
  - 1 Wählen Sie das Kontrollkästchen **Kennwort ändern** aus.
  - 1 Geben Sie ein neues Kennwort in das Feld **Neues Kennwort** ein.
  - 1 Geben Sie das gleiche Kennwort in das Bestätigungsfeld **Neues Kennwort bestätigen** ein.
5. Legen Sie folgende Benutzerberechtigungen fest:
  - 1 Wählen Sie die maximalen Beschränkungen für LAN-Benutzerberechtigungsebenen.
  - 1 Wählen Sie maximal gewährte serielle Schnittstellen-Benutzerberechtigung.
  - 1 Auf Dell PowerEdge x9xx-Systemen wählen Sie "Seriell über LAN aktivieren" aus, um Seriell über LAN zu aktivieren.
6. Geben Sie die Benutzergruppe für die DRAC/iDRAC- Benutzerberechtigungen an.
7. Klicken Sie auf **Änderungen anwenden**, um Änderungen zu speichern.
8. Klicken Sie auf **Zurück zum Fenster Remote-Zugriffsbenutzer**, um zum Fenster **Remote-Zugriffsbenutzer** zurückzukehren.

 **ANMERKUNG:** Sechs zusätzliche Benutzereinträge sind konfigurierbar, wenn DRAC installiert ist. Dies läuft auf insgesamt 16 Benutzer hinaus. Dieselben Benutzername- und Kennwortregeln sind für BMC/iDRAC- und RAC-Benutzer anwendbar. Wenn DRAC/iDRAC6 installiert ist, werden alle 16 Benutzereinträge DRAC zugewiesen.

## Plattformereignisfilter-Warnungen einstellen

Sie können den Server Administrator-Instrumentation Service zur Konfiguration der wichtigsten BMC-Funktionen wie Parameter und Warnungsziele des Plattformereignisfilters (PEF) verwenden. Führen Sie dazu folgende Schritte durch:

1. Klicken Sie auf das Objekt **System**.
2. Klicken Sie auf das Register **Alarmverwaltung**.
3. Klicken Sie auf **Plattformereignisse**.

Über das Fenster **Plattformereignisse** können Sie einzelne Maßnahmen für bestimmte Plattformereignisse ergreifen. Sie können die Ereignisse auswählen, bei denen Sie Maßnahmen zum Herunterfahren ergreifen wollen, und Warnungen für ausgewählte Maßnahmen generieren. Sie können auch Warnungen an bestimmte IP-Adressen Ihrer Wahl senden.

-  **ANMERKUNG:** Sie müssen mit Administrator-Berechtigungen angemeldet werden, um die BMC Plattform-Ereignis-Filterwarnungen zu konfigurieren.
-  **ANMERKUNG:** Mit den Einstellungen unter **Plattformereignisfilter-Warnungen aktivieren** kann die Generierung von Plattformereignisfilter-Warnungen deaktiviert oder aktiviert werden. Diese Einstellungen sind unabhängig von den einzelnen Plattformereignis-Warnungseinstellungen.
-  **ANMERKUNG:** **Systemstromsondenwarnungen** und **Systemstromsondenfehler** werden auf Dell-Systemen nicht ohne PMBus-Unterstützung unterstützt, wobei Server Administrator eine Konfiguration jedoch gestattet.
-  **ANMERKUNG:** Auf Dell PowerEdge 1900-Systemen werden die Plattformereignisfilter **PS/VRM/D2D-Warnung**, **PS/VRM/D2D-Fehler** und **Netzteil nicht vorhanden** nicht unterstützt, obwohl Server Administrator Ihnen erlaubt, diese Ereignisfilter zu konfigurieren.

4. Wählen Sie das Plattformereignis aus, für das Sie Maßnahmen zum Herunterfahren ergreifen wollen, oder generieren Sie Warnungen für ausgewählte Maßnahmen und klicken dann auf **Plattformereignisse festlegen**.

Im Fenster **Plattformereignisse festlegen** können Sie Maßnahmen festlegen, die getroffen werden sollen, wenn das System aufgrund eines Plattformereignisses heruntergefahren werden soll.

5. Wählen Sie eine der folgenden Maßnahmen:
  - 1 **Keine**  
Führt keine Aktion durch, wenn das Betriebssystem gesperrt oder abgestürzt ist.
  - 1 **System neustarten**  
Führt das Betriebssystem herunter und leitet einen Systemstart ein, wobei BIOS-Überprüfungen durchgeführt werden und das Betriebssystem neu geladen wird.
  - 1 **System aus- und wieder einschalten (Power Cycle)**  
Mit "Power Cycle" wird die Stromversorgung des Systems aus- und nach einer kurzen Pause wieder eingeschaltet; danach wird das System neu gestartet. Das Aus- und Einschalten ist dann nützlich, wenn Systemkomponenten wie Festplatten neu initialisiert werden sollen.
  - 1 **System ausschalten**  
Unterbricht die Stromzufuhr zum System.
  - 1 **Stromverminderung**  
Drosselt die CPU.

 **ANMERKUNG:** Stromverminderung wird nicht auf allen Systemen unterstützt.

 **VORSICHTSHINWEIS:** Wenn Sie eine Plattformereignis-Maßnahme zum Herunterfahren außer Keine oder Stromverminderung auswählen, wird Ihr System zwingend heruntergefahren, wenn das angegebene Ereignis vorkommt. Dieses Herunterfahren wird von der Firmware gestartet und wird ausgeführt, ohne das Betriebssystem oder jegliche Anwendungen herunterzufahren.

6. Wählen Sie am Kontrollkästchen **Warnung generieren** das Senden von Warnungen aus.

 **ANMERKUNG:** Zur Generierung einer Warnung muss sowohl die Einstellung **Warnung generieren** als auch die Einstellung **Plattformereigniswarnungen aktivieren** ausgewählt werden.

7. Klicken Sie auf **Änderungen übernehmen**.
8. Klicken Sie auf **Zurück zur Plattformereignisseite**, um zum Fenster **Plattformereignisfilter** zurückzukehren.

## Plattformereigniswarnungsziele einstellen

Sie können auch über das Fenster **Plattformereignisfilter** ein Ziel auswählen, an das eine Warnung über ein Plattformereignis gesendet werden soll. Je nachdem, wie viele Ziele angezeigt werden, können Sie eine separate IP-Adresse für jede Zieladresse konfigurieren. Eine Plattformereigniswarnung wird an jede Ziel-IP-Adresse gesandt, die Sie konfigurieren.

1. Klicken Sie auf **Ziele konfigurieren** im Fenster **Plattformereignisfilter**.

Im Fenster **Ziele konfigurieren** erscheint eine Reihe von Zielen.

2. Klicken Sie auf die Nummer des Zieles, das Sie konfigurieren möchten.

 **ANMERKUNG:** Die Zahl der Ziele, die Sie in einem bestimmten System konfigurieren können, kann variieren.

3. Wählen Sie das Kontrollkästchen **Ziel aktivieren** aus.

4. Klicken Sie auf **Zielnummer**, um eine eigene IP-Adresse für dieses Ziel einzugeben. Diese IP-Adresse ist die IP-Adresse, an die die Plattformereigniswarnung gesendet wird.

5. Geben Sie einen Wert in das Feld **Community-Zeichenkette** ein, der als Kennwort für die Authentifizierung von Meldungen dient, die zwischen einer Verwaltungsstation und einem verwalteten System hin- und hergesandt werden. Die Community-Zeichenkette (auch Community- Name genannt) wird mit jedem Paket mitgesandt, das zwischen der Verwaltungsstation und einem verwalteten System unterwegs ist.

6. Klicken Sie auf **Änderungen anwenden**.

7. Klicken Sie auf **Zurück zur Plattformereignisseite**, um zum Fenster **Plattformereignisfilter** zurückzukehren.

---

[Zurück zum Inhaltsverzeichnis](#)

# Setup und Administration

## Dell™ OpenManage™ Server Administrator Version 6.2 Benutzerhandbuch

- [Sicherheitsverwaltung](#)
- [Benutzerberechtigungen zuweisen](#)
- [Gastkonten und anonyme Konten in unterstützten Windows-Betriebssystemen deaktivieren](#)
- [SNMP-Agenten konfigurieren](#)
- [Firewall-Konfiguration auf Systemen, die unterstützte Red Hat Enterprise Linux- Betriebssysteme und SUSE Linux Enterprise Server ausführen](#)

## Sicherheitsverwaltung

Der Server Administrator bietet Sicherheit durch rollenbasierte Zugriffsregelung (RBAC), Authentisierung und Verschlüsselung für die Internet-basierte und die Befehlszeilen-Schnittstelle.

## Funktionsbasierte Zugriffssteuerung

RBAC erreicht Sicherheit durch Festlegung der Vorgänge, die von Personen in besonderen Funktionen ausgeführt werden können. Jedem Benutzer werden eine oder mehrere Rollen zugeteilt und jeder Rolle sind eine oder mehrere Benutzerberechtigungen zugewiesen, die für die Benutzer in dieser Rolle zugelassen sind. Mit RBAC entspricht Sicherheitsverwaltung genau der Organisationsstruktur.

## Benutzerberechtigungen

Server Administrator gewährt unterschiedliche Zugriffsrechte basierend auf den dem Benutzer zugewiesenen Gruppenberechtigungen. Die vier Benutzerebenen lauten: Benutzer, Hauptbenutzer, Administrator und Administrator mit erhöhten Rechten.

- 1 *Benutzer* können die meisten Informationen anzeigen.
- 1 *Hauptbenutzer* können Warnungsgrenzwerte einstellen und konfigurieren, welche Warnungsmaßnahmen ausgeführt werden sollen, wenn ein Warnungs- oder Fehlerereignis eintritt.
- 1 *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 das System auch konfigurieren, um E-Mails zu senden.
- 1 *Administratoren mit erhöhten Rechten* können Informationen anzeigen und verwalten.

Der Server Administrator erteilt Benutzern, die mit *Benutzerberechtigungen* angemeldet sind, schreibgeschützten Zugriff. Benutzer mit *Hauptbenutzerberechtigungen* erhalten Lese- und Schreibzugriff, während Benutzer, die mit *Administratorrechten* oder *erhöhten Administratorrechten* angemeldet sind, Lese-, Schreib- und Administrator-Zugriffsrechte erhalten. Siehe [Tabelle 2-1](#).

Tabelle 2-1. Benutzerberechtigungen

Benutzerberechtigungen	Zugriffstyp	
	Ansicht	Verwaltung
Benutzer	Ja	Nein
Hauptbenutzer	Ja	Ja
Administrator	Ja	Ja
Administrator mit erhöhten Rechten (nur Linux)	Ja	Ja

## Berechtigungsebenen für den Zugriff auf Server Administrator-Dienste

In [Tabelle 2-2](#) wird zusammengefasst, welche Benutzerebenen die Berechtigungen für den Zugriff auf die Server Administrator-Dienste sowie die Verwaltung dieser Dienste besitzen.

Tabelle 2-2. Server Administrator-Benutzerberechtigungen

Service	Erforderliche Benutzerberechtigungsstufe	
	Ansicht	Verwaltung
Instrumentation	B, H, A, EA	H, A, EA

Remotezugriff	B, H, A, EA	A, EA
Storage Management	B, H, A, EA	A, EA

[Tabelle 2-3](#) definiert die Abkürzungen der Benutzerberechtigungs Ebenen, die in [Tabelle 2-2](#) verwendet werden.

**Tabelle 2-3. Legende der Server Administrator-Benutzerberechtigungs Ebenen**

<b>U</b>	Benutzer
<b>P</b>	Hauptbenutzer
<b>A</b>	Administrator
<b>EA</b>	Administrator mit erhöhten Rechten

## Authentifizierung

Das Server Administrator-Authentifizierungsschema stellt sicher, dass die richtigen Zugriffstypen den korrekten Benutzerberechtigungen zugewiesen werden. Darüber hinaus validiert das Server Administrator-Authentifizierungsschema den Kontext, innerhalb dessen das gegenwärtige Verfahren ausgeführt wird, wenn die Befehlszeilenschnittstelle (CLI) aufgerufen 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 Microsoft® Windows®-Betriebssysteme verwendet Server Administrator-Authentifizierung zur Authentifizierung integrierte Windows Authentication (früher NTLM genannt). Dieses Authentifizierungssystem ermöglicht den Einbezug der Server Administrator-Sicherheit in ein Gesamtsicherheitschema für das Netzwerk.

