# Dell OpenManage Server Administrator Version 7.1

# Benutzerhandbuch

# Anmerkungen und Vorsichtshinweise

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

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

---



**2012 - 06**

# Inhalt

# 1

# Einführung

## Übersicht

Dell OpenManage Server Administrator (OMSA) bietet eine umfassende 1:1-Systemverwaltungslösung in zwei Formen: über eine integrierte Web-Browser-basierte grafische Benutzeroberfläche (GUI) und über eine Befehlszeilenschnittstelle (CLI) über das Betriebssystem. Server Administrator ist so ausgelegt, dass Systemadministratoren Systeme sowohl lokal als auch extern in 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.

Im Kontext von Server Administrator kann ein System ein Standalone-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:

- Systeme, die korrekt funktionieren und Systeme mit Problemen
- Systeme, die Remote-Wiederherstellungsarbeiten erfordern

Server Administrator bietet benutzerfreundliche Verwaltung und Administration von lokalen Systemen und Remote-Systemen über eine umfassende Palette von integrierten Verwaltungsdiensten. Server Administrator ist die einzige Installation auf dem verwalteten System und ist sowohl lokal als auch im Remote-Zugriff über die Startseite von **Server Administrator** zugänglich. Auf Systeme, die im Remote-Zugriff überwacht werden, haben Sie über Einwähl-, LAN- oder Wireless-Verbindungen Zugang. Server Administrator gewährleistet die Sicherheit der Verwaltungsverbindungen durch rollenbasierte Zugriffssteuerung (RBAC), Authentifizierung sowie SSL-Verschlüsselung (Secure Socket Layer).

## Installation

Sie können Server Administrator unter Verwendung der DVD *Dell Systems Management Tools and Documentation* installieren. Die DVD enthält 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 Installationsskripts und RPM-Pakete bereit, um Dell OpenManage Server Administrator und andere Komponenten der Managed System Software auf dem verwalteten System zu installieren oder zu deinstallieren. Lesen Sie für weitere Informationen das *Dell OpenManage Server Administrator Installation Guide* (Dell OpenManage Server Administrator-Installationshandbuch) und das Dell OpenManage Management Station Software Installation Guide (Dell OpenManage Management Station Software-Installationshandbuch) unter **support.euro.dell.com/manuals.**

**ANMERKUNG:** Wenn Sie die OpenSource-Pakete von der *Dell Systems Management Tools and Documentation*-DVD installieren, werden die entsprechenden Lizenzdateien automatisch auf das System kopiert. Wenn Sie diese Pakete entfernen, werden auch die entsprechenden Dateien entfernt.

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. Das 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** heruntergeladen werden.

Das *Server Update Utility-Benutzerhandbuch* bietet Informationen zur Beschaffung 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-Dient enthält Speicherverwaltungsinformationen in einer integrierten grafischen Ansicht.

Detaillierte Informationen zum Storage Management-Dienst finden Sie im *Dell OpenManage Server Administrator Storage Management User's Guide* (Benutzerhandbuch zu Dell OpenManage Server Administrator Storage Management) unter **support.dell.com/manuals**.

### Instrumentationsdienst

Der Instrumentationsdienst gewährt schnellen Zugriff auf detaillierte Fehler- und Leistungsinformationen, die von industriestandardmäßigen Systemverwaltungsagenten gesammelt werden, und erlaubt die Remote-Verwaltung überwachter Systeme, einschließlich Herunter- und Hochfahren des Systems und Sicherheit.

### Remote-Access-Controller

Der Remote Access Controller stellt eine vollständige Remote System Management-Lösung für Systeme dar, 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 bietet darüber hinaus eine Warnungsbenachrichtigung, wenn ein System ausgefallen ist, und ermöglicht den Neustart eines Systems im Remote-Zugriff. Darüber hinaus protokolliert der Remote Access Controller die wahrscheinliche Ursache von Systemabstürzen und speichert den letzten Absturzbildschirm.

### Protokolle

Server Administrator zeigt Protokolle von Befehlen, die das System erhalten oder selbst erzeugt hat, überwachte Hardwareereignisse und Systemwarnungen an. Sie können die Protokolle auf der Startseite anzeigen, drucken oder als Berichte speichern und sie als E-Mail an einen festgelegten Dienstkontakt senden.

# Was ist neu in dieser Version?

Im Folgenden werden die Highlights dieser Version von OpenManage Server Administrator dargestellt:

- Zusätzliche Unterstützung für die folgenden Betriebssysteme:
  - Red Hat Enterprise Linux 5.8 (32-Bit und 64-Bit)
  - Red Hat Enterprise Linux 6.1 (64-Bit)
  - VMware ESXi 5.0-Aktualisierung 1 und 5.1
- Zusätzlicher Support für die Mozilla Firefox 10-, 11- und 12-Browser
- Zusätzlicher Support für die folgenden Betriebssysteme:
  - PowerEdge M820
  - PowerEdge T420
  - PowerEdge T320
- Zusätzlicher Support für PowerEdge *OEM Ready*-Servermodelle, die Wiederverkäufern die benutzerdefinierte Markenbildung gestatten. Weitere Informationen stehen Ihnen unter **dell.com/oem** zur Verfügung.
- Zusätzlicher Support für die folgenden Netzwerkschnittstellenkarten (NICs), konvergierten Netzwerkadapter (CNAs) und Fibre Channels (FCs):
  - Brocade 10Gb CNA (BR1020, BR1741M-k)
  - Emulex Single Port FC16 HBA
  - Emulex Dual Port FC16 HBA
  - Qlogic QLE2460 Single Port FC4 Adapter
  - Qlogic QLE2462 Dual Port FC4 Adapter
  - Brocade BR815- Single Port FC8 Adapter
  - Brocade BR825- Dual Port FC8 Adapter
  - Qlogic QLE2562 Dual Port FC8 Adapter
  - Emulex LPe-12002 Dual Port FC8 Adapter
  - Qlogic QME2572 Dual Port FC8 Adapter
  - Emulex Lpe-1205-M Dual Port FC8 Adapter
  - Qlogic QLE2560 Single Port FC8 Adapter
  - Emulex LPe-12000 Single Port FC8 Adapter

  - Broadcom 57810 Dual Port 10GbE KR Blade Converged Mezzanine Card
  - Broadcom 57810 Dual Port 10Gb Base-T
  - Broadcom 57810 Dual Port 10GbE SFP
  - Qlogic QME8252-K Mezz
  - Qlogic P3+ Dual Port 10Gb SFP+/DA
- Zusätzlicher Support für die folgenden Betriebssysteme:
  - Red Hat Enterprise Linux 5.8 (32-Bit und 64-Bit)
  - Red Hat Enterprise Linux 6.1 (64-Bit)
  - VMware ESXi 5.0

Weitere Informationen zur Liste der hinzugefügten und nicht länger unterstützten Plattformen, zu Betriebssystemen und Browsers finden Sie in der Dell Systems Software Support Matrix Version 7.0 unter **support.dell.com/manuals→ Software→ Systems Management→ Dell OpenManage** Releases.

In der kontextabhängigen Online-Hilfe zu Server Administrator finden Sie weitere Informationen zu den mit dieser Version eingeführten Funktionen.

## Verfügbarkeit von Systemverwaltungsstandards

Dell OpenManage Server Administrator unterstützt die folgenden wichtigen Systemverwaltungsprotokolle:

- HTTPS (HyperText Transfer Protocol Secure)
- CIM (Common Information Model, gemeinsames Informationsmodell)
- Einfaches Netzwerkverwaltungsprotokoll (SNMP)

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. Die Unterstützung für CIM und SNMP ist betriebssystemabhängig und in einigen Fällen auch von der Version des Betriebssystems abhängig.

Informationen zu SNMP-Sicherheitsbedenken finden Sie in der **Infodatei** zu Dell OpenManage Server Administrator (im Lieferumfang der Server Administrator-Anwendung enthalten) oder unter **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 bedeutende Sicherheit zu Systemverwaltungsstandards 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 besteht.

Tabelle 1-1 zeigt die Systemverwaltungsstandards, die für jedes unterstützte Betriebssystem zur Verfügung stehen.

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

| Betriebssystem | SNMP | CIM |
|---|---|---|
| Windows Server 2008-Familie und Windows Server 2003-Familie | Auf dem Installationsmedium des Betriebssystems verfügbar | Immer installiert |
| Red Hat Enterprise Linux | Verfügbar im **net-snmp**-Paket auf dem Betriebssystem-Installationsdatenträger | Nicht verfügbar |
| SUSE Linux Enterprise Server | Verfügbar im **net-snmp**-Paket auf dem Betriebssystem-Installationsdatenträger | Nicht verfügbar |
| VMWare ESX | Verfügbar net-snmp-Paket, das vom Betriebssystem installiert wird | Verfügbar |

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

| Betriebssystem | SNMP | CIM |
|---|---|---|
| VMWare ESXi | SNMP-Trap-Support verfügbar<br>**ANMERKUNG:** ESXi unterstützt SNMP-Traps, nicht jedoch Hardwarebestands-aufnahme über SNMP. | Verfügbar |
| Citrix XenServer 6.0 | Verfügbar im **net-snmp**-Paket auf dem Betriebssystem-Installationsdatenträger | Nicht verfügbar |

# Server Administrator-Startseite

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

# Weitere nützliche Dokumente

Zusätzlich zu dieser Anleitung, können Sie auf die folgenden Anleitungen zugreifen, die unter **support.dell.com/manuals** zur Verfügung stehen. Auf der Seite **Handbücher** klicken Sie auf **Software→ Systemverwaltung**. Klicken Sie auf den entsprechenden Produktlink auf der rechten Seite, um auf die Dokumente zuzugreifen.

- Die *Dell Systems Software Support Matrix* (Dell Systems Software Support-Matrix) bietet Informationen über die verschiedenen Dell-Systeme, die durch diese Systemen unterstützten Betriebssysteme und die Dell OpenManage-Komponenten, die auf diesen Systemen installiert werden können.

- Das *Dell OpenManage Server Administrator Installation Guide* (Installationshandbuch zu Dell OpenManage Server Administrator) enthält Anleitungen zur Installation von Dell OpenManage Server Administrator.
- Das *Dell OpenManage Management Station Software Installation Guide* (Dell OpenManage Management Station Software-Installationshandbuch) enthält Anweisungen für die Installation der Dell OpenManage Management Station-Software.
- Das *Dell OpenManage Server Administrator SNMP Reference Guide* (Dell OpenManage Server Administrator SNMP-Referenzhandbuch) enthält die SNMP-Verwaltungsinformationen-Datenbank (MIB).
- Das *Dell OpenManage Server Administrator CIM Reference Guide* (Dell OpenManage Server Administrator CIM-Benutzerhandbuch) dokumentiert den CIM-Anbieter (Common Information Model), eine Erweiterung der standardmäßigen Verwaltungsobjektformat-Datei (MOF-Datei).
- Im *Dell OpenManage Server Administrator Messages Reference Guide* (Dell OpenManage Server Administrator-Meldungs-Referenzhandbuch) sind die Meldungen aufgeführt, die im Warnungsprotokoll auf der Startseite von **Server Administrator** oder auf der Ereignisanzeige des Betriebssystems angezeigt werden.
- Das *Dell OpenManage Server Administrator Command Line Interface User's Guide* (Dell OpenManage Server Administrator-Benutzerhandbuch für die Befehlszeilenschnittstelle) dokumentiert die vollständige Befehlszeilenschnittstelle für Server Administrator.
- Das *Integrated Dell Remote Access Controller User's Guide* (Benutzerhandbuch zum Integrated Dell Remote Access Controller) gibt detaillierte Auskunft über das Konfigurieren und Verwenden des iDRAC.
- Das *Dell Chassis Management Controller User's Guide* (Dell Chassis Management Controller-Benutzerhandbuch) gibt detaillierte Auskunft über die Installation, Konfiguration und Verwendung des Gehäuseverwaltungscontrollers (CMC).
- Das *Dell Online Diagnostics User's Guide* (Dell Online Diagnostics-Benutzerhandbuch) bietet umfassende Informationen über die Installation und Verwendung von Onlinediagnose auf Ihrem System.

- Das *Dell OpenManage Baseboard Management Controller Utilities User Guide* (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 User's Guide* (Dell OpenManage Server Administrator Storage Management-Benutzerhandbuch) ist ein umfassendes Nachschlagewerk für die Konfiguration und Verwaltung lokaler und Remote-Speicherkomponenten, die an ein System angeschlossen sind.
- Das Benutzerhandbuch zum *Dell Remote Access Controller Racadm User's Guide* (Dell Remote Access Controller / Racadm) finden Sie Informationen zur Verwendung des racadm-Befehlszeilen-Dienstprogramms.
- Das *Dell Remote Access Controller 5 User's Guide* (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 User's Guide* (Dell Update Packages-Benutzerhandbuch) enthält Informationen über Beschaffung und Verwendung von Dell Update Packages als ein Teil Ihrer Systemaktualisierungsstrategie.
- Das *Dell OpenManage Server Update Utility User's Guide* (Dell OpenManage Server Update Utility-Benutzerhandbuch) bietet Informationen über Beschaffung und Verwendung des Server-Aktualisierungsdienstprogramms (SUU), um Dell-Systeme zu aktualisieren oder die Aktualisierungen einzusehen, die für alle im Repository aufgelisteten Systeme verfügbar sind.
- Das *Dell Management Console User's Guide* (Benutzerhandbuch der Dell Management Console) enthält Informationen zur Installation, Konfiguration und Nutzung der Dell Management Console.
- Das *Dell Lifecycle Controller User Guide* (Benutzerhandbuch zum Dell Life Cycle Controller) enthält Informationen zum Einrichten und Verwenden des Unified Server Configurator, um System- und Speicherverwaltungs-Tasks über die gesamte Lebensdauer des Systems durchführen zu können.

- Das *Dell License Manager User's Guide* (Dell License Manager-Benutzerhandbuch) enthält Informationen zur Verwaltung der Komponenten-Server-Lizenzen für Dell yx2x-Server.
- Das *Glossar* mit Informationen zu den in diesem Dokument verwendeten Begriffen.

## Anfordern von technischer Unterstützung

Wenn Sie ein in diesem Handbuch beschriebenes Verfahren nicht verstehen, oder wenn Ihr Produkt nicht die erwartete Leistung erbringt, stehen Ihnen zur Unterstützung Hilfsprogramme zur Verfügung. Weitere Informationen zu diesen Hilfsprogrammen finden Sie unter „Wie Sie Hilfe bekommen" im *Hardware-Benutzerhandbuch* des Systems.

Ferner bietet Dell Unternehmensschulungen und Zertifizierungen an; weitere Informationen finden Sie unter **dell.com/training**. Diese Dienstleistungen stehen unter Umständen nicht an allen Standorten zur Verfügung.

# 2

# Setup und Administration

## Sicherheitsverwaltung

Dell OpenManage Server Administrator bietet Sicherheit durch rollenbasierte Zugriffskontrolle (RBAC), Authentifizierung und Verschlüsselung sowohl für die web-basierte Oberfläche als auch die Befehlszeilenoberfläche.

### 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.

- *Benutzer* können die meisten Informationen anzeigen.
- *Hauptbenutzer* können Warnungsschwellenwerte einstellen und konfigurieren, welche Warnungsmaßnahmen ausgeführt werden sollen, wenn ein Warnungs- oder Fehlerereignis eintritt.
- *Administratoren* können Maßnahmen zum Herunterfahren konfigurieren und durchführen, automatische Wiederherstellungsmaßnahmen für den Fall konfigurieren, dass 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.
- *Administratoren mit erhöhten Rechten* können Informationen anzeigen und verwalten.

Der Server Administrator erteilt Benutzern, die mit *Benutzer*berechtigungen angemeldet sind, Nur-Lese-Zugriff. Benutzer mit *Hauptbenutzer*berechtigungen erhalten Lese- und Schreibzugriff, während Benutzer, die mit *Administrator*-rechten oder *erhöhten Administrator*rechten angemeldet sind, Lese-, Schreib- und Administrator-Zugriffsrechte erhalten. Siehe Tabelle 2-1.

**Tabelle 2-1. Benutzerberechtigungen**

| Benutzerberechtigungen | Zugriffstyp | |
|---|---|---|
| | Ansicht | Verwalten |
| 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 werden die Benutzer zusammengefasst, die Berechtigungen für den Zugriff auf Server Administrator-Dienste und deren Verwaltung aufweisen.

**Tabelle 2-2. Server Administrator-Benutzerberechtigungsebenen**

| Dienst | Erforderliche Benutzerberechtigungsebene | |
|---|---|---|
| | Ansicht | Verwalten |
| Instrumentation | B, H, A, EA | H, A, EA |
| Remote-Zugriff | B, H, A, EA | A, EA |
| Speicherverwaltung | B, H, A, EA | A, EA |

Tabelle 2-3 definiert die Abkürzungen der Benutzerberechtigungsebenen, die in Tabelle 2-2 verwendet werden.

**Tabelle 2-3. Legende der Server Administrator-Benutzerberechtigungsebenen**

| | |
|---|---|
| U | Benutzer |
| P | Hauptbenutzer |
| A | Administrator |
| EA | Administrator mit erhöhten Rechten |

### Authentifizierung

Das Server Administrator-Authentisierungsschema stellt sicher, dass die richtigen Zugriffstypen den korrekten Benutzerberechtigungen zugewiesen werden. Darüber hinaus validiert das Server Administrator-Authentifizierungsschema den Kontext, in dem das gegenwärtige Verfahren ausgeführt wird, wenn die Befehlszeilenschnittstelle (CLI) aufgerufen wird. Dieses Authentifizierungsschema stellt sicher, dass alle Server Administrator-Funktionen korrekt authentifiziert werden, wobei es keine Rolle spielt, ob über die Startseite von **Server Administrator** oder über die CLI auf sie zugegriffen wird.

### Microsoft Windows-Authentifizierung

Für unterstützte Microsoft Windows-Betriebssysteme verwendet die Server Administrator-Authentifizierung Integrated Windows Authentication (früher als NTLM bekannt), um zu authentifizieren. Dieses Authentifizierungssystem ermöglicht den Einbezug der Server Administrator-Sicherheit in ein Gesamtsicherheitsschema 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 verwendet Server Administrator verschiedene Authentifizierungsmethoden, die auf der PAM-Bibliothek basieren (Pluggable Authentication Modules). Benutzer können sich entweder lokal oder im Remote-Zugriff bei Server Administrator anmelden und verschiedene Kontoverwaltungsprotokolle, wie z. B. LDAP, NIS, Kerberos und Winbind, verwenden.

### VMware ESX Server 4.X-Authentifizierung

VMware 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 Sie können ESX Server so konfigurieren, dass ein anderer verteilter Authentifizierungsmechanismus verwendet wird.

**ANMERKUNG:** Auf Systemen, auf denen das VMware ESXi Server 4.x-Betriebssystem ausgeführt wird, benötigen sämtliche Benutzer-Administratorrechte, um sich bei Server Administrator anmelden zu können. Informationen zur Rollenzuweisung finden Sie in der VMware-Dokumentation.

### VMware ESXi Server 5.XP1-Authentifizierung

ESXi Server authentifiziert Benutzer, die auf ESXi-Hosts zugreifen, unter Verwendung des vSphere/VI Client oder Software Development Kit (SDK). 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 durch: Einrichten von Benutzern, Gruppen, Berechtigungen und Rollen, Konfigurieren von Benutzerattributen, Hinzufügen Ihrer eigenen Zertifikate und Bestimmen, ob SSL verwendet werden soll.

**ANMERKUNG:** Auf Systemen, auf denen das VMware ESXi Server 5.0 P1-Betriebssystem ausgeführt wird, benötigen sämtliche Benutzer-Administratorrechte, um sich bei Server Administrator anmelden zu können. Informationen zur Rollenzuweisung finden Sie in der VMware-Dokumentation.

### Verschlüsselung

Zugriff auf den Server Administrator erfolgt über eine sichere HTTPS-Verbindung mittels Secure Socket Layer-Technologie (SSL) zur Gewährleistung 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 Server-Betriebssystemen zum Schutz der Benutzeranmeldeinformationen und anderer sensibler Daten verwendet, die über die Socket-Verbindung übertragen werden, wenn ein Benutzer auf die Startseite von **Server Administrators** 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 der Betriebssystemauslegung 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. Nennen Sie möglicherweise die Gastkonten um, um zu verhindern, dass die Remote-Skripte die Konten über die Standard-Gastkontonamen aktivieren 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 Benutzer zur OpenManage-Software hinzufügen wollen. Sie müssen keine neuen Benutzer in 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. Unter „Die Active Directory-Anmeldung verwenden“ auf Seite 53 finden Sie weitere Informationen zur Verwendung von 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 auf den Container, dem Sie den neuen Benutzer hinzufügen möchten. Wechseln Sie dann zu **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:

`useradd -d <Startverzeichnis> -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:** Weisen Sie jedem Benutzerkonto mit Zugriff auf den Server Administrator ein Kennwort zu, um den Zugriff auf die kritischen Systemkomponenten zu schützen.

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:

`useradd -d <Startverzeichnis> -g root <Benutzername>`

**ANMERKUNG:** Stellen Sie als primäre Gruppe `root` ein.

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:** Weisen Sie jedem Benutzerkonto mit Zugriff auf den Server Administrator ein Kennwort zu, um den Zugriff auf die kritischen Systemkomponenten zu schützen.

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 gleichwertiger Benutzer angemeldet sein, um diese Verfahren auszuführen.

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 Legende für das Hinzufügen der Rollendefinition zur Datei *omarolemap* auf.

**Tabelle 2-4. Legende 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.

### *Bewährte Verfahren bei der Verwendung der omarolemap-Datei*

Nachfolgend sind die bewährten Verfahren aufgeführt, die im Zusammenhang mit der **omarolemap**-Datei berücksichtigt werden sollten:

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

| | | |
|---|---|---|
| root | * | Administrator |
| +root | * | Hauptbenutzer |
| * | * | Benutzer |

- Ändern Sie nicht die **omarolemap**-Dateiberechtigungen oder das Dateiformat.
- Verwenden Sie nicht die Loop Back-Adresse für *<Hostname>*, z. B.: localhost oder 127.0.0.1.
- Wenn die Änderungen für die Datei **omarolemap** nach einem Neustart der Verbindungsdienste nicht wirksam werden, konsultieren Sie das Befehlsprotokoll, um die Fehler einzusehen.
- 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 in den folgenden Fällen die standardmäßigen Betriebssystembenutzerberechtigungen:
  - Ein Benutzer wird in der **omarolemap**-Datei heruntergestuft.
  - Es sind doppelte Einträge für Benutzernamen oder Gruppen mit dem gleichen *<Hostnamen>* vorhanden.
- *Leerzeichen* können anstelle von [Tab] als Begrenzungszeichen für Spalten verwendet werden.

### Erstellen von Server Administrator-Benutzern für VMware ESX 4.X, ESXi 4.X und ESXi 5.X

So fügen Sie der Tabelle „Benutzer“ einen Benutzer hinzu:

1. Melden Sie sich unter Verwendung des vSphere Client beim Host an.
2. Klicken Sie auf das Register **Benutzer und Gruppen** und klicken Sie auf **Benutzer**.
3. Klicken Sie auf eine beliebige Stelle in der Tabelle „Benutzer“ und klicken Sie auf **Hinzufügen**, um das Dialogfeld **Neuen Benutzer hinzufügen** zu öffnen.
4. 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.