## Red Hat® Enterprise Linux- und SUSE® Linux Enterprise Server-Authentifizierung

Für unterstützte Red Hat® Enterprise Linux®- und SUSE® LINUX Enterprise Server-Betriebssysteme basiert die Server Administrator-Authentifizierung auf der Pluggable Authentication Modules-Bibliothek (PAM). Benutzer können sich entweder lokal oder im Remote-Zugriff bei Server Administrator anmelden, indem verschieden Verwaltungsprotokolle, wie z. B. LDAP, NIS, Kerberos und Winbind verwendet werden.

## VMware ESX Server 3 und 4

ESX Server verwendet die PAM-Struktur (Pluggable Authentication Modules) für die Authentifizierung, wenn Benutzer auf den ESX Server-Host zugreifen. Die PAM-Konfiguration für VMware-Dienste befindet sich unter `/etc/pam.d/vmware-authd`, wo Pfade zu Authentifizierungsmodulen gespeichert sind.

Die Standardinstallation des ESX Server verwendet wie Linux die `/etc/passwd`-Authentifizierung, doch können Sie ESX Server so konfigurieren, dass ein anderer verteilter Authentifizierungsmechanismus verwendet wird.

## VMware ESX Server 3i und 4i

ESXi authentifiziert Benutzer, die unter Verwendung von vSphere/VI Client oder SDK auf ESXi-Hosts zugreifen. Für die Standardinstallation von ESXi wird eine lokale Kennwortdatenbank für die Authentifizierung verwendet. ESXi-Authentifizierungstransaktionen mit Server Administrator sind auch direkte Interaktionen mit dem `vmware-hostd`-Ablauf. Um sicherzustellen, dass die Authentifizierung für Ihre Site wirksam funktioniert, führen Sie grundlegende Tasks wie die folgenden aus: Einrichten von Benutzern, Gruppen, Berechtigungen und Rollen, Konfigurieren von Benutzerattributen, Hinzufügen Ihrer eigenen Zertifikate und Bestimmen, ob SSL verwendet werden soll.

## Verschlüsselung

Zugriff auf den 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 Microsoft Windows-, Red Hat Enterprise Linux- und SUSE® LINUX Enterprise-Betriebssystemen zum Schutz der Benutzeranmeldeinformationen und anderer Daten verwendet, die über die Socket-Verbindung übertragen werden, wenn ein Benutzer auf die Startseite von Server Administrator zugreift.

## Benutzerberechtigungen zuweisen

Allen Benutzern der Dell OpenManage-Software müssen Benutzerberechtigungen zugewiesen werden, bevor die Dell™ OpenManage™-Software installiert wird, um die Sicherheit kritischer Systemkomponenten zu gewährleisten. Neue Benutzer können sich bei der Dell OpenManage-Software mit ihren Benutzerberechtigungen anmelden.

**⚠ VORSICHTSHINWEIS:** Weisen Sie jedem Benutzerkonto, das auf Dell OpenManage Software zugreifen kann, ein Kennwort zu, um Ihre kritischen Systemkomponenten vor Zugriff zu schützen. Benutzer ohne zugewiesenes Kennwort können sich nicht bei der Dell OpenManage-Software anmelden, wenn diese aufgrund des Betriebssystemaufbaus auf einem System mit Windows Server 2003 ausgeführt wird.

 **VORSICHTSHINWEIS:** Gastkonten sollten für unterstützte Windows-Betriebssysteme deaktiviert sein, um Ihre kritischen Systemkomponenten vor Zugriff zu schützen. Erwägen Sie eine Umbenennung der Kontos, damit diese nicht von Remote-Skripts unter Verwendung des Namens aktiviert werden können.

 **ANMERKUNG:** Bei Fragen zur Zuweisung von Benutzergruppenberechtigungen für jedes unterstützte Betriebssystem lesen Sie die Dokumentation zum Betriebssystem.

 **ANMERKUNG:** Fügen Sie dem Betriebssystem neue Benutzer hinzu, wenn Sie der OpenManage-Software Benutzer hinzufügen wollen. Sie müssen keine neuen Benutzer aus der OpenManage-Software erstellen.

## Benutzer einer Domäne auf Windows-Betriebssystemen hinzufügen

 **ANMERKUNG:** Für die Durchführung der folgenden Verfahren muss Microsoft Active Directory® auf dem System installiert sein. Weitere Informationen zur Verwendung des Active Directory finden Sie unter "Microsoft Active Directory".

1. Wechseln Sie zu **Systemsteuerung** → **Verwaltung** → **Active Directory- Benutzer und Computer**.
2. In der Konsolenstruktur klicken Sie mit der rechten Maustaste auf **Benutzer** oder klicken Sie mit der rechten Maustaste auf den Container, dem Sie den neuen Benutzer hinzufügen möchten. Zeigen Sie dann auf **Neu** → **Benutzer**.
3. Geben Sie die entsprechenden Benutzernameninformationen in das Dialogfeld ein und klicken Sie auf **Weiter**.
4. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.
5. Doppelklicken Sie auf das Symbol für den eben erstellten Benutzer.
6. Klicken Sie auf das Register **Mitglied von**.
7. Klicken Sie auf **Hinzufügen**.
8. Wählen Sie die entsprechende Gruppe und klicken Sie auf **Hinzufügen**.
9. Klicken Sie zweimal hintereinander auf **OK**.

Neue Benutzer können sich bei der Dell OpenManage-Software mit den Benutzerberechtigungen der ihnen zugewiesenen Gruppe oder Domäne anmelden.

## Server Administrator-Benutzer für unterstützte Red Hat Enterprise Linux und SUSE LINUX Enterprise Server-Betriebssysteme erstellen

Administratorberechtigungen werden dem als `root` angemeldeten Benutzer zugewiesen. Führen Sie zum Erstellen von Benutzern mit Benutzer- und Hauptbenutzerberechtigungen folgende Schritte durch.

 **ANMERKUNG:** Sie müssen als `root` oder gleichwertiger Benutzer angemeldet sein, um diese Verfahren auszuführen.

 **ANMERKUNG:** Für die Durchführung dieser Verfahren muss das Dienstprogramm `useradd` auf dem System installiert sein.

### Benutzer erstellen

 **ANMERKUNG:** Um Informationen über das Erstellen von Benutzern und Benutzergruppen zu erhalten, lesen Sie die Dokumentation für das jeweilige Betriebssystem.

### Benutzer mit Benutzerberechtigungen erstellen

1. Führen Sie den folgenden Befehl von der Befehlszeile aus durch:

```
useradd -d <Verzeichnis Startseite> -g <Gruppe> <Benutzername>
```

wobei <Gruppe> nicht `root` ist.

 **ANMERKUNG:** Wenn die <Gruppe> nicht existiert, muss sie mit dem Befehl `groupadd` erstellt werden.

2. Geben Sie `passwd <Benutzername>` ein und drücken Sie <Eingabe>.
3. Wenn Sie dazu aufgefordert werden, geben Sie ein Kennwort für den neuen Benutzer ein.

 **ANMERKUNG:** Jedem Benutzerkonto mit Zugriff auf den Server Administrator muss ein Kennwort zugeteilt werden, um den Zugriff auf die kritischen Systemkomponenten zu sichern.

Der neue Benutzer kann sich jetzt mit Benutzergruppen-Zugriffsrechten bei Server Administrator anmelden.

### Benutzer mit Hauptbenutzerberechtigungen erstellen

1. Führen Sie den folgenden Befehl von der Befehlszeile aus durch:

```
useradd -d <Verzeichnis Startseite> -g root <Benutzername>
```

 **ANMERKUNG:** Sie müssen `root` als die primäre Gruppe setzen.

2. Geben Sie `passwd <Benutzername>` ein und drücken Sie `<Eingabe>`.
3. Wenn Sie dazu aufgefordert werden, geben Sie ein Kennwort für den neuen Benutzer ein.

 **ANMERKUNG:** Jedem Benutzerkonto mit Zugriff auf den Server Administrator muss ein Kennwort zugeteilt werden, um den Zugriff auf die kritischen Systemkomponenten zu sichern.

Der neue Benutzer kann sich jetzt mit Hauptbenutzergruppen-Zugriffsrechten bei Server Administrator anmelden.

### Server Administrator-Benutzerberechtigungen bei Linux-Betriebssystemen bearbeiten

 **ANMERKUNG:** Sie müssen als `root` oder als gleichwertiger Benutzer angemeldet sein, um diese Verfahren ausführen zu können.

1. Öffnen Sie die Datei `omarolemap`, die sich unter `/opt/dell/srvadmin/etc/omarolemap` befindet.
2. Fügen Sie in der Datei Folgendes hinzu:

```
<Benutzername>[Tab]<Hostname>[Tab]<Rechte>
```

[Tabelle 2-4](#) listet die Legenden für das Hinzufügen der Rollendefinition zur Datei `omarolemap` auf

**Tabelle 2-4. Legenden für das Hinzufügen der Rollendefinition in OpenManage Server Administrator**

<Benutzername>	<Hostname>	<Rechte>
Benutzername	Host-Name	Administrator
(+)Gruppenname	Domäne	Benutzer
Platzhalter (*)	Platzhalter (*)	Benutzer
[Tab] = \t (Tab-Zeichen)		

[Tabelle 2-5](#) listet die Beispiele für das Hinzufügen der Rollendefinition zur Datei `omarolemap` auf

**Tabelle 2-5. Beispiele für das Hinzufügen der Rollendefinition in OpenManage Server Administrator**

<Benutzername>	<Hostname>	<Rechte>
Bob	Ahost	Hauptbenutzer
+root	Bhost	Administrator
+root	Chost	Administrator
Bob	*.aus.amer.com	Hauptbenutzer
Mike	192.168.2.3	Hauptbenutzer

3. Speichern und schließen Sie die Datei.
4. Führen Sie von der Befehlszeile den folgenden Befehl aus, um den Verbindungsdienst neu zu starten:

```
service dsm_om_connsvc restart
```

 **ANMERKUNG:** Stellen Sie sicher, dass Sie den Verbindungsdienst neu starten, damit die Änderungen wirksam werden.

### Optimale Verfahrensweisen bei der Verwendung der omarolemap-Datei

Nachfolgend werden die besten Verfahrensweisen für die Arbeit mit der `omarolemap`-Datei aufgeführt:

- Löschen Sie nicht die folgenden Standardeinträge in der **omarolemap**-Datei.

1	root	*	Administrator
1	+root	*	Hauptbenutzer
1	*	*	Benutzer

- Ändern Sie nicht die **omarolemap**-Dateiberechtigungen oder das Dateiformat.
- Server Administrator verwendet die Standardbenutzerberechtigungen des Betriebssystems, wenn ein Benutzer in der **omarolemap**-Datei herabgesetzt ist.
- Verwenden Sie nicht die Loop Back-Adresse für *<Hostname>*, z. B.: localhost oder 127.0.0.1.
- Nachdem die Verbindungsdienste neu gestartet wurden und die Änderungen für die Datei **omarolemap** nicht wirksam werden, konsultieren Sie das Befehlsprotokoll zu den Fehlern.
- Wenn die **omarolemap**-Datei von einem System zu einem anderen kopiert wird, müssen die Dateiberechtigungen und Einträge der Datei erneut überprüft werden.
- Dem *Gruppennamen* muss ein + als Präfix vorangehen
- Server Administrator verwendet die Standard-Benutzerberechtigungen des Betriebssystems, wenn doppelte Einträge von Benutzernamen oder Benutzergruppen mit dem gleichen *<Hostname>* vorliegen.
- Leerzeichen* können anstelle von [Tab] als Begrenzungszeichen für Spalten verwendet werden.