5 Um einem Benutzer zu erlauben, über eine Befehls-Shell auf den ESX/ESXi-Host zuzugreifen, wählen Sie **Diesem Benutzer Shell-Zugriff gewähren** aus. Benutzer, die ausschließlich über den vSphere Client auf den Host zugreifen, benötigen keinen Shell-Zugriff.

6 Sie können den Benutzer zu einer Gruppe hinzufügen, indem Sie den Gruppennamen aus dem Drop-Down-Menü **Gruppe** auswählen und auf **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**.

Es wird ein roter Kreis mit einem X über dem Benutzernamen angezeigt, um anzuzeigen, dass dieses Konto deaktiviert ist.

## SNMP-Agenten konfigurieren

Der Server Administrator unterstützt den Systemverwaltungsstandard SNMP (einfaches Netzwerkverwaltungsprotokoll) 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. Zum Konfigurieren des SNMP-Agenten für die korrekte Interaktion mit Verwaltungsanwendungen, wie z. B. dem Dell OpenManage IT Assistant, führen Sie die in den folgenden Abschnitten beschriebenen Verfahren durch.

**ANMERKUNG:** Die Standardkonfiguration des SNMP-Agenten enthält normalerweise einen SNMP-Community-Namen wie z. B. **public**. Nennen Sie aus Sicherheitsgründen die Standard-SNMP-Community-Namen um. Informationen zur Umbenennen von SNMP-Community-Namen finden Sie im entsprechenden nachfolgenden Abschnitt.

**ANMERKUNG:** SNMP-Set-Vorgänge sind in Server Administrator Version 5.2 oder später standardmäßig deaktiviert. Server Administrator bietet Unterstützung, um SNMP-Set-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 finden im *Benutzerhandbuch zur Dell OpenManage Server Administrator-Befehlszeilenoberfläche*.

**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 SNMP-Set-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:

- „SNMP-Agenten für Systeme konfigurieren, auf denen unterstützte Windows-Betriebssysteme ausgeführt werden“ auf Seite 29.
- „SNMP-Agenten auf Systemen konfigurieren, auf denen unterstützte Red Hat Enterprise Linux-Betriebssysteme ausgeführt werden“ auf Seite 32.

- „SNMP-Agent auf Systemen konfigurieren, auf denen der unterstützte SUSE Linux Enterprise Server ausgeführt wird“ auf Seite 36.
- „SNMP-Agenten auf Systemen konfigurieren, die unterstützte VMware ESX 4.X-Betriebssysteme zu Proxy VMware MIBs ausführen“ auf Seite 39.
- „Konfigurieren des SNMP-Agent auf Systemen, die unterstützte VMware ESXi 4.X- und ESXi 5.X-Betriebssysteme ausführen“ auf Seite 41.

## 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 durch:

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 die Registerkarte **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-Dienst** 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.

   So fügen Sie einen Community-Namen hinzu:

   a Klicken Sie in der Liste **Akzeptierte Community-Namen** auf **Hinzufügen**.

      Das Fenster **Konfiguration von SNMP-Dienst** wird angezeigt.

   b Geben Sie in das Textfeld **Community-Name** den Community-Namen eines Systems ein, das Ihr System verwalten kann (die Standardeinstellung ist public [öffentlich]) und klicken Sie auf **Hinzufügen**.

      Das Fenster **Eigenschaften von SNMP-Dienst** wird angezeigt.

So bearbeiten Sie einen Community-Namen:

a Wählen Sie einen Community-Namen aus der Liste **Akzeptierte Community-Namen** aus, und klicken dann Sie auf **Bearbeiten**.

Das Fenster **Konfiguration von SNMP-Dienst** wird angezeigt.

b Nehmen Sie alle erforderlichen Änderungen am Community-Namen des Systems, das Ihr System verwalten kann, im Textfeld **Community-Name** vor und klicken Sie auf **OK**.

Das Fenster **Eigenschaften von SNMP-Dienst** wird angezeigt.

6 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 Management Station gesendet werden können.

1 Öffnen Sie das Fenster **Computerverwaltung**.

2 Erweitern Sie das Symbol **Computerverwaltung** im Fenster, falls erforderlich.

3 Erweitern Sie das Symbol **Dienste und Anwendungen** und klicken Sie auf **Dienste**.

4 Scrollen Sie durch die Liste der Dienste, bis Sie **SNMP-Dienste** finden, klicken Sie mit der rechten Maustaste auf **SNMP-Dienst** und dann auf **Eigenschaften**.

Das Fenster **Eigenschaften von SNMP-Dienst** wird angezeigt.

5 Klicken Sie auf das Register **Traps**, um eine Community für Traps hinzuzufügen oder um ein Trap-Ziel für eine Trap-Community hinzuzufügen.

a Zur Hinzufügung einer Community für Traps geben Sie den Community-Namen im Feld **Community-Name** ein und klicken dann auf **Zur Liste hinzufügen**, gleich neben dem Feld **Community-Name**.

**b** Zur Hinzufügung eines Trap-Ziels für eine Trap-Community wählen Sie den Community-Namen aus dem Drop-Down-Feld **Community-Name** und klicken Sie auf **Hinzufügen** im Feld **Trap-Ziele**.

Das Fenster **Konfiguration von SNMP-Dienst** wird angezeigt.

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

Das Fenster **Eigenschaften von SNMP-Dienst** wird angezeigt.

**6** Klicken Sie zum Speichern der Änderungen auf **OK**.

## SNMP-Agenten auf Systemen konfigurieren, auf denen unterstützte Red Hat Enterprise Linux-Betriebssysteme ausgeführt werden

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 SNMP-Set-Vorgängen und Senden von Traps an eine Management Station 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 Objektbezeichner (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 ESXi 4.0-Betriebssystemen gewährt die standardmäßige SNMP-Agent-Konfiguration Nur-Lese-Zugriff für die *öffentliche* Community nur an den *System*-Zweig MIB-II (gekennzeichnet mit der OID 1.3.6.1.2.1.1) der MIB-Struktur. Diese Konfiguration lässt nicht zu, dass Verwaltungsanwendungen Informationen von Server Administrator oder andere Systems Management-Informationen außerhalb des *System*-Zweigs MIB-II abrufen oder ändern.

#### Server Administrator SNMP Agent - Installationsmaßnahmen

Wenn Server Administrator die standardmäßige SNMP-Konfiguration während der Installation ermittelt, versucht die Anwendung, die SNMP-Agent-Konfiguration so zu ändern, dass die gesamte MIB-Struktur für die *öffentliche* Community Nur-Lese-Zugriff erhält. Server Administrator ändert die SNMP-Agent-Konfigurationsdatei „**/etc/snm, p/snmpd.conf**“ auf zwei verschiedene Arten:

Mit der ersten Änderung wird die Ansicht auf die gesamte MIB-Struktur freigegeben, und zwar durch Hinzufügen der folgenden Zeile, falls diese noch nicht existiert:

```
view all included.1
```

Mit der zweiten Änderung wird die Zeile für den standardmäßigen *Zugriff* abgeändert, so dass die *öffentliche* Community Nur-Lese-Zugriff auf die gesamte MIB-Struktur erhält. Der Server Administrator sucht die 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 der standardmäßigen SNMP-Agent-Konfiguration erlauben der *öffentlichen* Community den Nur-Lese-Zugriff auf die gesamte MIB-Struktur.

**ANMERKUNG:** Damit sichergestellt ist, dass Server Administrator die SNMP-Agent-Konfiguration ändern kann, um korrekten Zugriff auf die Systems Management-Daten zu gewähren, 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 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 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

Die Konfiguration des SNMP-Community-Namens bestimmt, 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 durch:

1. Suchen Sie 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 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 Management Station 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
```

## SNMP-Agent auf Systemen konfigurieren, auf denen der unterstützte SUSE Linux Enterprise Server ausgeführt wird

Server Administrator verwendet die SNMP-Dienste, die vom ***net-snmp***-Agenten bereitgestellt werden. Sie können den SNMP-Agenten so konfigurieren, dass der SNMP-Zugriff über Remote-Hosts aktiviert ist, der Community-Name geändert werden kann, SNMP-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:** Die Dokumentation des Betriebssystems enthält zusätzliche Details über die SNMP-Konfiguration.

### SNMP-Installationsmaßnahme für Server Administrator

Server Administrator-SNMP kommuniziert mit dem SNMP-Agenten unter Verwendung des SMUX-Protokolls. 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 während der Installation die Zeile **/etc/snmp/snmpd.conf** 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 erteilt Nur-Lese-Zugriff auf die komplette MIB-Struktur an die *öffentliche* Community ausschließlich vom lokalen Host. Mit dieser Konfiguration können SNMP-Verwaltungsanwendungen wie IT Assistant, die auf anderen Hosts ausgeführt werden, Server Administrator-Systeme nicht korrekt 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 der SNMP-Zugang auf den lokalen Host eingeschränkt ist. 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 über einen bestimmten Remote-Host auf ein System zu aktivieren, das Server Administrator ausführt, bearbeiten Sie die SNMP-Agent-Konfigurationsdatei **/etc/snmp/snmpd.conf** und führen die folgenden Schritte durch:

1. Suchen Sie 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_address
   ```

   **ANMERKUNG:** Sie können SNMP-Zugriff von mehreren 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 über alle Remote-Hosts auf ein System zu aktivieren, das Server Administrator ausführt, bearbeiten Sie die SNMP-Agent-Konfigurationsdatei **/etc/snmp/snmpd.conf** und führen die folgenden Schritte durch:

1. Suchen Sie 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 über ein System verwendet wird, das Server Administrator ausführt, bearbeiten Sie die SNMP-Agent-Konfigurationsdatei **/etc/snmp/snmpd.conf** und führen die folgenden Schritte durch:

1. Suchen Sie 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 Assistant zu ändern. Um Remote-Herunterfahren eines Systems von IT Assistant zu aktivieren, müssen SNMP-Set-Vorgänge aktiviert sein.

**ANMERKUNG:** Für den Neustart des Systems sind für die Änderungsverwaltungsfunktionalität keine SNMP-Set-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 die folgenden Schritte durch:

1. Suchen Sie 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-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:

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

### SNMP-Agenten auf Systemen konfigurieren, die unterstützte VMware ESX 4.X-Betriebssysteme zu Proxy VMware MIBs ausführen

Der ESX 4.X-Server kann durch eine einzige Standardschnittstelle 162 unter Verwendung des SNMP-Protokolls verwaltet werden. Hierzu wird `snmpd` zur Verwendung der Standardschnittstelle 162 konfiguriert, und `vmwarehostd` wird zur Verwendung einer anderen (unbenutzten) Schnittstelle konfiguriert, z. B. Schnittstelle 167. Alle SNMP-Aufforderungen des VMWare-MIB-Zweigs 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 (Remote Command-Line Interface) ***vicfg-snmp*** über ein Remote-System (Windows oder Linux). Die RCLI-Hilfsprogramme können von der VMware-Website unter **vmware.com/download/vi/drivers_tools.html** heruntergeladen werden.

So konfigurieren Sie den SNMP-Agent:

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_addr> --username root --password <password> -c <community name> -p X -t <Destination_IP_Address>@162/ <community name>`

   Hierbei steht X für eine unbenutzte Schnittstelle. 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 verwendet wird.

**ANMERKUNG:** Sie können mehrere 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 am 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 gestartet wurden, starten Sie die Dienste neu, 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
   ```

## Konfigurieren des SNMP-Agent auf Systemen, die unterstützte VMware ESXi 4.X- und ESXi 5.X-Betriebssysteme ausführen

Server Administrator unterstützt SNMP-Traps auf den VMware ESXi 4.X- und ESXi 5.X-Betriebssystemen. Wenn nur eine Standalone-Lizenz vorhanden ist, schlägt die SNMP-Konfiguration auf VMware ESXi-Betriebssystemen fehl. Server Administrator unterstützt SNMP-Get- und -Set-Vorgänge auf VMWare ESXi 4.x- und ESXi 5.x-Betriebssystemen nicht, da die erforderliche SNMP-Unterstützung nicht verfügbar ist. Die VMware vSphere-CLI (Befehlszeilenoberfläche) wird verwendet, um Systeme zu konfigurieren, die VMware ESXi 4.X und ESXi 5.X ausführt, um SNMP-Traps an eine Management Station zu senden.

**ANMERKUNG:** Weitere Informationen zur Verwendung der VMware vSphere-Befehlszeilenschnittstelle finden Sie unter **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
   <username> --password <password> -c <community> -t
   <hostname>@162/<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 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 die SNMP-Schnittstelle auf mindestens einer externen Netzwerkschnittstelle geöffnet sein. Wenn der Server Administrator ermittelt, dass keine SNMP-Schnittstelle der Firewall aller externen Netzwerkschnittstellen geöffnet ist, zeigt der Server Administrator eine Warnmeldung an und trägt eine Meldung im Systemprotokoll ein.

Um den SNMP-Anschluss zu öffnen, muss die Firewall deaktiviert, eine gesamte externe Netzwerkschnittstelle der Firewall geöffnet oder der SNMP-Anschluss von mindestens einer externen Netzwerkschnittstelle der Firewall geöffnet werden. Diese Maßnahme kann vor oder nach dem Start des Server Administrators durchgeführt werden.

Um die SNMP-Schnittstelle auf Red Hat Enterprise Linux mittels einer der zuvor beschriebenen Methoden zu öffnen, führen Sie die folgenden Schritte durch:

1. Geben Sie an der Befehlsaufforderung von Red Hat Enterprise Linux den Befehl `setup` ein, und drücken Sie auf 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-Konfiguration** mit dem Nach-Unten-Pfeil aus und drücken Sie <Eingabe>.

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

3 Drücken Sie <Tab>, um **Sicherheitsstufe** auszuwählen und drücken Sie auf 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-Schnittstellennummer 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> die Informationen über die Firewall-Sicherheitsstufen nicht angezeigt werden.

a Zur Deaktivierung der Firewall wählen Sie **Keine Firewall** oder **Deaktiviert** aus und gehen dann zu Schritt Schritt 7.

b Zum Öffnen einer ganzen Netzwerkschnittstelle oder der SNMP-Schnittstelle wählen Sie **Hoch**, **Mittel** oder **Aktiviert** und fahren Sie mit Schritt 4 fort.

4 Drücken Sie <Tab>, um zu **Anpassen** zu wechseln, und drücken Sie auf <Eingabe>.

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

5 Wählen Sie aus, ob eine gesamte Netzwerkschnittstelle oder nur eine SNMP-Schnittstelle auf allen Netzwerkschnittstellen geöffnet werden soll.

a Um eine gesamte Netzwerkschnittstelle zu öffnen, wechseln Sie mit der Tabulatortaste zu einer vertrauenswürdigen Komponente und drücken Sie die Leertaste. Ein Sternchen im Feld links neben dem Gerätenamen zeigt an, dass die gesamte Schnittstelle geöffnet ist.

b Um eine SNMP-Schnittstelle auf allen Netzwerkschnittstellen zu öffnen, wechseln Sie mit der **Tabulatortaste** zu **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 **Beenden** auszuwählen, und drücken Sie die **Eingabetaste**.

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

1. Konfigurieren Sie SuSEfirewall2, indem Sie auf einer Konsole Folgendes ausführen:
   ```
   a.# yast2 firewall
   ```
2. Verwenden Sie die Pfeiltasten, um zu **Zulässige Dienste** zu wechseln.
3. Drücken Sie auf **Alt+d**, um das Dialogfeld **Zusätzliche zulässige Schnittstellen** zu öffnen.
4. Drücken Sie auf **Alt+T**, um den Cursor zum Textfeld **TCP-Schnittstellen** zu bewegen.
5. Geben Sie **snmp** in das Textfeld ein.
6. Drücken Sie auf **Alt-O** und **Alt-N**, um zum nächsten Bildschirm zu wechseln.
7. Drücken Sie auf **Alt-A**, um die Änderungen zu akzeptieren und sie zu übernehmen.

# 3

# Server Administrator verwenden

## Server Administrator-Sitzung starten

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

Daraufhin wird der Bildschirm **Server Administrator Anmelden** angezeigt. Die Standardschnittstelle für Dell OpenManage Server Administrator ist 1311. Falls erforderlich, können Sie die Schnittstelle ändern. Weitere Informationen zum Einrichten Ihrer Systemeinstellungen finden Sie unter „Dell Systems Management Server Administration-Verbindungsdienst und Sicherheits-Setup“ auf Seite 60.

**ANMERKUNG:** Server, die auf XenServer 6.0 ausgeführt werden, können über die Befehlszeilenschnittstelle (CLI) oder einen zentralen Webserver verwaltet werden, der auf einem separaten Rechner installiert ist.

## An- und Abmelden

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

- Server Administrator, Lokales System
- Server Administrator, Verwaltetes System
- Zentraler Webserver

### 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.

Diese Option ist für Server, die auf XenServer 6.0 ausgeführt werden, nicht verfügbar.

So 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-**Anmeldungs**fensters ein.

   Wenn Sie über eine definierte Domäne auf Server Administrator zugreifen, müssen Sie auch den korrekten **Domänen** namen angeben.

2 Wählen Sie das Kontrollkästchen für **Active Directory-Anmeldung** aus, um sich unter Verwendung des Microsoft Active Directory anzumelden. Siehe „Die Active Directory-Anmeldung verwenden“ auf Seite 53.

3 Klicken Sie auf **Senden**.

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

**ANMERKUNG:** Weitere Informationen zum Konfigurieren des Active Directory auf Systemen, die CLI verwenden, finden Sie im *Dell OpenManage Management Station Software-Installationshandbuch*.

## 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 doppelt auf das Symbol **Dell OpenManage Server Administrator** auf Ihrem Desktop.

2 Geben Sie die IP-Adresse oder den Systemnamen oder den vollständigen qualifizierten Domänennamen (FQDN) des verwalteten Systems ein.

**ANMERKUNG:** Wenn Sie den Systemnamen oder den FQDN eingegeben haben, konvertiert der Web Server-Host von Dell OpenManage Server Administrator den Systemnamen oder den FQDN zur IP-Adresse des verwalteten Systems. Sie können auch die Schnittstellennummer des verwalteten Systems eingeben. Beispiel: Host-Name:Schnittstellennummer oder IP-Adresse:Schnittstellennummer. Wenn Sie eine Verbindung zu einem verwalteten Knoten des Citrix XenServer 6.0 herstellen, verwenden Sie die Schnittstelle 5986 im Format „Host-Name:Schnittstellennummer“ oder „IP-Adresse:Schnittstellennummer".

3 Wenn Sie eine Intranet-Verbindung verwenden, wählen Sie das Kontrollkästchen **Zertifikatswarnungen ignorieren** aus.

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“ auf Seite 53.

5 Klicken Sie auf **Senden**.

#### Verfahren 2

Öffnen Sie Ihren Webbrowser, 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 Standardschnittstellennummer

oder

`https://IP-Adresse:1311`

wobei `IP-Adresse` die IP-Adresse für das verwaltete System ist und `1311` die Standardschnittstellennummer. 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 bei Server Administrator anmelden zu können. Anleitungen zum Einrichten von neuen Benutzern finden Sie unter „Setup und Administration“ auf Seite 19.

### Zentraler Web Server-Anmeldung

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

1 Klicken Sie doppelt auf das Symbol **Dell OpenManage Server Administrator** auf Ihrem Desktop. Die Seite „Remote-Anmeldung“ wird angezeigt.

**VORSICHTSHINWEIS: Auf dem Anmeldebildschirm befindet sich das Kontrollkästchen Zertifikatswarnungen ignorieren. Verwenden Sie diese Option mit Vorsicht. Es wird empfohlen, diese Option nur in vertrauenswürdigen Intranet-Umgebungen zu verwenden.**

2. Klicken Sie auf den Link **Webserver verwalten** oben rechts auf dem Bildschirm.
3. Geben Sie den **Benutzernamen**, das **Kennwort** und den **Domänennamen** ein (wenn Sie über eine definierte Domäne auf Server Administrator zugreifen), und klicken Sie auf **Senden**.
4. Wählen Sie das Kontrollkästchen für **Active Directory-Anmeldung** aus, um sich unter Verwendung von Microsoft Active Directory anzumelden. Siehe „Die Active Directory-Anmeldung verwenden“ auf Seite 53.
5. Klicken Sie auf **Senden**.

Klicken Sie zum Beenden der Server Administrator-Sitzung auf der „Allgemeine Navigationsleiste“ auf **Abmelden**. Die Schaltfläche **Abmelden** befindet sich in der rechten oberen Ecke der Startseite von **Server Administrator**.

**ANMERKUNG:** Wenn Sie Server Administrator unter Verwendung von Mozilla Firefox Version 3.0 und 3.5 oder Microsoft Internet Explorer Version 7.0 oder 8.0 starten, erscheint eventuell eine zwischengeschaltete Warnungsseite, auf der das Problem mit dem Sicherheitszertifikat angezeigt wird. Zur Gewährleistung der Systemsicherheit wird dringend empfohlen, entweder ein neues X.509-Zertifikat zu erstellen, ein bestehendes wiederzuverwenden oder ein Stammzertifikat oder eine Zertifikatskette von einer Zertifizierungsstelle (CA) zu importieren. Um solche Warnungsmeldungen über das Zertifikat zu vermeiden, muss das Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle stammen. Weitere Informationen zur X.509-Zertifikatsverwaltung finden Sie unter „X.509-Zertifikatsverwaltung“.

Um die Systemsicherheit zu gewährleisten, empfiehlt Dell, ein Stammzertifikat 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-Webserver noch immer einen nicht vertrauens-unwürdigen Zertifikatsfehler meldet, können Sie durch die Verwendung der Datei **certutil.exe** die Zertifizierungsstelle des verwalteten Systems trotzdem 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 unter Verwendung der erweiterten Schemalösung von Dell bei 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 User's Guide* (Dell OpenManage-Installations- und -Sicherheitsbenutzerhandbuch).

### Einfache Anmeldung

Die Option der einfachen Anmeldung auf Windows-Betriebssystemen 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 **support.microsoft.com/default.aspx?scid=kb;en-us;Q258063**.

Für den Zugriff auf lokale Rechner ist es nicht erforderlich, dass Sie auf der Maschine ein Konto mit entsprechenden Berechtigungen haben (Benutzer, Hauptbenutzer oder Verwalter). Andere Benutzer werden gegen Microsoft Active Directory authentisiert. Um Server Administrator mit Hilfe von Einfachanmeldungs-Authentifizierung gegen Microsoft Active Directory zu starten, müssen die folgenden Parameter ebenfalls eingereicht werden:

```
authType=ntlm&application=[Plugin-Name]
```

wobei *Plugin-Name* = *omsa*, *ita* usw.

Beispiel:

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

Um Server Administrator mit Hilfe von Einfachanmeldungs-Authentifizierung gegen die Benutzerkonten des lokalen Rechners zu starten, müssen die folgenden Parameter ebenfalls eingereicht werden:

```
authType=ntlm&application=[Plugin-
Name]&locallogin=true
```

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

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 (wenn Sie aktuell 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 Skripts, die von Server Administrator verwendet werden. Um Skripts auf der Client-Seite zu aktivieren, führen Sie folgende Schritte auf dem Remote-Verwaltungssystem durch.

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

#### Internet Explorer

1. Klicken Sie im Webbrowser auf **Extras→ Internetoptionen→ Sicherheit**.
2. Klicken Sie auf das Symbol **Vertrauenswürdige Sites**.
3. Klicken Sie auf **Sites**.
4. Kopieren Sie die Webadresse für den Zugriff auf das verwaltete Remote-System von der Adresszeile des Browsers und fügen Sie die Adresse im Feld **Diese Website zur Zone hinzufügen** ein.

5 Klicken Sie auf **Stufe anpassen**.

Bei Microsoft Windows Server 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 des Internet Explorer-Webbrowsersteuerelements zulassen**.

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

Um einfache Anmeldung für Server Administrator ohne Eingabeaufforderung für Benutzeranmeldeinformationen zuzulassen, führen Sie folgende Schritte durch:

1 Klicken Sie im Webbrowser auf **Extras→ Internetoptionen→ Sicherheit**.

2 Klicken Sie auf das Symbol **Vertrauenswürdige Sites**.

3 Klicken Sie auf **Sites**.

4 Kopieren Sie die Webadresse für den Zugriff auf das verwaltete Remote-System von der Adresszeile des Browsers 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.

8 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→ Skripts 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-Startseite

**ANMERKUNG:** Verwenden Sie nicht die Webbrowser-Symbolleistenschaltflächen (wie z. B. **Zurück** und **Aktualisieren**), während Sie Server Administrator verwenden. Verwenden Sie nur die Navigationshilfen von Server Administrator.

Mit wenigen Ausnahmen besteht die **Server Administrator**-Startseite aus drei Hauptbereichen:

- Die allgemeine navigationsleiste enthält Verknüpfungen zu den allgemeinen Diensten.
- Die system tree (systemstruktur) zeigt alle sichtbaren Systemobjekte an, basierend auf den Zugriffsrechten des Benutzers.
- Das maßnahmenfenster zeigt die verfügbaren Verwaltungsmaßnahmen für das gewählte Systemstrukturobjekt an, basierend auf den Zugriffsrechten des Benutzers. Das Maßnahmenfenster enthält drei Funktionsbereiche:
  - Die Maßnahmenregister zeigen die Primärmaßnahmen oder Maßnahmenkategorien an, die, basierend auf den Zugriffsrechten des Benutzers, für das gewählte Objekt verfügbar sind.
  - Die Maßnahmenregister sind aufgeteilt in Unterkategorien aller verfügbaren sekundären Optionen für die Maßnahmenregister, basierend auf den Zugriffsrechten des Benutzers.
  - 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 in der oberen rechten Ecke des Fensters 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 grafischen 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-Startseite für einen mit Administratorrechten angemeldeten Benutzer.

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

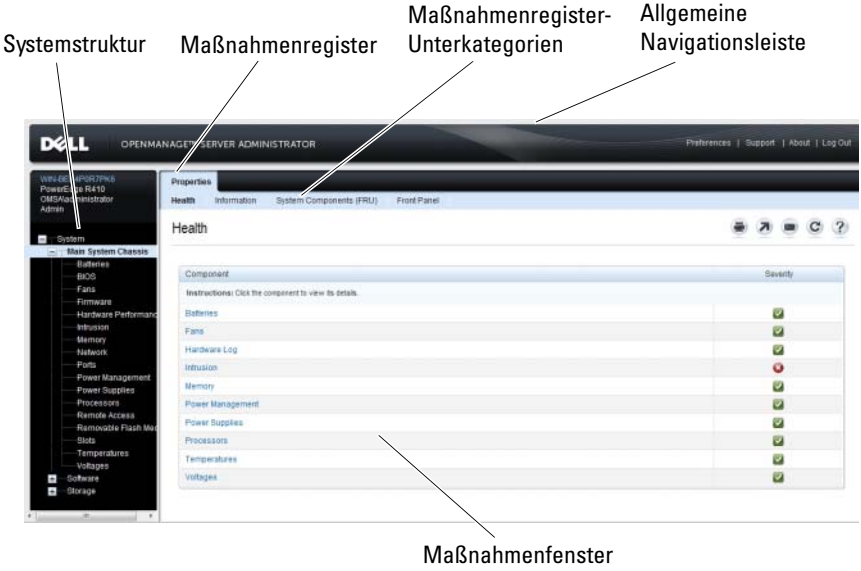
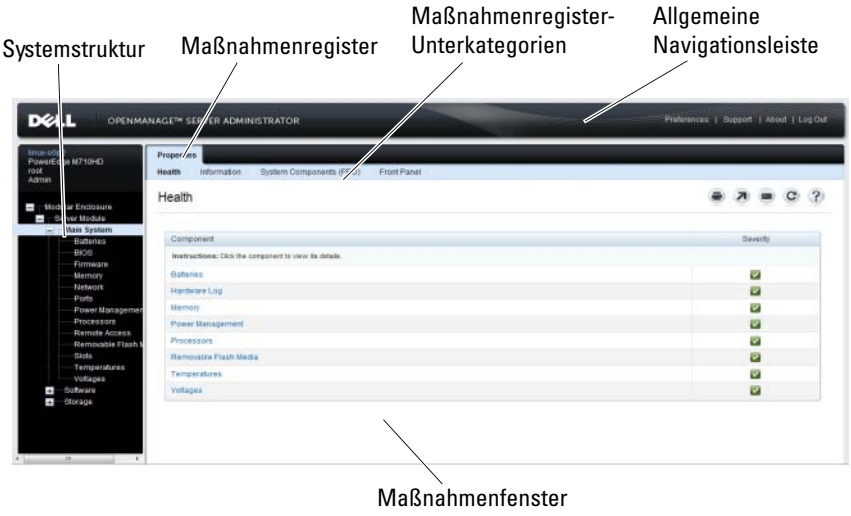



Abbildung 3-2 zeigt ein Beispiel-Layout für die Server Administrator-Startseite für einen mit Administratorrechten angemeldeten Benutzer auf einem modularen System.

**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 das 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 mit mehr Detail im Maßnahmenfenster 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-Zugriffsrechten angemeldet sind, Zugriff auf kritische Systemfunktionen wie die Herunterfahren-Funktion im Register **Herunterfahren**.

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

Tabelle 3-2 führt die Verfügbarkeit von Server Administrator-Funktionen für modulare und nicht-modulare Systeme auf. Ein Häkchen zeigt an, dass die Funktion verfügbar ist. Ein Kreuz bedeutet, dass die Funktion nicht verfügbar ist.

**Tabelle 3-2. Unterschiede der Server Administrator-Schnittstellen bei modularen und nicht-modularen Systemen**

| Funktionen | Modulares System | Nicht-modulares System |
|---|---|---|
| Batterien | ✓ | ✓ |
| Netzteile | ✗ | ✓ |
| Lüfter | ✗ | ✓ |
| Hardwareleistung | ✗ | ✓ (ab System *xx0x*) |
| Eingriff | ✗ | ✓ |
| Speicher | ✓ | ✓ |
| Netzwerk | ✓ | ✓ |
| Schnittstellen | ✓ | ✓ |
| Power Management (Energieverwaltung) | ✓ | ✓ (ab System *xx0x*) |
| Prozessoren | ✓ | ✓ |
| Remote-Zugriff | ✓ | ✓ |
| Wechselbarer Flash-Datenträger | ✓ | ✓ |
| Steckplätze | ✓ | ✓ |
| Temperatures (Temperaturen) | ✓ | ✓ |
| Spannungen | ✓ | ✓ |
| Modulares Gehäuse (Gehäuse- und CMC-Informationen) | ✓ | ✗ |

### Allgemeine Navigationsleiste

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

- Klicken Sie auf **Einstellungen,** um die Startseite **Einstellungen** zu öffnen. Siehe „Einstellungen-Startseite verwenden".
- Klicken Sie auf **Support,** um eine Verbindung mit der Dell Support-Website herzustellen.
- Klicken Sie auf **Info**, um die Server Administrator-Version und Copyright-Informationen anzuzeigen.
- Klicken Sie auf **Abmelden,** um die aktuelle Server Administrator-Programmsitzung zu beenden.

### System Tree (Systemstruktur)

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

Um einen Zweig der Struktur zu expandieren, 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 vorbestimmten Unterkategorie des ersten Maßnahmenregisters für das ausgewählte Objekt. Die vorbestimmte 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 Startseite. Im Datenbereich werden Tasks ausgeführt oder Details zu Systemkomponenten angezeigt. Der Inhalt des Fensters hängt von dem gegenwärtig ausgewählten Systemstrukturobjekt und Maßnahmenregister ab. Wenn Sie z. B. **BIOS** in der Systemstruktur wählen, wird automatisch das Register **Eigenschaften** ausgewählt und die Versionsinformationen für die System-BIOS erscheinen im Datenbereich. Der Datenbereich des Maßnahmenfensters enthält viele allgemeine 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 3-3. System/Servermodul-Komponentenstatusanzeigen**

| | |
|---|---|
|  | Komponente ist funktionsfähig (normal). |
|  | Komponente befindet sich im Warnzustand (nicht-kritisch). Ein Warnzustand tritt ein, wenn eine Sonde oder ein anderes Überwachungsmittel einen Wert für eine Komponente ermittelt, der zwischen bestimmte Minimal- und Maximalwerte fällt. Ein Warnzustand erfordert sofortige Aufmerksamkeit. |
|  | Komponente ist ausgefallen oder befindet sich in einem kritischen Zustand. Ein kritischer Zustand tritt ein, wenn eine Sonde oder ein anderes Überwachungsmittel einen Wert für eine Komponente ermittelt, der zwischen bestimmte Minimal- und Maximalwerte fällt. Ein kritischer Zustand erfordert sofortige Aufmerksamkeit. |
|  | Funktionszustand der Komponente ist unbekannt. |

### *Task-Schaltflächen*

Die meisten auf der Server Administrator-Startseite auftretenden Fenster enthalten mindestens fünf Task-Schaltflächen: **Drucken**, **Exportieren**, **E-Mail**, **Hilfe** und **Aktualisieren**. In bestimmten Server Administrator-Fenstern gibt es weitere Task-Schaltflächen. Protokollfenster enthalten beispielsweise auch die Task-Schaltflächen **Speichern unter** und **Protokoll löschen**.

- Durch Klicken auf **Drucken** ( ) wird eine Kopie des geöffneten Fensters auf dem Standarddrucker ausgegeben.
- Durch Klicken auf **Exportieren** ( ) wird eine Textdatei erstellt, in der die Werte jedes Datenfeldes in dem geöffneten Fenster aufgelistet sind. Die Exportdatei wird an dem von Ihnen bestimmten Speicherort gespeichert. Unter „Benutzer- und Systemeinstellungen vornehmen“ finden Sie eine Anleitung zum Anpassen von Begrenzungszeichen, mit denen die Datenfeldwerte getrennt werden.
- 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.
- Durch Klicken auf **Aktualisieren** ( ) werden Statusinformationen über Systemkomponenten in den Datenbereich des Maßnahmenfensters geladen.
- Durch Klicken auf **Speichern unter** wird eine HTML-Datei des Maßnahmenfensters in einer **.zip**-Datei gespeichert.
- Durch Klicken auf **Protokoll löschen** werden alle Ereignisse aus dem im Datenbereich des Maßnahmenfensters angezeigten Protokoll gelöscht.
- Durch Klicken auf **Hilfe** ( ) werden weitere Einzelheiten über das bestimmte Fenster oder die betrachtete Task-Schaltfläche bereitgestellt.

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

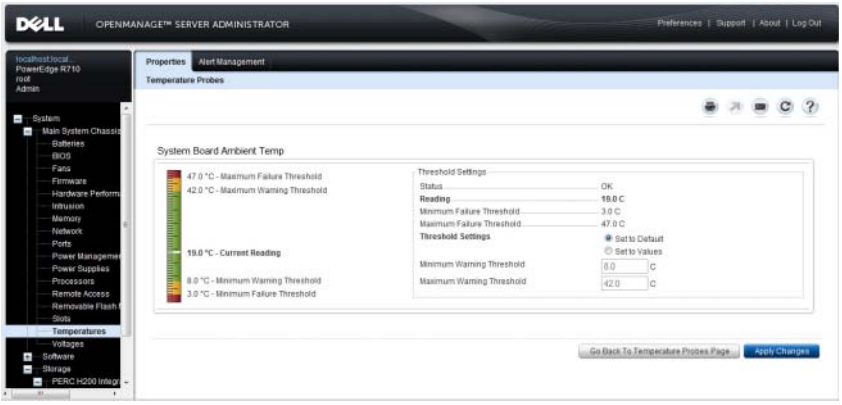
### *Unterstrichene Einträge*

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 Online-Hilfe ist verfügbar für jedes Fenster der Startseite von Server Administrator. 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. Online-Hilfe ist verfügbar für alle Fenster, die angezeigt werden können, basierend auf den Software- und Hardwaregruppen, die der Server Administrator auf dem System feststellt, und der Benutzerberechtigungsebene.

## Einstellungen-Startseite verwenden

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

Die verfügbaren Konfigurationsoptionen der Einstellungen-Startseite sind:

- Allgemeine Einstellungen
- Server Administrator

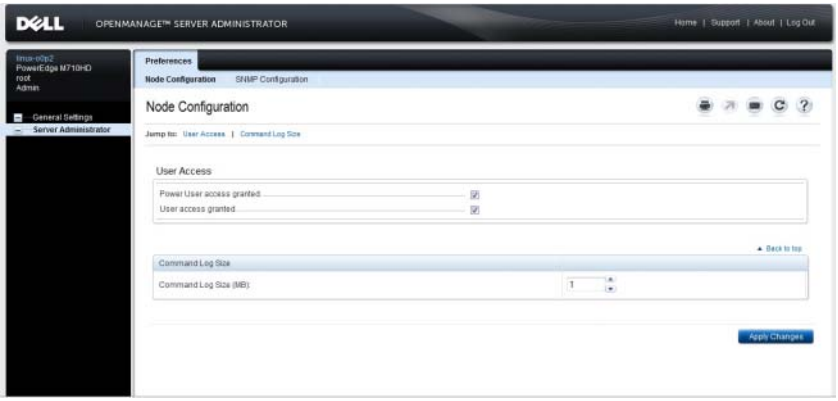
Sie können das Register **Einstellungen** einsehen, nachdem Sie sich zur Verwaltung eines Remote-Systems angemeldet haben. Dieses Register ist auch verfügbar, wenn Sie sich zur Verwaltung des Server Administrator Web Servers oder des lokalen Systems anmelden.

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

- Die allgemeine Navigationsleiste enthält Verknüpfungen zu den allgemeinen Diensten.
  - Klicken Sie auf **Startseite**, um zur Server Administrator-Startseite zurückzukehren.
- Im linken Fenster der Startseite **Einstellungen** (wo auf der Server Administrator-Startseite die Systemstruktur angezeigt wird) werden die Einstellungskategorien für das verwaltete System angezeigt.
- Das Maßnahmenfenster zeigt die verfügbaren Einstellungen und vorbestimmtem Einstellungen für das verwaltete System oder den Server Administrator Web Server an.

Abbildung 3-4 zeigt ein Beispiel-Layout für eine Einstellungen-Startseite.

**Abbildung 3-4. Beispiel einer Einstellungen-Startseite – Managed System**




## Managed System-Einstellungen

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

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 die Registerkarte **Einstellungen** aufweisen oder nicht.