## Server Administrator-Benutzer für VMware ESX Server 3 und 3i erstellen

So fügen Sie der Tabelle Users (Benutzer) einen Benutzer hinzu:

- Melden Sie sich über den ESX Server 3 oder 3i-Host am VI Client an.
- Wählen Sie den Server aus dem Bestandsaufnahme Fenster aus.
- Klicken Sie auf das Register **Users & Groups (Benutzer und Gruppen)** und klicken Sie auf **Users (Benutzer)**.
- Klicken Sie mit der rechten Maustaste an eine beliebige Stelle in der Tabelle **Users (Benutzer)** und klicken Sie auf **Add (Hinzufügen)**, um das Dialogfeld **Add New User (Neuen Benutzer hinzufügen)** zu öffnen.
- Geben Sie einen Anmeldenamen, einen Benutzernamen, eine numerische Benutzer-ID (UID) sowie ein Kennwort ein; das Festlegen des Benutzernamens und der UID ist optional. Wenn Sie die UID nicht festlegen, weist der VI Client die nächste verfügbare UID zu. Wenn der Benutzer in der Lage sein soll, über eine Befehls-Shell auf den ESX Server 3-Host zuzugreifen, wählen Sie **Grant shell access to this user (Diesem Benutzer Shell-Zugriff gewähren)** aus.
- Geben Sie für jede vorhandene Gruppe, der der Benutzer zugehören soll, den Gruppennamen ein und klicken Sie auf **Add (Hinzufügen)**. Wenn Sie einen nicht existierenden Gruppennamen eingeben, warnt Sie der VI Client und fügt die Gruppe nicht der Liste der **Group membership (Gruppenmitgliedschaft)** hinzu.
- Klicken Sie auf **OK**.

Der von Ihnen eingegebene Anmelde Name und der Benutzername werden jetzt in der Tabelle **Users (Benutzer)** angezeigt.

## Server Administrator-Benutzer für VMware ESX Server 4 und 4i erstellen

So fügen Sie der Tabelle Users (Benutzer) einen Benutzer hinzu:

- Melden Sie sich unter Verwendung des vSphere Client am Host an.
- Klicken Sie auf das Register **Users & Groups (Benutzer und Gruppen)** und klicken Sie auf **Users (Benutzer)**.
- Klicken Sie an einer beliebigen Stelle in der Tabelle Users (Benutzer) und klicken Sie auf **Add (Hinzufügen)**, um das Dialogfeld Add New User (Neuen Benutzer hinzufügen) zu öffnen.
- Geben Sie einen Anmeldenamen, einen Benutzernamen, eine numerische Benutzer-ID (UID) sowie ein Kennwort ein; das Festlegen des Benutzernamens und die UID ist optional. Wenn Sie die UID nicht festlegen, weist der vSphere Client die nächste verfügbare UID zu.
- Um einem Benutzer zu erlauben, über eine Befehls-Shell auf den ESX- Host zuzugreifen, wählen Sie **Grant shell access to this user (Diesem Benutzer Shell-Zugriff gewähren)** aus. Benutzer, die ausschließlich über den vSphere Client auf den Host zugreifen, benötigen keinen Shell- Zugriff.
- Sie können den Benutzer einer Gruppe hinzufügen, indem Sie den Gruppennamen aus dem Drop-down-Menü **Group (Gruppe)** auswählen und auf **Add (Hinzufügen)** klicken.

7. Klicken Sie auf **OK**.

---

## Gastkonten und anonyme Konten in unterstützten Windows-Betriebssystemen deaktivieren

 **ANMERKUNG:** Sie müssen mit Administratorberechtigungen angemeldet sein, um dieses Verfahren durchzuführen.

1. Öffnen Sie das Fenster **Computerverwaltung**.
2. Erweitern Sie in der Konsolenstruktur das Fenster **Lokale Benutzer und Gruppen** und klicken Sie auf **Benutzer**.
3. Doppelklicken Sie das Benutzerkonto **Gast** oder **IUSR\_Systemname**, um die Eigenschaften für diese Benutzer anzuzeigen, oder klicken Sie mit der rechten Maustaste auf das Benutzerkonto **Gast** oder **IUSR\_Systemname** und wählen Sie **Eigenschaften** aus.
4. Wählen Sie **Konto ist deaktiviert** und klicken Sie auf **OK**.

Ein roter Kreis mit einem X wird über dem Benutzernamen eingeblendet. Das Konto ist deaktiviert.

---

## SNMP-Agenten konfigurieren

Der Server Administrator unterstützt die Systemverwaltungsnorm einfaches Netzwerkverwaltungsprotokoll (SNMP) auf allen unterstützten Betriebssystemen. Die SNMP-Unterstützung ist entweder installiert oder nicht installiert. Dies hängt vom Betriebssystem ab und davon, wie das Betriebssystem installiert wurde. In den meisten Fällen wird SNMP als Teil der Betriebssysteminstallation installiert. Ein installierter unterstützter Systemverwaltungsprotokoll-Standard, z. B. SNMP, ist vor der Installation von Server Administrator erforderlich.

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 z. B. dem Dell OpenManage™ 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**. Aus Sicherheitsgründen sollten Sie die SNMP Community-Namen von ihren Standardwerten ändern. Informationen zur Änderung von SNMP-Community-Namen erhalten Sie im entsprechenden untenstehenden Abschnitt.

 **ANMERKUNG:** SNMP-Satzvorgänge sind in Server Administrator Version 5.2 oder später standardmäßig deaktiviert. Server Administrator bietet Support, um SNMP-Satz-Vorgänge in Server Administrator zu aktivieren oder zu deaktivieren. Sie können die **Server Administrator-Seite SNMP-Konfiguration** unter **Einstellungen** oder die Server Administrator-Befehlszeilenoberfläche (CLI) verwenden, um die SNMP-Satz-Vorgänge in Server Administrator zu aktivieren oder zu deaktivieren. Weitere Informationen zur Server Administrator-CLI erhalten Sie hier: *Dell OpenManage Server Administrator-Befehlszeilenoberfläche: Benutzerhandbuch*.

 **ANMERKUNG:** Damit IT Assistant Verwaltungsinformationen von einem System abrufen kann, auf dem Server Administrator ausgeführt wird, muss der durch IT Assistant verwendete Community-Name mit einem Community-Namen auf dem System übereinstimmen, auf dem Server Administrator ausgeführt wird. Damit IT Assistant Informationen oder durchgeführte Maßnahmen auf einem System ändern kann, auf dem Server Administrator ausgeführt wird, muss der durch IT Assistant verwendete Community-Name mit einem zum Einstellen von Vorgängen berechtigenden Community-Namen auf dem System übereinstimmen, auf dem Server Administrator ausgeführt wird. Damit IT Assistant Traps (asynchrone Ereignisbenachrichtigungen) von einem System empfangen kann, auf dem Server Administrator ausgeführt wird, muss das Server Administrator ausführende System so konfiguriert sein, dass es Traps an das System sendet, auf dem IT Assistant ausgeführt wird.

Die folgenden Verfahren enthalten schrittweise Anleitungen für die Konfiguration des SNMP-Agenten für jedes unterstützte Betriebssystem.

1. "["SNMP-Agenten für Systeme konfigurieren, auf denen unterstützte Windows-Betriebssysteme ausgeführt werden"](#)
1. "["Konfiguration des SNMP-Agenten auf Systemen, die unterstützte Red Hat Enterprise Linux- und VMware ESX 4.0-Betriebssysteme ausführen"](#)
1. "["Konfiguration des SNMP-Agenten auf Systemen, die unterstützte SUSE Linux Enterprise Server- und VMware ESX 3.5-Betriebssysteme ausführen"](#)

## SNMP-Agenten für Systeme konfigurieren, auf denen unterstützte Windows-Betriebssysteme ausgeführt werden

Der Server Administrator verwendet die SNMP-Dienste, die vom Windows 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. Führen Sie zur Konfiguration des SNMP-Agenten für korrekte Interaktion mit Verwaltungsanwendungen, wie z. B. IT Assistant, die im Folgenden beschriebenen Verfahren durch.

 **ANMERKUNG:** Weitere Einzelheiten zur SNMP-Konfiguration finden Sie in der Dokumentation des Betriebssystems.

## SNMP-Zugriff durch Remote Hosts aktivieren

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.

Damit ein System mit einem Windows Server 2003-Betriebssystem 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 Remote-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 Verwaltungsanwendungen verwendete SNMP-Community-Name muss mit einem SNMP-Community-Namen übereinstimmen, der auf dem Server Administrator-System konfiguriert wurde, sodass die Verwaltungsanwendungen Verwaltungsinformationen vom Server Administrator 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 in das Textfeld **Community-Name** den Community- Namen eines Systems ein, das das System verwalten kann (die **Standardeinstellung** ist public [öffentlich]) 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. Nehmen Sie alle erforderlichen Änderungen am Community-Namen des Systems, das das System verwalten kann, im Textfeld **Community-Name** vor und klicken Sie auf **OK**.

Das Fenster **Eigenschaften von SNMP-Dienst** wird angezeigt.
6. Klicken Sie auf **OK** zum Speichern der Änderungen.

## Aktivieren von SNMP-Set-Vorgängen

SNMP-Set-Vorgänge müssen auf dem Server Administrator-System aktiviert sein, damit Server Administrator-Attribute mittels IT Assistant geändert 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 dann auf **Dienste**.
4. Rollen 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** aus 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 zum Speichern der Änderungen auf **OK**.

## Konfigurieren des Systems zum Senden von SNMP-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 Server Administrator-System konfigurieren, damit SNMP-Traps an eine Verwaltungsstation 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 Drop-down-Feld **Community-Name** und klicken Sie auf **Hinzufügen** unter dem Feld **Trap-Ziele**.
  - c. Das Fenster **Konfiguration von SNMP-Dienst** wird angezeigt.

Geben Sie das Trap-Ziel ein und klicken Sie auf **Hinzufügen**.

Das Fenster **Eigenschaften von SNMP-Dienst** wird angezeigt.
6. Klicken Sie zum Speichern der Änderungen auf **OK**.

## Konfiguration des SNMP-Agenten auf Systemen, die unterstützte Red Hat Enterprise Linux- und VMware ESX 4.0-Betriebssysteme ausführen

Server Administrator verwendet die SNMP-Dienste, die vom net-snmp-SNMP-Agenten bereitgestellt werden. 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 dem IT Assistant führen Sie die im Folgenden beschriebenen Verfahren aus.

 **ANMERKUNG:** Weitere Einzelheiten zur SNMP-Konfiguration finden Sie in der Dokumentation des Betriebssystems.

### Konfiguration von SNMP-Agent Access Control

Der Zweig der Verwaltungsinformationsbasis (MIB), der vom Server Administrator implementiert wird, wird mit dem OID 1.3.6.1.4.1.674 gekennzeichnet. Verwaltungsanwendungen müssen Zugriff auf diesen Zweig der MIB-Struktur besitzen, um Systeme verwalten zu können, die Server Administrator ausführen.

Bei Red Hat Enterprise Linux- und VMware ESX 4.0-Betriebssystemen gibt die standardmäßige SNMP-Agent-Konfiguration den Nur-Lesen-Zugriff für die "öffentliche" Community nur an die "System"-Teilstruktur MIB-II (gekennzeichnet mit der OID 1.3.6.1.2.1.1) der MIB-Struktur. Diese Konfiguration erlaubt es nicht, dass Verwaltungsanwendungen Informationen vom Server Administrator oder andere Systems Management-Informationen außerhalb des "System"-Zweigs MIB-II abrufen oder ändern.