Im Register „Einstellungen“ können Sie Folgendes durchführen:

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

## Server Administrator Web Server-Einstellungen

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

Aufgrund der Trennung des Server Administrator Web Servers vom verwalteten System werden die folgenden Optionen angezeigt, wenn Sie sich unter Verwendung des Manage Web Server-Links bei Server Administrator Web Server anmelden:

- Web Server-Einstellungen
- X.509-Zertifikatsverwaltung

Weitere Informationen zum Zugriff auf diese Funktionen finden Sie unter „Server Administrator-Dienste“.

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

##### *Benutzer- und Systemeinstellungen vornehmen*

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

2. Klicken Sie auf **Allgemeine Einstellungen**.
3. Um einen vorbestimmten E-Mail-Empfänger hinzuzufügen, geben Sie die E-Mail-Adresse des festgelegten Dienstkontakts im Feld **Senden an**: ein und klicken Sie auf **Änderungen übernehmen**.

   **ANMERKUNG:** Durch Klicken auf **E-Mail** in einem beliebigen Fenster wird eine E-Mail-Nachricht, an die eine HTML-Datei des Fensters angehängt ist, an die vorgegebene E-Mail-Adresse gesendet.

   **ANMERKUNG:** Die Webserver-URL wird nicht bewahrt, wenn Sie den OpenManage Server Administrator-Dienst oder das System, auf dem Server Administrator installiert ist, neu starten. Verwenden Sie den Befehl omconfig, um die URL neu einzugeben.

Führen Sie folgende Schritte durch, um die Secure Port-Systemeinstellungen festzulegen.

1. Klicken Sie auf **Einstellungen** auf der allgemeinen Navigationsleiste.

   Die **Einstellungen**-Startseite wird eingeblendet.

2. Klicken Sie auf **Allgemeine Einstellungen** und auf das Register **Web-Server**.

3. Im Fenster **Servereinstellungen** stellen Sie die Optionen nach den Erfordernissen ein.

   - Mit der Funktion **Sitzungszeitüberschreitung** kann die Zeit begrenzt werden, die eine Server Administrator-Sitzung aktiv bleiben kann. Wählen Sie die Optionsschaltfläche **Aktivieren**, um Server Administrator die Sitzung beenden zu lassen, wenn für einen bestimmte Anzahl Minuten keine Benutzermaßnahme stattfindet. Benutzer, deren Sitzung beendet wird, müssen sich erneut anmelden. Wählen Sie die Optionsschaltfläche **Deaktivieren**, um die Zeitüberschreitungsfunktion von Server Administrator zu deaktivieren.
   - Das Feld **HTTPS-Schnittstelle** bestimmt die sichere Schnittstelle für Server Administrator. Die sichere Standardschnittstelle für Server Administrator ist 1311.

   **ANMERKUNG:** Die Änderung der Schnittstellennummer auf eine ungültige bzw. eine bereits belegte Schnittstellennummer kann andere Anwendungen oder Browser beim Zugriff auf Server Administrator auf dem verwalteten System beeinträchtigen. Eine Liste der Standardschnittstellen erhalten Sie im *Dell OpenManage-Installations- und -Sicherheitsbenutzerhandbuch*.

   - Das Feld **Zu bindende IP-Adresse** legt die IP-Adresse(n) für das Managed System fest, mit der sich 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.

- Aus dem Feld **Senden an** gehen die E-Mail-IDs hervor, an die standardmäßig E-Mails zu Aktualisierungen gesendet werden. Sie können mehrere E-Mail-IDs konfigurieren und ein Komma zum Abtrennen der einzelnen E-Mail-IDs verwenden.
- 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 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 eingeben werden.

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

- Im Feld **Befehlsprotokollumfang** wird die maximale Dateigröße in MB für die Befehlsprotokolldatei festgelegt.

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

- Das Feld **Support-Verknüpfung** enthält die URL für die Unternehmenseinheit, die die Unterstützung für das verwaltete System leistet.
- Das Feld **Benutzerdefinierte Begrenzungszeichen** bestimmt das Zeichen, das zur Trennung der Datenfelder der Dateien verwendet wird, die durch die Schaltfläche **Exportieren** erstellt werden. Das Zeichen; ist das standardmäßige Begrenzungszeichen. Andere Optionen sind!, @, #, $, %, ^, *, ~, ?, | und ,.
- Das Feld **SSL-Verschlüsselung** gibt die Verschlüsselungsstufen für die gesicherten HTTPS-Sitzungen an. Zu den verfügbaren Verschlüsselungsstufen gehören **Automatische Verhandlung** und **128 Bit oder höher**.
  - **Automatische Verhandlung** – Ermöglicht die Verbindung über Browser mit beliebiger Verschlüsselungsstärke. Der Browser verhandelt automatisch mit dem Server Administrator Web Server und verwendet die höchste verfügbare Verschlüsselungsstufe für die Sitzung. Frühere Browser mit schwächerer Verschlüsselung können sich mit dem Server Administrator verbinden.

- **128-Bit oder höher** – Ermöglicht Verbindungen über Browser mit 128-Bit- oder höherer Verschlüsselungsstärke. Eine der folgenden Verschlüsselungssammlungen ist basierend auf dem Browser für beliebige feststehende 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

- **Schlüsselsignierungsalgorithmus** – Zeigt die unterstützten Signierungsalgorithmen an. Wählen Sie in der Drop-Down-Liste einen Algorithmus aus. Wenn Sie 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 `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 Server Administrator importieren oder erstellen.

**ANMERKUNG:** Die Option **128 Bit oder höher** lässt keine Verbindungen von Browsern mit niedrigeren SSL-Verschlüsselungsstärken zu, wie z. B. 40 Bit und 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 Parteien weder gesehen noch geändert werden können. Um die Systemsicherheit zu gewährleisten, wird Folgendes dringend empfohlen:

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

Die folgenden Optionen sind verfügbar:

- **Neues X.509-Zertifikat generieren** – Erstellt ein Zertifikat für den Zugriff auf Server Administrator.
- **Zertifikate aufrechterhalten** – Wählt ein bestehendes Zertifikat aus, auf das Ihr Unternehmen Besitzanspruch hat, und es wird dieses Zertifikat verwendet, um den Zugriff auf Server Administrator zu steuern.
- **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.
- **Zertifikatskette von einer CA importieren** – Mit dieser Option können Sie die Antwort auf das Zertifikat (im Format PKCS#7) von der vertrauenswürdigen Zertifizierungsstelle importieren. Zu den vertrauenswürdigen Zertifizierungsstellen gehören Verisign, Thawte und Entrust.

### Server Administrator Web Server-Maßnahmenregister

Im Folgenden werden die Aktionsregisterkarten aufgelistet, die angezeigt werden, wenn Sie sich zum Verwalten des Server Administrator-Webservers anmelden:

- Herunterfahren
- Protokolle
- Sitzungsverwaltung

# Server Administrator-Befehlszeilenschnittstelle verwenden

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

In vielen Fällen lässt die CLI Benutzer mit gut definierten Aufgaben Informationen über das System schnell abrufen. Mit CLI-Befehlen können Administratoren beispielsweise Stapelverarbeitungsprogramme oder Skripts schreiben, die zu bestimmten Zeiten ausgeführt werden. 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 Sammlung von Informationen 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*.

# 4

# Server Administrator-Dienste

## Übersicht

Der Dell OpenManage Server Administrator-Instrumentierungsdienst 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 alle Gehäuse, die das System ausmachen.
Auf der Subsystemebene kann man Informationen über Spannungen, Temperaturen, Lüftergeschwindigkeiten und Speicherfunktionen an den wichtigsten Punkten des Systems anzeigen. Eine detaillierte Beschreibung aller Einzelheiten zu den relevanten Betriebskosten (COO) des Systems ist in einer Zusammenfassung verfügbar. Die Versionsinformationen für BIOS, Firmware, Betriebssystem und installierte Systems Management Software können einfach abgerufen werden.

Ferner können Systemadministratoren den Instrumentierungsdienst zur Ausführung der folgenden wesentlichen Tasks verwenden:

- Festlegung der Minimal- und Maximalwerte für bestimmte kritische Komponenten. Diese Werte, Schwellenwerte genannt, bestimmen den Bereich, in dem ein Warnungsereignis für die betreffende Komponente auftritt (Minimal- und Maximalausfallwerte werden vom Hersteller des Systems festgelegt).
- 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, die über Rund-um-die-Uhr-Überwachung verfügen, festlegen, dass keine Maßnahmen zu ergreifen sind, und sich auf das menschliche Urteil über die beste Reaktion auf ein Ereignis verlassen.

- 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 Netzwerkverwaltungsstationen akzeptieren zu können, die Microsoft Windows Server 2003 ausführen. Weitere Details finden Sie unter 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 **Einstellungen** zeigt standardmäßig auf das Fenster **Zugriffskonfiguration** im Register **Einstellungen**.

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

**ANMERKUNG:** Kontextbezogene Online-Hilfe ist verfügbar für jedes Fenster der Startseite von Server Administrator. Klicken Sie auf **Hilfe**, um ein unabhängiges Hilfefenster zu öffnen, 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. Online-Hilfe ist verfügbar für alle Fenster, die angezeigt werden können, basierend auf den Software- und Hardwaregruppen, die der Server Administrator auf dem System feststellt, und der Benutzerberechtigungsebene.

**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-Zugriffsrechten 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 des Benutzers. Die Systemkomponenten sind nach Komponententyp kategorisiert. Beim Erweitern des Hauptobjekts–„**Modulares Gehäuse**“–„**System-/Servermodul**“–sind die Hauptkategorien von Systemkomponenten, die möglicherweise angezeigt werden: „**Hauptsystemgehäuse/Hauptsystem**“, „**Software**“ und „**Lagerung**.“

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

Detaillierte Informationen zur Storage Management-Dienst-Komponente finden Sie im *Benutzerhandbuch zu Dell OpenManage Server Administrator Storage Management* **unter support.dell.com/manuals**.

# Server Administrator-Startseite-Systemstrukturobjekte

## Nicht unterstützte Funktionen in OpenManage Server Administrator

Aufgrund der Einschränkungen der VMware ESX- und ESXi-Betriebssysteme in den Versionen 4.X und 5.X sind einige der vormals verfügbaren Funktionen von OpenManage Server Administrator in dieser Version nicht mehr verfügbar. Hierzu gehören:

### Nicht unterstützte Funktionen auf ESXi 4.X

- Informationen zur Fibre Channel over Ethernet (FCoE)-Fähigkeit und iSCSI over Ethernet (iSoE)-Fähigkeit

### Nicht unterstützte Funktionen unter ESXi 4.X/5.X

- Informationen zur FCoE-Fähigkeit und zur iSoE-Fähigkeit
- Warnungsverwaltung – Warnungsmaßnahmen
- Netzwerkschnittstelle – Verwaltungsstatus
- Netzwerkschnittstelle – DMA
- Netzwerkschnittstelle – IP-Adresse

- Netzwerkschnittstelle – Maximale Übertragungseinheit
- Netzwerkschnittstelle – Betriebsstatus
- Einstellungen – SNMP-Konfiguration
- Remote-Herunterfahren – Ein-/Ausschalten mit vorherigem Herunterfahren des Betriebssystems
- Info-Details – Details zu den Server Administrator-Komponenten, die nicht auf der Registerkarte **Details** aufgeführt sind
- Rolemap

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

**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-Zugriffsrechten angemeldet sind, Zugriff auf kritische Systemfunktionen wie die Herunterfahren-Funktion im Register Herunterfahren.

## Modulares Gehäuse

**ANMERKUNG:** Für die Zwecke von Server Administrator bezieht sich der Begriff *modulares Gehäuse* auf ein System, das möglicherweise ein oder mehrere modulare Systeme enthält, die in der Systemstruktur als separate Servermodule 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 genauso ein komplettes System wie ein Servermodul.

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

**Eigenschaften**

**Unterregister: Informationen**

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

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

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

So rufen Sie das Fenster **Anmelden** des Geräteverwaltungs-Controllers (CMC) über die Startseite von Server Administrator auf:

1. Klicken Sie auf das Objekt **Modulares Gehäuse**.
2. Klicken Sie auf das Register **CMC-Informationen** und dann auf **CMC-Web-Schnittstelle starten**. Das CMC-Fenster **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**.

**Eigenschaften**

**Unterregister: Funktionszustand | Zusammenfassung | Bestandsinformationen | Autom. Wiederherstellung**

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

- Den aktuellen Warnungsfunktionszustand für Hardware- und Softwarekomponenten im Objekt **Hauptsystemgehäuse/Hauptsystem** und das **Speicher**-Objekt anzeigen.
- Die detaillierten Zusammenfassungen für alle Komponenten im überwachten System anzeigen.
- Die Bestandsinformationen für das überwachte System anzeigen und konfigurieren.
- Die automatischen Systemwiederherstellungsmaßnahmen (Betriebssystem-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 nach eingestellter Zeitüberschreitungsperiode (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 Zeitüberschreitungsperiode ist und *h* das Heartbeat-Intervall. 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, in dem 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, funktioniert die Funktion eventuell nicht richtig. Wenn dies eintritt, müssen Sie das System manuell neu starten. Der Watchdog-Zeitgeber kann maximal auf 720 Sekunden eingestellt werden.

### Herunterfahren

### Unterregister: Remote-Herunterfahren | Temperaturbedingtes Herunterfahren | Web Server herunterfahren

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

- Die Optionen zum Herunterfahren und Remote-Herunterfahren des Betriebssystems konfigurieren.
- Die Schweregradstufe des temperaturbedingten Herunterfahrens einstellen, das das System herunterfährt, wenn ein Temperatursensor eine Warnung oder einen Fehlerwert zurückgibt.

  **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.

- Fahren Sie den DSM SA-Verbindungsdienst (Web Server) herunter.

  **ANMERKUNG:** Server Administrator ist nach wie vor 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:

- Das Protokoll für die integrierte Systemverwaltung (ESM) oder das Systemereignisprotokoll (SEL) als Liste aller mit den Hardwarekomponenten des Systems verbundenen Ereignissen anzeigen. Das Statusanzeigesymbol neben dem Protokollnamen wechselt vom normalen Status ( ) zum nicht-kritischen Status ( ), wenn die Protokolldatei 80 Prozent der Kapazität erreicht. Auf den Dell PowerEdge *x*9xx- *und* xx1x-Systemen wechselt das Statusanzeigesymbol neben dem Protokollnamen zum kritischen Status ( ), wenn die Protokolldatei 100 Prozent der Kapazität erreicht.

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

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

  **ANMERKUNG:** Im *Server Administrator-Meldungs-Referenzhandbuch* finden Sie eine vollständige Erklärung von Beschreibung, Schweregrad und Ursache aller Warnungsereignis-IDs.

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

**ANMERKUNG:** Unter „Server Administrator-Protokolle“ erhalten Sie vollständige Anweisungen zum Anzeigen, Drucken, Speichern und Senden von Protokollen per E-Mail.

**Warnungsverwaltung**

**Unterregister: Warnungsmaßnahmen | Plattformereignisse | SNMP-Traps**

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

- Die aktuellen Warnungsmaßnahmen-Einstellungen anzeigen und die Warnungsmaßnahmen festlegen, die ausgeführt werden sollen, wenn ein Systemkomponentensensor einen Warnungs- oder Ausfallwert sendet.
- Die aktuellen Plattformereignisfilter-Einstellungen anzeigen und die Plattformereignisfilter-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 Plattformereignis gesendet werden soll.

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

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

  **ANMERKUNG:** Im Fenster **Warnungsmaßnahmen** sind alle Warnungsmaßnahmen für alle potenziellen Systemkomponentensensoren aufgelistet, auch wenn diese in Ihrem System 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:

- Sitzungsinformationen für die aktuellen Benutzer anzeigen, die sich bei Server Administrator angemeldet haben.
- 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:

- Batterien
- BIOS
- Lüfter
- Firmware
- Hardwareleistung
- Eingriff
- Speicher
- Netzwerk
- Schnittstellen
- Energieverwaltung
- Netzteile
- Prozessoren
- Remote-Zugriff
- Wechselbarer Flash-Datenträger
- Steckplätze
- Temperatures (Temperaturen)
- Spannungen

**ANMERKUNG:** Hardware-Leistung wird nur auf Dell PowerEdge-Systemen ab Version *xx*0x unterstützt. Die Netzteiloption ist auf Dell PowerEdge 1900-Systemen nicht verfügbar. Die Energieverwaltung wird auf bestimmten Dell PowerEdge-Systemen ab Version *xx*0x unterstützt. Die Funktionen für die Netzteil- und die Stromversorgungsüberwachung sind nur auf Systemen verfügbar, die mit mindestens zwei redundanten, im laufenden Betrieb austauschbaren Netzteilen ausgerüstet sind. Diese Funktionen sind für dauerhaft installierte, nicht-redundante Netzteile, die keine Energieverwaltungsschaltung aufweisen, nicht verfügbar.

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 die folgende Registerkarte: **Eigenschaften**.

### Eigenschaften

**Unterregister: Funktionszustand | Informationen | Systemkomponenten (FRU) | Vorderes Bedienfeld**

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

- Den Zustand oder Status von Hardwarekomponenten und Sensoren anzeigen. Neben jeder aufgelisteten Komponente ist das Symbol „System/Servermodul-Komponentenstatusanzeigen“ zu sehen. gibt an, dass eine Komponente funktionsfähig ist (normal). gibt an, dass eine Komponente sich im Warnzustand (nicht-kritisch) befindet, der sofortige Aufmerksamkeit erfordert. gibt an, dass eine Komponente sich in einem (kritischen) Ausfall-Zustand befindet, der sofortige Aufmerksamkeit erfordert. gibt an, dass der Funktionszustand der Komponente nicht bekannt ist. Die verfügbaren überwachten Komponenten umfassen:
  - Batterien
  - Lüfter
  - Hardware-Protokoll
  - Eingriff
  - Speicher
  - Netzwerk
  - Energieverwaltung
  - Netzteile
  - Prozessoren
  - Temperatures (Temperaturen)
  - Spannungen

  **ANMERKUNG:** Batterien werden nur auf den Dell PowerEdge-Systemen *x9xx* und *xx*0x unterstützt.
  Netzteile sind auf Dell PowerEdge 1900-Systemen nicht verfügbar. Die Energieverwaltung wird nur auf bestimmten Dell PowerEdge *xx*0x-Systemen unterstützt. Die Funktionen für die Netzteil- und die Stromversorgungsüberwachung sind nur auf Systemen verfügbar, die mit mindestens zwei redundanten, im laufenden Betrieb austauschbaren Netzteilen ausgerüstet sind. Diese Funktionen sind für dauerhaft installierte, nicht-redundante Netzteile, die keine Energieverwaltungsschaltung aufweisen, nicht verfügbar.

**ANMERKUNG:** Wenn die QLogic QLE2460 4GB Single-Port Fibre Channel HBA-, QLogic QLE2462 4GB Dual-Port Fibre Channel HBA-, Qlogic QLE2562 Dual Port FC8 Adapter- oder Qlogic QLE2560 Single Port FC8 Adapter-Karten auf yx2x-Systemen installiert sind, wird der Bildschirm „Systemkomponenten (FRU)“ nicht angezeigt.

- Informationen über die Attribute des Hauptsystemgehäuses, wie z.B. den Host-Namen, die iDRAC-Version, Lifecycle Controller-Version, das Gehäuse-Modell, Gehäuseschloss, die Service-Tag-Nummer des Gehäuses, Express-Servicecode und Gehäusesystemkennnummer anzeigen. Das Attribut „Express-Servicecode (ESC)“ ist eine 11-stellige „nur-numerische“ Konvertierung der Service-Tag-Nummer des Dell-Systems. Sie können dieses Attribut in ein Telefon eingeben, während Sie den technischen Support von Dell für Auto-Call-Routing anrufen.
- Detaillierte Informationen über die in Ihrem System eingebauten vor Ort austauschbaren Einheiten (FRUs) anzeigen (im Unterregister **Systemkomponenten (FRU)**).
- Aktivieren oder deaktivieren Sie die Schaltflächen am vorderen Bedienfeld des verwalteten Systems, und zwar den Netzschalter und die Schaltfläche Nicht-maskierbarer Interrupt (NMI) (falls auf dem System vorhanden). Wählen Sie außerdem die Zugriffsebene für die LCD-Sicherheit des verwalteten Systems aus. Die LCD-Informationen des verwalteten Systems stehen im Drop-Down-Menü zur Auswahl zur Verfügung. Sie können auch die Indikation von Remote-KVM-Sitzung über das Unterregister **Vorderes Bedienfeld** aktivieren.

### *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 das System ausgeschaltet wird. Die Batterie speichert die BIOS-Setup-Konfiguration des Systems, wodurch das System effizient neu starten kann. Das Maßnahmenfenster des **Batterien-**Objekts kann die folgenden Register aufweisen, abhängig von den Gruppenberechtigungen des Benutzers: **Eigenschaften** und **Warnungsverwaltung**.

**Eigenschaften**

**Unterregister: Informationen**

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