### Server Administrator SNMP Agent - Installationsmaßnahmen

Wenn der Server Administrator diese Konfiguration während der Installation entdeckt, versucht er die SNMP-Agent-Konfiguration so zu ändern, dass die öffentliche Community einen Lesezugriff für die gesamte MIB-Struktur bekommt. 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 Standard-"Zugriff" abgeändert, sodass 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 der Server Administrator die obenstehende Zeile findet, dann ändert er sie folgendermaßen ab:

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

Diese Änderungen an 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 Verwaltungsanwendungen verwendete SNMP-Community-Name muss mit einem SNMP-Community-Namen übereinstimmen, der auf dem Server Administrator-System konfiguriert wurde, sodass die Verwaltungsanwendungen Verwaltungsinformationen vom 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
```

## Aktivieren von SNMP-Set-Vorgängen

SNMP Set-Vorgänge müssen auf dem System aktiviert werden, auf dem Server Administrator ausgeführt wird, um Server Administrator-Attribute mithilfe des IT Assistant zu ändern.

Zur Aktivierung von SNMP-Set-Vorgängen auf dem System, auf dem Server Administrator ausgeführt wird, bearbeiten Sie die SNMP-Agentenkonfigurationsdatei `/etc/snmp/snmpd.conf` und führen Sie folgende Schritte durch:

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.

Zur Konfiguration des Systems, das Server Administrator ausführt, um Traps an eine Verwaltungsstation zu senden, bearbeiten Sie die SNMP-Agentenkonfigurationsdatei `/etc/snmp/snmpd.conf` und führen Sie 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:

```
service snmpd restart
```

## Konfiguration des SNMP-Agenten auf Systemen, die unterstützte SUSE Linux Enterprise Server- und VMware ESX 3.5-Betriebssysteme ausführen

Server Administrator verwendet die SNMP-Dienste, die vom net-snmp-Agenten bereitgestellt werden. Sie können den SNMP-Agenten so konfigurieren, dass der SNMP-Zugriff von Remote-Hosts aktiviert ist, der Community-Name geändert werden kann, Set-Vorgänge aktiviert sind und Traps an eine Management Station gesendet werden. Führen Sie zur Konfiguration des SNMP-Agenten für korrekte Interaktion mit Verwaltungsanwendungen wie z. B. IT Assistant die im Folgenden beschriebenen Verfahren durch.

 **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 das Server Administrator-SNMP mit dem SNMP-Agenten eine Verbindung herstellt, sendet es 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 SNMP-Agent-Konfigurationsdatei `/etc/snmp/snmpd.conf` während der Installation die folgende Zeile hinzu, falls 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 gibt nur schreibgeschützten Zugriff auf die komplette MIB-Struktur an die "public" Community vom lokalen Host. Mit dieser Konfiguration können SNMP Verwaltungsanwendungen wie IT Assistant, die auf anderen Hosts ausgeführt werden, Server Administrator-Systeme nicht richtig ermitteln und verwalten. 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-Zugriff von einem bestimmten Remote-Host zu einem System zu aktivieren, das Server Administrator ausführt, bearbeiten Sie die SNMP-Agent-Konfigurationsdatei `/etc/snmp/snmpd.conf` und führen Sie folgende Schritte aus:

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-Zugriff von allen Remote-Hosts auf ein System zu aktivieren, das Server Administrator ausführt, bearbeiten Sie die SNMP-Agenten-Konfigurationsdatei `/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 127.0.0.1 löschen. 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 Management Stations 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, sodass die Verwaltungsanwendungen Verwaltungsinformationen vom Server Administrator abrufen können.

Zum Ändern des standardmäßigen SNMP-Community-Namens, der zum Abrufen von Verwaltungsinformationen von einem System verwendet wird, das Server Administrator ausführt, bearbeiten Sie die SNMP-Agent-Konfigurationsdatei `/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 werden, auf dem Server Administrator ausgeführt wird, um Server Administrator-Attribute mithilfe des IT Assistent zu ändern. Um Remote-Herunterfahren eines Systems von IT Assistent zu aktivieren, müssen SNMP Set-Vorgänge aktiviert sein.

 **ANMERKUNG:** Für den Neustart des Systems sind für die Änderungsverwaltungsfunktionalität keine SNMP-Satz-Vorgänge erforderlich.

Zum Aktivieren von SNMP-Set-Vorgängen auf einem System, das Server Administrator ausführt, bearbeiten Sie die SNMP-Agent-Konfigurationsdatei `/etc/snmp/snmpd.conf` und führen Sie folgende Schritte durch:

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.

Zur Konfiguration des Systems, das Server Administrator ausführt, um Traps an eine Management Station zu senden, bearbeiten Sie die SNMP-Agent-Konfigurationsdatei `/etc/snmp/snmpd.conf` und führen Sie 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
```

## Konfiguration des SNMP-Agenten auf Systemen, die unterstützte VMware ESX 4.0-Betriebssysteme zu Proxy VMware MIBs ausführen

Der ESX4.0-Server kann durch eine einzelne Standardschnittstelle 161 unter Verwendung des SNMP-Protokolls verwaltet werden. Hierzu wird `snmpd` zur Verwendung der Standardschnittstelle 161 konfiguriert und `vmwarehostd` wird zur Verwendung einer anderen (unbenutzten) Schnittstelle konfiguriert, z. B. Schnittstelle 167. Alle SNMP-Aufforderungen der VMWare-MIB-Teilstruktur werden unter Verwendung der Proxy-Funktion des `snmpd`-Daemon zu `vmware-hostd` umgeleitet.

Die VMWare-SNMP-Konfigurationsdatei kann manuell auf dem ESX-Server modifiziert werden oder durch Ausführen des VMWare RCLI-Befehls `vicfg-snmp` über ein Remote-System (Windows oder Linux). Die RCLI-Hilfsprogramme können von der VMWare-Website ([http://www.vmware.com/download/vi/drivers\\_tools.html](http://www.vmware.com/download/vi/drivers_tools.html)) heruntergeladen werden.

Nachstehend sind die für die Konfiguration erforderlichen Schritte aufgeführt. Es folgt auf diese Schritte ein Python-Skript, das den Konfigurationsablauf automatisiert. Sie können den Inhalt kopieren und in eine Datei einfügen und sie zur Konfiguration auf dem ESX-Server ausführen.

1. Bearbeiten Sie die VMWare-SNMP-Konfigurationsdatei (`/etc/vmware/snmp.xml`) entweder manuell oder führen Sie die folgenden `vicfg-snmp`-Befehle aus, um die SNMP-Konfigurationseinstellungen zu modifizieren. Hierzu zählen die SNMP-Abhörschnittstelle, die Community-Zeichenkette und die IP-Adresse/Schnittstelle des Trap-Ziels sowie der Trap-Community-Name. Aktivieren Sie anschließend den VMWare SNMP-Dienst.

```
a. vicfg-snmp.pl --server <ESX_IP_Adr> --username root --password <Kennwort> -c <Community-Name> -p X -t
   <DMC_IP_Adresse>@162/<Community-Name>
```

Hierbei steht X für einen nicht verwendeten Port. Sie können eine unbenutzte Schnittstelle ausfindig machen, indem Sie die Datei `/etc/services` nach der Schnittstellenzuweisung für definierte Systemdienste durchsehen. Führen Sie außerdem den Befehl `netstat -a` auf dem ESX-Server aus, um sicherzustellen, dass die ausgewählte Schnittstelle nicht gegenwärtig von einer anderen Anwendung/einem anderen Dienst in Anspruch genommen wird.



**ANMERKUNG:** Sie können mehrfache IP-Adressen eingeben, indem Sie eine Liste verwenden, in der die einzelnen Einträge durch Kommas getrennt sind.

- b. Führen Sie zum Aktivieren des VMWare-SNMP-Diensts den folgenden Befehl aus:

```
vicfg-snmp.pl --server <ESX_IP_Adr> --username root --password <Kennwort>
```

```
-E
```

- c. Führen Sie zum Anzeigen der Konfigurationseinstellungen den folgenden Befehl aus:

```
vicfg-snmp.pl --server <ESX_IP_Adr> --username root --password <Kennwort>
```

```
-s
```

Nach der Modifizierung sieht die Konfigurationsdatei folgendermaßen aus:

```
<?xml version="1.0">
<config>
<snmpSettings>
<enable>true</enable>
<communities>public</communities>
<targets>143.166.152.248@162/public</targets>
<port>167</port>
</snmpSettings>
</config>
```

2. Wenn der SNMP-Dienst bereits auf dem System ausgeführt wird, können Sie ihn anhalten, indem Sie den folgenden Befehl eingeben:

```
service snmpd stop
```

3. Fügen Sie dem Ende von `/etc/snmp/snmpd.conf` die folgende Zeile hinzu:

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

wobei X für die oben festgelegte ungenutzte Schnittstelle steht, während SNMP konfiguriert wird.

4. Konfigurieren Sie das Trap-Ziel unter Verwendung des folgenden Befehls: `<Ziel_IP_Adresse> <Community_Name>`

Die trapsink-Angabe ist erforderlich, damit Traps gesendet werden können, die in den proprietären MIBs definiert sind.

5. Starten Sie den mgmt-vmware-Dienst mit dem folgenden Befehl:

```
service mgmt-vmware restart
```

6. Starten Sie den snmpd-Dienst mit dem folgenden Befehl neu:

```
service snmpd start
```

 **ANMERKUNG:** Wenn srvadmin installiert ist und die Dienste bereits begonnen haben, sollten diese neu gestartet werden, da sie vom snmpd-Dienst abhängig sind.

7. Führen Sie den folgenden Befehl aus, damit der snmpd-Daemon bei jedem Neustart startet:

```
chkconfig snmpd on
```

8. Führen Sie den folgenden Befehl aus, um sicherzustellen, dass die SNMP-Schnittstellen offen sind, bevor Traps an die Management Station gesendet werden.

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

## Konfiguration des SNMP-Agenten auf Systemen, die unterstützte VMware ESXi 4.0-Betriebssysteme ausführen

Server Administrator unterstützt SNMP-Traps auf VMware ESXi 4. Server Administrator unterstützt nicht die SNMP-Get- und Set-Abläufe auf VMware ESXi 4, da VMware ESXi 4 nicht die erforderliche SNMP-Unterstützung bietet. The VMware vSphere CLI (Befehlszeilenoberfläche) wird verwendet, um ein System zu konfigurieren, das VMware ESXi 4 ausführt, um SNMP-Traps an eine Management Station zu senden.

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

### 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.

Führen Sie zum Konfigurieren des ESXi-Systems, das Server Administrator zum Senden von Traps an eine Management Station ausführt, die folgenden Schritte aus:

1. Installieren Sie VMware vSphere CLI.
2. Öffnen Sie eine Eingabeaufforderung auf dem System, auf dem die VMware vSphere CLI installiert ist.
3. Wechseln Sie zu dem Verzeichnis, in dem die VMware vSphere CLI installiert ist. Der Standardspeicherort auf Linux befindet sich unter `/usr/bin`. Der Standardspeicherort auf Windows befindet sich unter `C:\Program Files\VMware\VMware vSphere CLI\bin`.
4. Führen Sie den folgenden Befehl aus:

```
vicfg-snmp.pl --server <Server> --username <Benutzername> --password <Kennwort> -c <Community> -t <Hostname>/<Community>
```

wobei `<Server>` der Hostname oder die IP-Adresse des ESXi-Systems ist, `<Benutzername>` der Benutzer auf dem ESXi-System, `<Kennwort>` das Kennwort des ESXi-Benutzers, `<Community>` der SNMP Community-Name und `<Hostname>` der Hostname oder die IP-Adresse der Management Station.

 **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.

---

## Firewall-Konfiguration auf Systemen, die unterstützte Red Hat Enterprise Linux-Betriebssysteme und SUSE Linux Enterprise Server ausführen

Wenn Sie beim Installieren von Red Hat Enterprise Linux/SUSE Linux die Firewall-Sicherheit aktivieren, wird die SNMP-Schnittstelle an allen externen Netzwerkschnittstellen standardmäßig geschlossen. Damit SNMP-Verwaltungsanwendungen wie IT Assistant Informationen von Server Administrator ermitteln

und empfangen können, muss der SNMP-Anschluss auf mindestens einer externen Netzwerkschnittstelle geöffnet sein. Wenn der Server Administrator ermittelt, dass kein SNMP-Anschluss der Firewall aller externen Netzwerkschnittstellen geöffnet ist, zeigt der Server Administrator eine Warnmeldung an und trägt eine Meldung im System-Protokoll 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 die SNMP-Schnittstelle auf RHEL mittels einer der zuvor beschriebenen Methoden zu öffnen, führen Sie die folgenden Schritte aus:

1. Geben Sie bei der Befehlsaufforderung von Red Hat Enterprise Linux den Befehl `setup` ein und drücken Sie die **Eingabetaste**, 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 Configuration (Firewall-Konfiguration)** mit dem Nach-unten-Pfeil aus und drücken Sie die **Eingabetaste**.

Der Bildschirm **Firewall-Konfiguration** wird geöffnet.

3. Drücken Sie die **Tabulatortaste**, um **Security Level (Sicherheitsstufe)** auszuwählen, und drücken Sie die Leertaste, um die Sicherheitsstufe auszuwählen, die Sie einstellen möchten. 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 grafische Benutzeroberfläche von X Window System verwenden, dann kann es sein, dass bei neueren Versionen von Red Hat Enterprise Linux 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. Zum Öffnen einer ganzen Netzwerkschnittstelle oder der SNMP- Schnittstelle wählen Sie **Hoch, Mittel** oder **Aktiviert** und fahren Sie mit [Schritt 4](#) fort.

- d. Drücken Sie die **Tabulatortaste**, um zu **Customize (Anpassen)** zu wechseln, und drücken Sie die **Eingabetaste**.

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 gesamte Netzwerkschnittstelle zu öffnen, wechseln Sie mit der **Tabulatortaste** zu einer 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 eine SNMP-Schnittstelle auf allen Netzwerkschnittstellen zu öffnen, wechseln Sie mit der **Tabulatortaste** zu **Other ports (Weitere Schnittstellen)** und geben Sie `snmp:udp` ein.

6. Drücken Sie die **Tabulatortaste**, um **OK** auszuwählen, und drücken Sie die **Eingabetaste**.

Der Bildschirm **Firewall-Konfiguration** wird geöffnet.

7. Drücken Sie die **Tabulatortaste**, um **OK** auszuwählen, und drücken Sie die **Eingabetaste**.

Das Menü **Hilfsprogramm auswählen** wird eingeblendet.

8. Drücken Sie die **Tabulatortaste**, um **Quit (Beenden)** auszuwählen, und drücken Sie die **Eingabetaste**.

Um die SNMP-Schnittstelle auf SUSE Linux Enterprise Server zu öffnen, führen Sie die folgenden Schritte aus:

1. Konfigurieren Sie SuSEfirewall2, indem Sie Folgendes auf einer Konsole ausführen: `a.# yast2 firewall`
2. Verwenden Sie die Pfeiltasten, um zu **Zulässige Dienste** zu wechseln.
3. Geben Sie ``Alt+d'` ein, um das Dialogfeld **Additional Allowed Ports (Zusätzliche zulässige Schnittstellen)** zu öffnen.
4. Geben Sie ``Alt+T'` ein, um den Cursor zum Textfeld **TCP Ports (TCP- Schnittstellen)** zu bewegen.
5. Geben Sie in das Textfeld ``snmp'` ein.
6. Geben Sie ``Alt-O'` und ``Alt-N'` ein, um zum nächsten Bildschirm zu wechseln.
7. Geben Sie ``Alt-A'` ein, um den Änderungen zuzustimmen und sie zu übernehmen.



[Zurück zum Inhaltsverzeichnis](#)

## Server Administrator verwenden

Dell™ OpenManage™ Server Administrator Version 6.2 Benutzerhandbuch

- [Server Administrator-Sitzung starten](#)
- [An- und Abmelden](#)
- [Server Administrator-Homepage](#)
- [Online-Hilfe verwenden](#)
- [Voreinstellungen-Homepage verwenden](#)
- [Server Administrator Web Server-Maßnahmeregister](#)
- [Server Administrator steuern](#)
- [Server Administrator-Befehlszeilenschnittstelle verwenden](#)

### Server Administrator-Sitzung starten

Klicken Sie zum Starten einer Server Administrator-Sitzung auf das Symbol **Dell™ OpenManage™ Server Administrator** auf dem Desktop.

Der Bildschirm **Server Administrator-Anmeldung** wird angezeigt. Der Standardanschluss für Dell™ OpenManage™ Server Administrator ist 1311. Falls erforderlich, können Sie den Anschluss ändern. Anleitungen zum Setup Ihrer Systemeinstellungen erhalten Sie unter "[Dell Systems Management Server Administration-Verbindungsdiens und Sicherheits-Setup](#)".

### An- und Abmelden

Sie können sich auf drei verschiedene Weisen am OpenManage Server Administrator anmelden. Dies sind:

- 1 Server Administrator, Lokales-System-Anmeldung
- 1 Server Administrator, Managed-System-Anmeldung
- 1 Anmeldung am zentralen Web Server

### Server Administrator, Lokales-System-Anmeldung

Diese Art der Anmeldung ist nur verfügbar, wenn Sie die Server Instrumentation- und Server Administrator Web Server-Komponenten auf dem lokalen System installieren.

Mit diesem Anmeldefenster melden Sie sich bei Server Administrator auf einem lokalen System an:

1. Geben Sie Ihren zugewiesenen **Benutzernamen** und Ihr **Kennwort** in die entsprechenden Felder des Systems Management-**Anmeldefensters** ein.  
Wenn Sie von einer definierten Domäne auf den Server Administrator zugreifen, müssen Sie ebenfalls den korrekten **Domänennamen** angeben.
2. Wenn Ihr System ein Microsoft Windows-Betriebssystem ausführt und der Windows Domain angehört, wählen Sie eine Domäne aus der Domänenliste aus.
3. Wählen Sie das Kontrollkästchen für Active Directory-Anmeldung, um sich mit Microsoft® Active Directory® anzumelden. Siehe '[Die Active Directory-Anmeldung verwenden](#)'.
4. Klicken Sie auf **OK**.

Um die Server Administrator-Sitzung zu beenden, klicken Sie auf die Schaltfläche **Abmelden** oben rechts auf der Startseite von Server Administrator.

 **ANMERKUNG:** Im OpenManage Installation and Security-Benutzerhandbuch finden Sie Informationen zur Konfiguration von Active Directory auf Systemen ohne CLI.

### Server Administrator Managed System-Anmeldung

Diese Art der Anmeldung ist nur verfügbar, wenn Sie die Server Administrator Web Server-Komponente installieren. So melden Sie sich bei Server Administrator an, um ein Remote-System zu verwalten:

#### Verfahren 1

1. Klicken Sie auf das Symbol **Dell™ OpenManage™ Server Administrator** auf Ihrem Desktop.
2. Geben Sie Ihren zugewiesenen **Hostnamen/die IP-Adresse, den Benutzernamen** und das **Kennwort** des verwalteten Systems in die entsprechenden Felder des **Anmeldefensters** der Remote-Verwaltung ein. Wenn erforderlich, können Sie auch den Computernamen oder den FQDN (Fully Qualified Domain Name) in das Feld **Hostname/IP-Adresse** eingeben.
3. Wählen Sie das Kontrollkästchen **Zertifikatswarnungen ignorieren** aus, wenn Sie eine Intranet-Verbindung verwenden.

4. Wählen Sie das Kontrollkästchen **Active Directory-Anmeldung** aus. Markieren Sie diese Option, um sich mit der Microsoft Active Directory®-Authentifizierung anzumelden. **Markieren Sie dieses Kontrollkästchen nicht, wenn Sie keine Active Directory-Software benutzen, um den Zugriff auf Ihr Netzwerk zu steuern.** Siehe ['Die Active Directory-Anmeldung verwenden'](#).
5. Klicken Sie auf **OK**.

## Verfahren 2

Öffnen Sie Ihren Internet-Browser, geben Sie einen der folgenden Einträge in das Adressfeld ein und drücken Sie <Eingabe>:

`https://Host-Name:1311`

wobei `Host-Name` der zugewiesene Name des verwalteten Knotensystems ist und 1311 die Standardschnittstellenummer

oder

`https://IP-Adresse:1311`

wobei `IP-Adresse` die IP-Adresse für das verwaltete System ist und 1311 die standardmäßige Schnittstellenummer. Geben Sie `https://` (nicht `http://`) in das Adressfeld ein, um eine gültige Antwort im Browser zu erhalten.

 **ANMERKUNG:** Sie müssen bereits zugewiesene Benutzer-Zugriffsrechte haben, um sich beim Server Administrator anmelden zu können. Anleitungen zur Einrichtung von neuen Benutzern finden Sie unter **Setup und Administration**.

## Anmeldung am zentralen Web Server

Diese Art der Anmeldung ist nur verfügbar, wenn Sie die **Server Administrator Web Server**-Komponente installieren. Verwenden Sie diese Anmeldung, um den zentralen OpenManage Server Administrator Web Server zu verwalten:

1. Klicken Sie auf das Symbol **Dell OpenManage Server Administrator** auf dem Desktop. Die Seite Remote-Anmeldung wird angezeigt.
2. Klicken Sie auf den Link **Web Server verwalten** oben rechts auf dem Bildschirm.
3. Geben Sie den **User Name (Benutzernamen)**, das **Password (Kennwort)** und den **Domain Name (Domännennamen)** ein (wenn Sie über eine definierte Domäne auf Server Administrator zugreifen) und klicken Sie auf **OK**.
4. Wählen Sie das **Kontrollkästchen für Active Directory-Anmeldung** aus, um sich mit Microsoft® Active Directory® anzumelden. Siehe ['Die Active Directory-Anmeldung verwenden'](#).
5. Klicken Sie auf **OK**.

Zum Beenden der Server Administrator-Sitzung klicken Sie auf der ["Allgemeine Navigationsleiste"](#) auf **Abmelden**. Die Schaltfläche **Abmelden** befindet sich in der rechten oberen Ecke der Homepage des Server Administrators.

 **ANMERKUNG:** Wenn Sie Server Administrator mit Internet Explorer® Version 7.0 starten, wird eventuell eine Zwischenwarnungsseite eingeblendet, die das Problem mit dem Sicherheitszertifikat anzeigt. Zur Gewährleistung der Systemsicherheit wird empfohlen, entweder ein neues X.509-Zertifikat zu erstellen, ein bestehendes wieder zu verwenden oder eine Stammzertifikatskette von einer Zertifizierungsstelle (CA) zu importieren. Um solche Warnungsmeldungen über das Zertifikat zu vermeiden, muss das Zertifikat von einer zuverlässigen Zertifizierungsstelle stammen. Weitere Informationen zur X.509-Zertifikatsverwaltung finden Sie unter ["X.509-Zertifikatsverwaltung"](#).

## Die Option Zertifikat ignorieren verwenden

Auf dem Anmeldebildschirm befindet sich das Kontrollkästchen "Zertifikatswarnungen ignorieren".

 **VORSICHTSHINWEIS:** Sie sollten die Option "Zertifikatswarnungen ignorieren" mit Bedacht verwenden. Es wird dringend empfohlen, diese Option nur in vertrauenswürdigen Intranet-Umgebungen zu verwenden. Um die Systemsicherheit zu gewährleisten, empfiehlt Dell dringend, ein Root-Zertifikat oder eine Zertifikatskette von einer Zertifizierungsstelle (CA) zu importieren. Einzelheiten können Sie der VMware-Dokumentation entnehmen.

 **ANMERKUNG:** Wenn die Zertifizierungsstelle auf dem verwalteten System gültig ist und der Server Administrator Web Server noch immer einen Zertifikatsfehler meldet, können Sie durch die Verwendung von `certutil.exe` die CA des verwalteten Systems als vertrauenswürdig einstufen. In der Dokumentation Ihres Betriebssystems finden Sie Details zum Zugriff auf diese `.exe`-Datei. Auf unterstützten Windows-Betriebssystemen können Sie auch die Option Zertifikat-Snap-In verwenden, um Zertifikate zu importieren.

## Die Active Directory-Anmeldung verwenden

Wählen Sie das Kontrollkästchen "Active Directory-Anmeldung" aus, um sich mit der Dell Extended Schema Solution bei Microsoft® Active Directory anzumelden.

Diese Lösung ermöglicht Ihnen, Zugriff auf Server Administrator zu gewähren. Sie können damit Server Administrator-Benutzer und -Berechtigungen zu bestehenden Benutzern in Ihrer Active Directory-Software hinzufügen bzw. steuern. Weitere Informationen finden Sie unter "Microsoft Active Directory verwenden" im *Dell OpenManage Installation and Security-Benutzerhandbuch*.

## Einfache Anmeldung

Die Option der Einzelanmeldung auf Microsoft Windows®-Systemen ermöglicht allen angemeldeten Benutzern, die Anmeldungsseite zu umgehen und durch Klicken auf das **Dell OpenManage Server Administrator**-Symbol auf dem Desktop auf die Server Administrator-Webanwendung zuzugreifen.

 **ANMERKUNG:** Weitere Informationen zur einfachen Anmeldung finden Sie im Knowledge-Base-Artikel unter <http://support.microsoft.com/default.aspx?scid=kb;en-us;Q258063>.

Für den lokalen Maschinenzugang ist es nicht erforderlich, dass Sie auf der Maschine ein Konto mit korrekten Berechtigungen haben (Benutzer, Hauptbenutzer oder Verwalter). Andere Benutzer werden gegen Microsoft Active Directory authentisiert. Um Server Administrator mithilfe von Einzelanmeldungsauthentisierung gegen Microsoft Active Directory zu starten, müssen die folgenden Parameter ebenso eingereicht werden:

```
authType=ntlm&application={Plugin-Name}
```

Wobei *Plugin-Name* = *omsa*, *ita* etc.

Beispiel:

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

Um Server Administrator mithilfe der einfachen Anmeldungs-Authentifizierung gegen die Benutzerkonten der lokalen Maschine zu starten, müssen die folgenden Parameter ebenso eingereicht werden:

```
authType=ntlm&application={Plugin-Name}&locallogin=true
```

Wobei *Plugin-Name* = *omsa*, *ita* etc.

Beispiel:

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

Server Administrator wurde auch erweitert, um anderen Produkten (wie z. B. Dell OpenManage IT Assistant) direkten Zugriff auf Server Administrator-Webseiten zu geben, ohne über die Anmeldeseite gehen zu müssen Anmeldung (wenn Sie zurzeit angemeldet sind und die erforderlichen Berechtigungen haben).

## Konfiguration von Sicherheitseinstellungen auf Systemen, die ein unterstütztes Microsoft Windows-Betriebssystem ausführen

Sie müssen die Sicherheitseinstellungen für Ihren Browser so konfigurieren, dass die Anmeldung am Server Administrator über ein Remote-Verwaltungssystem erfolgt, das ein unterstütztes Microsoft Windows-Betriebssystem ausführt.

Die Sicherheitseinstellungen für den Browser verhindern auf der Client-Seite möglicherweise die Ausführung von Skripten, die vom Server Administrator verwendet werden. Um Skripten auf der Client-Seite zu aktivieren, führen Sie folgende Schritte auf dem Remote-Verwaltungssystem durch.

 **ANMERKUNG:** Wenn der Browser nicht für die Verwendung von Skripten auf der Client-Seite konfiguriert wurde, wird bei der Anmeldung am Server Administrator möglicherweise ein leerer Bildschirm angezeigt. In diesem Fall wird eine Fehlermeldung ausgegeben mit der Anweisung, die Browser-Einstellungen zu konfigurieren.

### Internet Explorer

1. Klicken Sie in Ihrem Internet-Browser auf **Extras** → **Internetoptionen** → **Sicherheit**.
2. Klicken Sie auf das Symbol **Vertrauenswürdige Site**.
3. Klicken Sie auf **Sites**.
4. Kopieren Sie die Web-Adresse für den Zugriff auf das verwaltete Remote-System von der Adresszeile des Browsers aus und fügen Sie die Adresse im Feld **Diese Website zur Zone hinzufügen** ein.
5. Klicken Sie auf **Stufe anpassen**.

Für Windows 2003:

- Unter **Verschiedenes** wählen Sie die Optionsschaltfläche **Meta Refresh zulassen**.
- Unter **Active Scripting** wählen Sie die Optionsschaltfläche **Aktivieren**.
- Unter **Active Scripting** wählen Sie die Optionsschaltfläche **Skriptzugriff auf Internet Explorer Web Browser-Steuerungen zulassen**.

6. Klicken Sie auf **OK**, um die neuen Einstellungen zu speichern. Schließen Sie den Browser und melden Sie sich bei Server Administrator an.

Um Einfache Anmeldung für Server Administrator ohne Eingabeaufforderung für Benutzeranmeldeinformationen zuzulassen, führen Sie folgende Schritte aus:

1. Klicken Sie in Ihrem Internet-Browser auf **Extras** → **Internetoptionen** → **Sicherheit**.
2. Klicken Sie auf das Symbol **Vertrauenswürdige Site**.

3. Klicken Sie auf **Sites**.
4. Kopieren Sie die Web-Adresse für den Zugriff auf das verwaltete Remote- System von der Adresszeile des Browsers aus und fügen Sie die Adresse im Feld **Diese Website zur Zone hinzufügen** ein.
5. Klicken Sie auf **Stufe anpassen**.
6. Unter **Benutzerauthentifizierung** wählen Sie die Optionsschaltfläche **Automatische Anmeldung mit aktuellem Benutzernamen und Kennwort** aus.
7. Klicken Sie auf **OK**, um die neuen Einstellungen zu speichern. Schließen Sie den Browser und melden Sie sich bei Server Administrator an.

## Mozilla Firefox

1. Starten Sie den Browser.
2. Klicken Sie auf **Bearbeiten→ Einstellungen**.
3. Klicken Sie auf **Erweitert→ Scripts und Plug-ins**.
4. Stellen Sie sicher, dass das **Navigator**-Kontrollkästchen unter **JavaScript aktivieren für** markiert ist.
5. Klicken Sie auf **OK**, um die neuen Einstellungen zu speichern.
6. Schließen Sie den Browser.
7. Melden Sie sich bei Server Administrator an.

## Server Administrator-Homepage

 **ANMERKUNG:** Verwenden Sie nicht die Web-Browser-Symboleleistenschaltflächen (wie z. B. **Zurück** und **Aktualisieren**), während Sie Server Administrator verwenden. Verwenden Sie nur die Navigationshilfen des Server Administrators.

Mit nur wenigen Ausnahmen besteht die Server Administrator-Homepage aus drei Hauptbereichen:

- 1 Die [Allgemeine Navigationsleiste](#) enthält Verknüpfungen zu den allgemeinen Diensten.
- 1 Die [Systemstruktur](#) zeigt alle sichtbaren Systemobjekte an, basierend auf den Zugriffsrechten des Benutzers.
- 1 Das [Maßnahmenfenster](#) zeigt die verfügbaren Verwaltungsmaßnahmen für das gewählte Systemstrukturobjekt an, basierend auf den Zugriffsrechten des Benutzers. Das Maßnahmenfenster enthält drei Funktionsbereiche:
  - o Die Maßnahmenregister zeigen die Primärmaßnahmen oder Maßnahmenkategorien an, die, basierend auf den Zugriffsrechten des Benutzers, für das gewählte Objekt verfügbar sind.
  - o Die Maßnahmenregister sind aufgeteilt in Unterkategorien aller verfügbaren sekundären Optionen für die Maßnahmenregister, basierend auf den Zugriffsrechten des Benutzers.
  - o Der "[Datenbereich](#)" zeigt die Informationen für das gewählte Systemstrukturobjekt, Maßnahmenregister und die Unterkategorie an, basierend auf den Zugriffsrechten des Benutzers.

Wenn man bei der Server Administrator-Startseite angemeldet ist, werden darüber hinaus das Systemmodell, der zugewiesene Systemname und der Benutzername des gegenwärtigen Benutzers sowie die Benutzerberechtigungen oben rechts im Fenster angezeigt.

[Tabelle 3-1](#) listet die Feldnamen der Benutzeroberfläche und das zutreffende System auf, wenn Server Administrator auf dem System installiert ist.

**Tabelle 3-1. Systemverfügbarkeit für die folgenden Feldnamen der Benutzeroberfläche**

Feldname der Benutzeroberfläche	Zutreffendes System
Modulares Gehäuse	Modulares System
Servermodul	Modulares System
Hauptsystem	Modulares System
System	Nicht modulares System
Hauptsystemgehäuse	Nicht modulares System

[Abbildung 3-1](#) zeigt ein Beispiel-Layout für die Server Administrator-Homepage für einen mit Administratorrechten angemeldeten Benutzer.

**Abbildung 3-1. Beispielstartseite von Server Administrator - nicht modulares System**



Abbildung 3-2 zeigt ein Beispiel-Layout für die Server Administrator-Homepage für einen mit Administratorrechten angemeldeten Benutzer auf einem modularen System.

Abbildung 3-2. Beispielstartseite von Server Administrator - modulares System



Durch Klicken auf ein Objekt in der Systemstruktur wird ein entsprechendes Maßnahmenfenster für das Objekt geöffnet. Sie können durch Klicken auf Maßnahmenregister zur Auswahl von Hauptkategorien in das Maßnahmenfenster wechseln und auf die Maßnahmenregister-Unterkategorien klicken, um Zugriff auf weiterführende Informationen oder spezifischere Maßnahmen zu erhalten. Die im Datenbereich des Maßnahmenfensters angezeigten Informationen können von Systemprotokollen über Statusanzeigen bis hin zu Systemsondenanzeigen reichen. Im Datenbereich des Maßnahmenfensters unterstrichene Elemente zeigen eine weitere Funktionalitätsebene an. Wenn Sie auf ein unterstrichenes Element klicken, wird dadurch ein neuer Maßnahmenbereich im Maßnahmenfenster mit einem höheren Maß an Detail erstellt. Zum Beispiel wird durch Klicken auf **Hauptsystemgehäuse/Hauptsystem** in der Unterkategorie Funktionszustand des Maßnahmenregisters Eigenschaften der Zustandsstatus aller im Objekt Hauptsystemgehäuse/Hauptsystem enthaltenen Komponenten angezeigt, deren Funktionszustand überwacht wird.

**ANMERKUNG:** Administrator- oder Hauptbenutzer-Zugriffsrechte sind zur Ansicht der meisten der konfigurierbaren Systemstrukturobjekte, Systemkomponenten, Maßnahmenregister oder Datenbereichsfunktionen erforderlich. Darüber hinaus haben nur Benutzer, die mit Administrator-Rechten angemeldet sind, Zugriff auf kritische Systemfunktionen wie die Herunterfahren-Funktion im Register **Herunterfahren**.

## Unterschiede der Server Administrator-Schnittstellen bei modularen und nicht-modularen Systemen

In der folgenden Tabelle sehen Sie die Verfügbarkeit von Server Administrator-Funktionen für modulare und nicht-modulare Systeme. Ein Häkchen zeigt an, dass die Funktion verfügbar ist. Ein Kreuz bedeutet, dass die Funktion nicht verfügbar ist.

Funktionen	Modulares System	Nicht-modulares System
Batterien	✓	✓
Netzteile	✗	✓
Lüfter	✗	✓
Hardwareleistung	✗	✓
		(ab System xx0x)
Eingriff	✗	✓
Speicher	✓	✓
Netzwerk	✓	✓
Ports	✓	✓
Power Management	✓	✓

		(ab System xx0x)
Prozessoren	✓	✓
Remotezugriff	✓	✓
Wechselbarer Flash-Datenträger	✓	✓
Steckplätze	✓	✓
Temperaturen	✓	✓
Spannungen	✓	✓
Modulares Gehäuse (Gehäuse- und CMC-Informationen)	✓	✗

## Allgemeine Navigationsleiste

Die allgemeine Navigationsleiste und ihre Verknüpfungen stehen allen Benutzerstufen im Programm zur Verfügung.

- 1 Wenn Sie auf **Einstellungen** klicken, wird die **Einstellungs-Homepage** geöffnet. Siehe [Voreinstellungen-Homepage verwenden](#)".
- 1 Durch Klicken auf **Support** werden Sie mit der Dell Support-Website verbunden.
- 1 Durch Klicken auf **Hilfe** öffnet sich das Fenster der kontextsensitiven Onlinehilfe. Siehe [Online-Hilfe verwenden](#)".
- 1 Klicken Sie auf **Info** zur Anzeige der Server Administrator-Version und Copyright-Informationen.
- 1 Klicken Sie auf **Abmelden**, um die aktuelle Server Administrator-Programmsitzung zu beenden.

## Systemstruktur

Die Systemstruktur wird auf der linken Seite der Server Administrator-Homepage angezeigt und enthält die anzeigbaren Komponenten des Systems. Die Systemkomponenten werden nach Komponententyp kategorisiert. Wenn Sie das Hauptobjekt (**Modulares Gehäuse**→ **System/Servermodul** genannt) erweitern, sind die System-/Servermodulkomponenten-Hauptkategorien, die erscheinen können, **Hauptsystemgehäuse/Hauptsystem**, **Software** und **Speicher**.

Um einen Zweig der Struktur zu erweitern, klicken Sie auf das Pluszeichen (  ) links neben einem Eintrag oder doppelklicken Sie auf den Eintrag. Ein Minuszeichen (  ) zeigt einen expandierten Eintrag an, der nicht weiter expandiert werden kann.

## Maßnahmenfenster

Wenn Sie auf ein Element der Systemstruktur klicken, werden Details über die Komponenten bzw. das Objekt im Datenbereich des Maßnahmenfensters angezeigt. Durch Klicken auf ein Maßnahmenregister werden alle verfügbaren Benutzeroptionen in einer Liste von Unterkategorien angezeigt.

Wenn Sie auf ein Objekt in der System-/Servermodulstruktur klicken, wird das Maßnahmenfenster dieses Objekts geöffnet und die verfügbaren Maßnahmenregister werden angezeigt. Der Datenbereich geht standardmäßig zu einer voreingestellten Unterkategorie des ersten Maßnahmenregisters für das gewählte Objekt. Die voreingestellte Unterkategorie ist gewöhnlich die erste Option. So wird z. B. durch Klicken auf das Objekt **Hauptsystemgehäuse/Hauptsystem** ein Maßnahmenfenster geöffnet, in dem das Maßnahmenregister **Eigenschaften** mit der Unterkategorie **Funktionszustand** im Datenbereich des Fensters angezeigt wird.

## Datenbereich

Der Datenbereich befindet sich unter den Maßnahmenregistern auf der rechten Seite der Homepage. Im Datenbereich werden Tasks ausgeführt oder Details zu Systemkomponenten angezeigt. Der Inhalt des Fensters hängt von dem gegenwärtig gewählten Systemstrukturobjekt und Maßnahmenregister ab. Wenn Sie z. B. **BIOS** in der Systemstruktur wählen, wird automatisch das Register **Eigenschaften** gewählt und die Versionsinformationen für die System-BIOS im Datenbereich angezeigt. Der Datenbereich des Maßnahmenfensters enthält viele verbreitete Funktionen, einschließlich Statusanzeigen, Task-Schaltflächen, unterstrichene Einträge und Messanzeigen.

Die Benutzeroberfläche von Server Administrator zeigt das Datum im Format <MM/TT/JJJJ> an.

## System/Servermodul-Komponentenstatusanzeigen

Die Symbole neben den Komponentennamen zeigen den Status der jeweiligen Komponenten an (seit der letzten Seitenaktualisierung).

Tabelle 3-2. System/Servermodul-Komponentenstatusanzeigen

	Ein grünes Kontrollhäkchen zeigt an, dass eine Komponente in Ordnung (normal) ist.
	Ein gelbes Dreieck mit einem Ausrufezeichen zeigt an, dass für eine Komponente ein Warnzustand (nicht kritisch) besteht. Ein Warnzustand tritt ein, wenn eine Sonde oder ein anderes Überwachungsmittel einen Wert für eine Komponente ermittelt, der zwischen bestimmte Mindest- und Höchstwerte fällt. Ein Warnzustand erfordert umgehenden Eingriff.
	Ein rotes X bedeutet, dass eine Komponente einen Ausfall- (kritischen) Zustand erreicht hat. Ein kritischer Zustand tritt ein, wenn eine Sonde oder ein anderes Überwachungsmittel einen Wert für eine Komponente ermittelt, der zwischen bestimmte Mindest- und Höchstwerte fällt. Ein kritischer Zustand

	erfordert sofortigen Eingriff.
	Eine Leerstelle bedeutet, dass der Funktionszustand der Komponente unbekannt ist.

### Task-Schaltflächen

Die meisten innerhalb der Server Administrator-Homepage enthaltenen Fenster enthalten mindestens vier Task-Schaltflächen: **Drucken**, **Exportieren**, **E-Mail** und **Aktualisieren**. In spezifischen Server Administrator-Fenstern befinden sich weitere Task-Schaltflächen. Protokollfenster enthalten beispielsweise auch die Task-Schaltflächen **Speichern unter** und **Protokoll löschen**. Für spezifische Informationen über einzelne Task-Schaltflächen klicken Sie auf **Hilfe** in jedem Homepage-Fenster des Server Administrators zur Anzeige detaillierter Informationen über das betrachtete Fenster.

- 1 Klicken Sie auf **Drucken**, wird eine Kopie des geöffneten Fensters auf dem Standarddrucker ausgegeben.
- 1 Durch das Klicken auf **Exportieren** wird eine Textdatei erstellt, in der die Werte jedes Datenfeldes in dem offenen Fenster aufgelistet sind. Die Exportdatei wird in dem von Ihnen bestimmten Speicherort gespeichert. Unter "[Benutzer- und Systemeinstellungen vornehmen](#)" finden Sie eine Anleitung zur benutzerspezifischen Einstellung der Begrenzungszeichen, mit denen die Datenfeldwerte getrennt werden.
- 1 Durch Klicken auf **E-Mail** wird eine an den vorbestimmten E-Mail-Empfänger adressierte E-Mail-Meldung erstellt. Unter "[Benutzer- und Systemeinstellungen vornehmen](#)" finden Sie eine Anleitung zur Einrichtung Ihres E-Mail-Servers und des Standard-E-Mail-Empfängers .
- 1 Durch Klicken auf **Aktualisieren** werden Statusinformationen über Systemkomponenten in den Datenbereich des Maßnahmenfensters geladen.
- 1 Durch Klicken auf **Speichern unter** wird eine HTML-Datei des Maßnahmenfensters in einer **.zip**-Datei gespeichert.
- 1 Durch Klicken auf **Protokoll löschen** werden alle Ereignisse aus dem im Datenbereich des Maßnahmenfensters angezeigten Protokoll gelöscht.

 **ANMERKUNG:** Die Schaltflächen **Export**, **E-Mail**, **Speichern unter** und **Protokoll löschen** werden nur für Benutzer angezeigt, die mit Hauptbenutzer- oder Admin-Rechten angemeldet sind.

### Unterstrichene Einträge

Durch Klicken auf einen unterstrichenen Eintrag im Datenbereich des Maßnahmenfensters werden weiterführende Details über den Eintrag angezeigt.

### Messanzeigen

Temperatursonden, Lüftersonden und Spannungssonden werden jeweils durch eine Messanzeige dargestellt. Abbildung [Abbildung 3-3](#) zeigt z. B. Messwerte von der CPU-Lüftersonde eines Systems.

Abbildung 3-3. Messanzeige



### Online-Hilfe verwenden

Kontextbezogene Onlinehilfe ist verfügbar für jedes Fenster der Homepage des Server Administrators. Durch Klicken auf **Help (Hilfe)** auf der allgemeinen Navigationsleiste wird ein unabhängiges Hilfefenster geöffnet, das detaillierte Informationen über das betrachtete Fenster enthält. Die Onlinehilfe ist **darauf** ausgelegt, Sie durch die spezifischen Maßnahmen zu leiten, die zur Ausführung aller Aspekte der Server Administrator-Dienste erforderlich sind. Onlinehilfe ist verfügbar für alle Fenster, die angesehen werden können, basierend auf den Software- und Hardwaregruppen, die der Server Administrator auf dem System feststellt, und dem Benutzer-Zugriffsrecht.

### Voreinstellungen-Homepage verwenden

Im linken Fenster der Startseite **Voreinstellungen** (wo auf der Server Administrator-Startseite die Systemstruktur angezeigt wird) werden alle verfügbaren Konfigurationsoptionen im Systemstrukturfenster angezeigt.

S. [Tabelle 3-3](#) für verfügbare Konfigurationsoptionen der Einstellungs-Startseite.

Tabelle 3-3. Konfigurationsoptionen der Voreinstellungen-Homepage verwalten

	.....	Allgemeine Einstellungen
---	-------	--------------------------

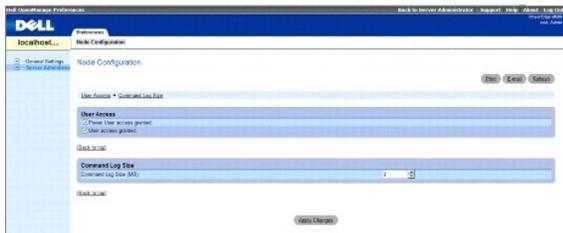
Sie können das Register **Voreinstellungen** einsehen, nachdem Sie sich zur Verwaltung eines Remote-Systems angemeldet haben. Dieses Register ist auch verfügbar, wenn Sie sich zur Verwaltung des Server Administrator Web Servers oder des lokalen Systems anmelden.

Wie die Server Administrator-Startseite besteht auch die **Voreinstellungen**-Startseite aus drei Hauptbereichen:

- 1 Die allgemeine Navigationsleiste enthält Verknüpfungen zu den allgemeinen Diensten.
  - o Klicken auf **Zurück zu Server Administrator** kehrt zur Server Administrator-Homepage zurück.
- 1 Im linken Fenster der Startseite **Voreinstellungen** (wo auf der Server Administrator-Startseite die Systemstruktur angezeigt wird) werden die **Voreinstellungskategorien** für das verwaltete System angezeigt.
- 1 Das **Maßnahmenfenster** zeigt die verfügbaren Einstellungen und Voreinstellungen für das verwaltete System oder den Server Administrator Web Server an.

[Abbildung 3-4](#) zeigt ein Beispiel-Layout für eine Einstellungen-Homepage.

**Abbildung 3-4. Beispiel einer Voreinstellungen-Startseite**



- Managed System

## Managed System-Voreinstellungen

Wenn Sie sich bei einem Remote-System anmelden, befindet sich die Voreinstellungen-Startseite standardmäßig im Knotenkonfigurationsfenster im Register **Voreinstellungen**.

Klicken Sie auf das Objekt Server Administrator, um Benutzern den Zugriff als Benutzer oder Hauptbenutzer zu gewähren bzw. zu verweigern. Abhängig von den Benutzergruppen-Berechtigungen kann das Maßnahmenfenster des Server Administrator-Objekts das Register **Voreinstellungen** aufweisen oder nicht.

Im Register Einstellungen können Sie Folgendes durchführen:

- 1 Zugriff von Benutzern mit Benutzer- oder Hauptbenutzerrechten aktivieren oder deaktivieren
- 1 Die Befehlsprotokollgröße konfigurieren
- 1 SNMP konfigurieren

## Server Administrator Web Server-Voreinstellungen

Wenn Sie sich zur Verwaltung des Server Administrator Web Servers anmelden, befindet sich die **Voreinstellungen**-Startseite standardmäßig im Fenster **Benutzer-Voreinstellungen** im Register Voreinstellungen.

Wegen der Trennung des Server Administrator Web Servers von verwalteten System werden die folgenden Optionen angezeigt, wenn Sie sich mit dem Manage Web Server-Link beim Server Administrator Web Server anmelden:

- 1 Web Server-Voreinstellungen
- 1 X.509-Zertifikatsverwaltung

Weitere Informationen zum Zugriff auf diese Funktionen finden Sie unter '[Dienste des Server Administrator](#)'.

## Dell Systems Management Server Administration-Verbindungsdienst und Sicherheits-Setup

Dieser Abschnitt behandelt die folgenden Themen:

- 1 [Benutzer- und Systemeinstellungen vornehmen](#)
- 1 [X.509-Zertifikatsverwaltung](#)

### Benutzer- und Systemeinstellungen vornehmen

Benutzer- und Secure Port-Systemeinstellungen werden auf der Startseite **Einstellungen** eingestellt.

 **ANMERKUNG:** Zum Festlegen oder Zurücksetzen von Benutzer- oder Systemeinstellungen 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-Systemeinstellungen 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.

- 1 Mit der Funktion **Sitzungszeitüberschreitung** kann die Zeit begrenzt werden, in der eine Server Administrator-Sitzung aktiv bleiben kann. Wählen Sie die Optionsschaltfläche **Enable (Aktivieren)** aus, um den Server Administrator die Sitzung beenden zu lassen, wenn während eines festgelegten Zeitraums von Minuten keine Benutzermaßnahme stattfindet. Benutzer, deren Sitzung beendet wird, müssen sich erneut anmelden. Wählen Sie die Optionsschaltfläche **Deaktivieren**, um die Zeitüberschreitungsfunktion des Server Administrators zu deaktivieren.

- 1 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. Eine Liste der Standardschnittstellen erhalten Sie im *Dell OpenManage-Installations- und Sicherheitsbenutzerhandbuch*.

- 1 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:** Wenn der Wert für **IP-Adresse binden an** auf einen anderen Wert als **Alle** geändert wird, dann kann dies dazu führen, dass andere Anwendungen oder Browser nicht mehr auf den Server Administrator im verwalteten System zugreifen können.

- 1 Die Felder **SMTP-Servername** und **DNS-Suffix für SMTP-Server** bestimmen das Suffix für das Einfache Mail-Übertragungsprotokoll (SMTP) und den Domänennamenserver (DNS) einer Firma oder Organisation. Um für den Server Administrator das Versenden von E-Mails zu aktivieren, muss die IP-Adresse und das DNS-Suffix für den SMTP-Server für die Firma oder Organisation in die entsprechenden Felder eingegeben werden.

 **ANMERKUNG:** Aus Sicherheitsgründen gestattet Ihre Firma eventuell nicht, dass E-Mails über den SMTP-Server an Empfänger außerhalb gesendet werden.

- 1 Im Feld **Befehlsprotokollumfang** wird der maximale Umfang (in MB) für die Befehlsprotokolldatei festgelegt.

 **ANMERKUNG:** Dieses Feld wird nur angezeigt, wenn Sie sich zur Verwaltung des Server Administrator Web Servers anmelden.

- 1 Das Feld **Support-Verknüpfung** enthält die URL für die Geschäftsabteilung, die die Unterstützung für das verwaltete System leistet.

- 1 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 ,.

- 1 Das Feld **SSL-Verschlüsselung** gibt die Verschlüsselungsstufen für die gesicherten HTTPS-Sitzungen an. Die verfügbaren Verschlüsselungsstufen enthalten **Automatische Verhandlung** und **128 Bit oder höher**.

- o **Automatische Verhandlung:** Um Verbindung vom Browser mit jeder Verschlüsselungsstärke zu erlauben. Der Browser verhandelt automatisch mit dem Server Administrator Web Server und verwendet die höchste verfügbare Verschlüsselungsstufe für die Sitzung. Legacy-Browser mit der schwächeren Verschlüsselung können an den Server Administrator anschließen.
- o **128-Bit oder höher:** Um Verbindungen von Browsern mit 128 Bit oder höherer Verschlüsselungskraft zu erlauben. Eine der folgenden Chiffre-Folgen ist basierend auf den Browser für jegliche feststehenden Sitzungen anwendbar:

SSL\_RSA\_WITH\_RC4\_128\_SHA

SSL\_RSA\_WITH\_RC4\_128\_MD5

SSL\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA

TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA

SSL\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA

TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA

TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA

SSL\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA

- 1 **Key Signing Algorithm (Schlüsselsignierungsalgorithmus)** zeigt die unterstützten Signierungsalgorithmen an. Wählen Sie aus der Drop-down-Liste einen Algorithmus aus. Wenn Sie entweder SHA 512 oder SHA 256 auswählen, müssen Sie sicherstellen, dass Ihr Betriebssystem/Browser diesen Algorithmus unterstützt. Wenn Sie eine dieser Optionen auswählen, ohne dass die erforderliche Betriebssystem-/Browserunterstützung zur Verfügung steht, zeigt Server Administrator den Fehler "cannot display the webpage" ("Webseite kann nicht angezeigt werden") an. Dieses Feld bezieht sich ausschließlich auf von Server Administrator automatisch erstellte, selbst unterzeichnete Zertifikate. Die Drop-down-Liste wird grau unterlegt, wenn Sie neue Zertifikate in den Server Administrator importieren oder in diesem erstellen.

 **ANMERKUNG:** Die Option **128-bit or higher (128 Bit oder höher)** lässt keine Verbindungen von Browsern mit niedrigeren SSL-Verschlüsselungsstärken zu, wie z. B. 40 Bit, 56 Bit.

 **ANMERKUNG:** Starten Sie den Server Administrator Web Server erneut, um die Änderungen wirksam zu machen.

 **ANMERKUNG:** Wenn die Verschlüsselungsstufe auf **128 Bit oder höher** eingestellt ist, können Sie mit einem Browser mit denselben oder höheren Verschlüsselungsstufen auf die Server Administrator-Einstellungen zugreifen oder diese modifizieren.

4. Wenn Sie alle Einstellungen im Fenster **Servereinstellungen** vorgenommen haben, klicken Sie auf **Änderungen anwenden**.

## 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. Um die Systemsicherheit zu gewährleisten, wird empfohlen:

- 1 Entweder ein neues X.509-Zertifikat zu erstellen, ein bestehendes X.509-Zertifikat wiederzuverwenden oder ein Stammzertifikat bzw. eine Zertifikatskette von einer Zertifizierungsstelle (CA) zu importieren.
- 1 Alle Systeme, auf denen Server Administrator installiert ist, haben eindeutige Host-Namen.

 **ANMERKUNG:** Für die Zertifikatsverwaltung müssen Sie mit Administrator-Zugriffsrechten angemeldet sein.

Um X.509-Zertifikate über die Voreinstellungen-Startseite zu verwalten, klicken Sie auf **Allgemeine Einstellungen**, dann auf das Register **Web Server** und auf **X.509-Zertifikat**.

Sie können damit folgende Aufgaben ausführen:

- 1 **Ein neues X.509-Zertifikat erstellen** - Verwenden Sie diese Option, um ein Zertifikat für den Zugriff auf Server Administrator zu erstellen.
- 1 **Zertifikate aufrechterhalten** - Mit dieser Option wird ein bestehendes Zertifikat ausgewählt, auf das Ihr Unternehmen Anspruch hat, und es wird dieses Zertifikat verwendet, um den Zugriff auf Server Administrator zu steuern.
- 1 **Ein Stammzertifikat importieren** - Mit dieser Option können Sie das Stammzertifikat sowie die Antwort auf das Zertifikat (im Format PKCS#7) importieren, die Sie von der vertrauenswürdigen Zertifizierungsstelle erhalten haben.
- 1 **Zertifikatskette von einer CA importieren** - Diese Option ermöglicht Ihnen, die Antwort auf das Zertifikat (im Format PKCS#7) von der vertrauenswürdigen Zertifizierungsstelle zu importieren. Einige zuverlässige Zertifizierungsstellen sind Verisign, Thawte und Entrust.

---

## Server Administrator Web Server-Maßnahmeregister

Wenn Sie sich zur Verwaltung des Server Administrator Web Servers anmelden, werden die folgenden Maßnahmeregister angezeigt:

- 1 Herunterfahren
- 1 Protokolle
- 1 Sitzungsverwaltung

---

## Server Administrator steuern

Der Server Administrator startet automatisch jedes Mal, wenn Sie das verwaltete System neu starten. Für einen manuellen Start, Stopp oder Neustart des Server Administrators führen Sie die folgenden Anleitungen aus.

 **ANMERKUNG:** Zur Steuerung des Server Administrators müssen Sie mit Administratorrechten angemeldet sein (als `root` auf unterstützten Red Hat® Enterprise Linux® oder SUSE® LINUX Server -Betriebssystemen).

## Server Administrator starten

## Unterstützte Microsoft Windows-Betriebssysteme

Um Server Administrator auf Systemen zu starten, auf denen ein unterstütztes Microsoft Windows-Betriebssystem ausgeführt wird, führen Sie folgende Schritte durch:

1. Öffnen Sie das Fenster **Dienste**.
2. Klicken Sie mit der rechten Maustaste auf das **Verbindungsdienstsymbol** von **Dell Systems Management Server Administration (DSM SA)**.
3. Klicken Sie auf **Start** (Starten).

## Unterstützte Red Hat Enterprise Linux und SUSE LINUX Enterprise Server- Betriebssysteme

Zum Starten des Server Administrators auf Systemen, die ein unterstütztes Red Hat Enterprise Linux oder SUSE LINUX Enterprise Server-Betriebssystem ausführen, führen Sie den folgenden Befehl von der Befehlszeile aus:

```
dsm_om_connsvc start
```

## Server Administrator anhalten

### Unterstützte Microsoft Windows-Betriebssysteme

Um Server Administrator anzuhalten, führen Sie folgende Schritte durch:

1. Öffnen Sie das Fenster **Dienste**.
2. Klicken Sie mit der rechten Maustaste auf das Symbol **DSM SA- Verbindungsdienst**.
3. Klicken Sie auf **Anhalten**.

### Unterstützte Red Hat Enterprise Linux und SUSE LINUX Enterprise Server- Betriebssysteme

Zum Stoppen des Server Administrators auf Systemen, die ein unterstütztes Red Hat Enterprise Linux oder SUSE LINUX Enterprise Server-Betriebssystem ausführen, führen Sie den folgenden Befehl von der Befehlszeile aus:

```
dsm_om_connsvc stop
```

## Server Administrator neu starten

### Unterstützte Microsoft Windows-Betriebssysteme

Um Server Administrator neu zu starten, führen Sie folgende Schritte durch:

1. Öffnen Sie das Fenster **Dienste**.
2. Klicken Sie mit der rechten Maustaste auf das Symbol **DSM SA- Verbindungsdienst**.
3. Klicken Sie auf **Neu starten**.

### Unterstützte Red Hat Enterprise Linux und SUSE LINUX Enterprise Server- Betriebssysteme

Zum Neustarten des Server Administrators auf Systemen, die ein unterstütztes Red Hat Enterprise Linux oder SUSE LINUX Enterprise Server-Betriebssystem ausführen, führen Sie den folgenden Befehl von der Befehlszeile aus:

```
dsm_om_connsvc restart
```

---

## Server Administrator-Befehlszeilenschnittstelle verwenden

Die Befehlszeilenschnittstelle des Server Administrators (CLI) ermöglicht es Benutzern, wichtige Systemverwaltungs-Tasks von der Befehlseingabeaufforderung des Betriebssystems eines überwachten Systems auszuführen.

In vielen Fällen lässt die CLI Benutzer mit wohlgedachten Aufgabenplänen Informationen über das System schnell abrufen. Mit CLI-Befehlen können Administratoren beispielsweise Stapelverarbeitungsprogramme oder Skripts schreiben, die zu bestimmten Zeiten ausgeführt werden sollen. Wenn diese Programme ausgeführt werden, können sie Berichte über wichtige Komponenten, z. B. Lüftergeschwindigkeit, sammeln. Mit zusätzlichem Skripting kann die CLI zur Sammlung von Daten während Spitzenbelastungszeiten verwendet werden, die dann mit den zu Zeiten geringerer Systembelastung gesammelten Daten verglichen werden. Befehlsergebnisse können zur späteren Analyse an eine Datei weitergeleitet werden. Die Berichte können Administratoren bei der Ermittlung von Daten helfen, die zur Feststellung von Gebrauchsmustern, zur Rechtfertigung des Einkaufs neuer Systemressourcen oder zur Konzentration auf den Zustand einer Problemkomponente verwendet werden können.

Vollständige Anleitungen über die Funktionen und Verwendung der CLI finden Sie im Benutzerhandbuch für die *Dell OpenManage Server Administrator-Befehlszeilenschnittstelle*.

---

[Zurück zum Inhaltsverzeichnis](#)