**Warnungsverwaltung**

Im 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-Speicherchipsatz 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, die serielle Schnittstelle, Netzwerkschnittstellen-Controller-Karten, Festplattenlaufwerkssequenz, benutzerzugängliche USB-Schnittstellen, CPU Virtualization Technology, CPU-Hyperthreading, Netzstromwiederherstellungsmodus, Integrierter SATA-Controller, Konsolenumleitung und Failsafe-BAUD-Rate der Konsolenumleitung. Sie können auch Folgendes konfigurieren: ein internes USB-Gerät, Einstellungen des Controllers des optischen Laufwerks, den Watchdog-Zeitgeber der automatischen Systemwiederherstellung (ASR), einen integrierten Hypervisor sowie zusätzliche LAN-Netzwerkschnittstellen für Hauptplatineninformationen. Sie können außerdem die Einstellungen von TPM (Trusted Platform Module) und TCM (Trusted Cryptographic Module) anzeigen.

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.

Bei yx2x-Systemen werden die konfigurierbaren BIOS-Funktionen in bestimmte Kategorien gruppiert. Hierbei handelt es sich um die folgenden Kategorien: Systeminformationen, Speichereinstellungen, Systemprofileinstellungen, Starteinstellungen für Unified Extensible Firmware Interface (UEFI [Vereinheitlichte erweiterbare Firmware-Schnittstelle]), Netzwerkschnittstellen-Controller-Karten, Einmaliger Start und Einschubdeaktivierung. Wenn Sie beispielsweise auf der Seite **System-BIOS-Einstellungen** auf die Verknüpfung **Speichereinstellungen** klicken, werden die Funktionen angezeigt, die zum Systemspeicher gehören. Sie können die Einstellungen anzeigen und bearbeiten, indem Sie zu den entsprechenden Kategorien navigieren.

Auf der Seite **BIOS-Setup – Systemsicherheit** können Sie ein BIOS-Setup-Kennwort festlegen. Zum Aktivieren und Ändern der BIOS-Einstellungen müssen Sie das Kennwort eingeben. Ansonsten werden die BIOS-Einstellungen im schreibgeschützten Modus angezeigt. Nach der Festlegung des Kennworts müssen Sie das System neu starten.

Wenn offene Werte aus der vorherigen Sitzung vorhanden sind oder die bandinterne Konfiguration durch eine bandexterne Schnittstelle deaktiviert wurde, wird die BIOS-Setup-Konfiguration durch den Server-Administrator nicht genehmigt.

**ANMERKUNG:** Die NIC-Konfigurationsinformationen innerhalb des Server Administrator BIOS-Setups sind für integrierte NICs eventuell ungenau. Das Verwenden des BIOS-Setup-Bildschirms, um NICs zu aktivieren oder zu 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 Register „BIOS-Setup“ 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-Instrumentierungsdienst. Wenn Sie **Lüfter** in der Gerätestruktur wählen, werden Details im Datenbereich im rechten Teil der Server Administrator-Startseite angezeigt. Das Maßnahmenfenster des **Lüfter**-Objekts kann die folgenden Register aufweisen, abhängig von den Gruppenberechtigungen des Benutzers: **Eigenschaften** und **Warnungsverwaltung**.

**Eigenschaften**

**Unterregister: Lüftersonden**

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

- Zeigen Sie die Strommesswerte Ihrer System-Lüftersonden an und geben Sie Minimal- und Maximalwerte für die Lüftersonden-Warnungschwelle ein.

  **ANMERKUNG:** Einige Lüftersondenfelder unterscheiden sich, je nachdem, welche Firmware Ihr System hat: BMC oder ESM. Einige Schwellenwerte können in BMC-Systemen nicht geändert werden.

- Lüftersteuerungsoptionen auswählen.

**Warnungsverwaltung**

**Unterregister: Warnungsmaßnahmen | SNMP-Traps**

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

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

### *Firmware*

Klicken Sie auf das Objekt **Firmware**, um Ihre Systemfirmware 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 Gruppenberechtigungen 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 **Hardware**-Objekts kann, abhängig von den Gruppenberechtigungen des Benutzers, das folgende Register aufweisen: **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 |
|---|---|
| Herabgesetzt | 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 **Eingriff**-Objekts kann, abhängig von den Gruppenberechtigungen des Benutzers, folgende Register aufweisen: **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:

- Die aktuellen Warnungsmaßnahmen-Einstellungen anzeigen und die Warnungsmaßnahmen festlegen, die ausgeführt werden sollen, wenn der Eingriffssensor einen Warnungs- oder Ausfallwert sendet.
- Die derzeitigen SNMP-Trap-Warnungsschwellenwerte anzeigen und die Warnungsschwellenwerte für den Eingriffssensor festlegen. Die ausgewählten Traps werden ausgelöst, wenn das System bei dem ausgewählten Schweregrad ein entsprechendes Ereignis 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-Vorfehlersensoren überwachen die Speichermodule durch Zählen der ECC-Speicherkorrekturen. Server Administrator überwacht auch Speicherredundanzinformationen, falls das betreffende System diese Funktion unterstützt. Das Maßnahmenfenster des **Eingriff**-Objekts kann, abhängig von den Gruppenberechtigungen des Benutzers, das folgende Register aufweisen: **Eigenschaften und Warnungsverwaltung**.

**Eigenschaften**

**Unterregister: Speicher**

Auf der Registerkarte **Eigenschaften** können Sie den Speicherredundanzstatus, die Speicher-Array-Attribute, die Gesamtkapazität der Speicher-Arrays, die Details der Speicher-Arrays, die Speichergerätedetails sowie den Speichergerätestatus abrufen.

**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 muss, prüfen Sie den Protokolleintrag *Wechsel zu Ersatzspeicherbank festgestellt* im ESM-Systemprotokoll, um herauszufinden, welches Speichermodul versagte.

**Warnungsverwaltung**

**Unterregister: Warnungsmaßnahmen | SNMP-Traps**

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

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

### *Netzwerk*

Klicken Sie auf das **Netzwerk-Objekt**, um die NICs des Systems zu verwalten. Der Server Administrator überwacht den Status jeder NIC im System, um eine kontinuierliche Remoteverbindung zu gewährleisten Dell OpenManage Server Administrator erstattet über FCoE- und iSoE-Fähigkeit der NICs Bericht. Des Weiteren wird über NIC-Teamingdetails Bericht erstattet, wenn diese bereits auf dem System konfiguriert wurden. Zwei oder mehrere physische NICs können zu einem einzigen logischen NIC kombiniert werden, dem ein Administrator eine IP-Adresse zuweisen kann. Teaming kann unter Verwendung von NIC-Herstellerhilfsprogrammen konfiguriert werden. Beispiel: Broadcom – BACS. Wenn einer der physischen NICs ausfällt, kann weiterhin auf die IP-Adresse zugegriffen werden, da sie an den logischen NIC und nicht an einen einzigen physischen NIC gebunden ist. Wenn die Teamschnittstelle konfiguriert ist, werden die Teameigenschaften im Detail angezeigt. Die Beziehung zwischen physischen NICs und Teamschnittstellen bzw. umgekehrt wird ebenfalls gemeldet, wenn diese physischen NICs Mitglieder der Teamschnittstelle sind.

Auf einem Windows2008 Hypervisor-Betriebssystem meldet der Server Administrator die IP-Adressen der physikalischen NIC-Schnittstellen, die zur Zuordnung eines IP zu einem virtuellen Computer verwendet werden, nicht.

**ANMERKUNG:** Dass die Reihenfolge, in der Geräte erkannt werden, der physikalischen Anordnung der Ports am Gerät entspricht, ist nicht gewährleistet. Klicken Sie auf den Hyperlink unter der Schnittstellennamen, um die NIC-Informationen abzurufen.

Bei ESX- und ESXi-Betriebssystemen wird das Netzwerkgerät als Gruppe betrachtet. Beispiele: Die virtuelle Ethernet-Schnittstelle, die durch die Dienstkonsole (vswif) verwendet wird und die virtuelle Netzwerkschnittstelle, die durch VMKernel-Geräte (vmknic) auf ESX und das vmknic-Gerät auf ESXi verwendet wird.

Das Maßnahmenfenster des **Netzwerk**-Objekts kann, abhängig von den Gruppenberechtigungen des Benutzers, das folgende Register aufweisen: **Eigenschaften**.

**Eigenschaften**

**Unterregister: Informationen**

Über das Register **Eigenschaften** können Sie Informationen zu den auf dem System installierten physischen NIC-Schnittstellen als auch Teamschnittstellen anzeigen.

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

***Schnittstellen***

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

**Eigenschaften**

**Unterregister: Informationen**

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

***Energieverwaltung***

**ANMERKUNG:** Die Funktionen für die Netzteil- und die Stromversorgungsüberwachung sind nur auf Systemen verfügbar, die mit mindestens zwei redundanten, im laufenden Betrieb austauschbaren Netzteilen ausgerüstet sind. Diese Funktionen sind für dauerhaft installierte, nicht-redundante Netzteile, die keine Energieverwaltungsschaltung aufweisen, nicht verfügbar.

**Überwachung**

**Unterregister: Verbrauch | Statistik**

Im Register „Verbrauch" können Sie die Leistungsaufnahmeinformationen des System in Watt und 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-Toleranzbereich des Systems sowie den Spitzen-Toleranzbereich 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 des Systems 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 Netzteile-Objekt, 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 Netzteil-Objekts kann, abhängig von den Gruppenberechtigungen des Benutzers, folgende Register aufweisen: **Eigenschaften** und **Warnungsverwaltung**.

**ANMERKUNG:** Die Funktionen für die Netzteil- und die Stromversorgungsüberwachung sind nur auf Systemen verfügbar, die mit mindestens zwei redundanten, im laufenden Betrieb austauschbaren Netzteilen ausgerüstet sind. Diese Funktionen sind für dauerhaft installierte, nicht-redundante Netzteile, die keine Energieverwaltungsschaltung aufweisen, nicht verfügbar.

**Eigenschaften**

**Unterregister: Elemente**

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

- Informationen über die Attribute der Netzteilredundanz anzeigen.
- Überprüfen Sie den Status der einzelnen Netzteilkomponenten, einschließlich der Firmware-Version des Netzteils, der Nenn-Eingangswattleistung und der maximalen Ausgangswattleistung. Das Attribut der Nenn-Eingangswattleistung wird nur auf PMBus-Systemen angezeigt, die mit *xx1x* beginnen.

**Warnungsverwaltung**

**Unterregister: Warnungsmaßnahmen | SNMP-Traps**

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

- Die aktuellen Warnungsmaßnahmen-Einstellungen anzeigen und die Warnungsmaßnahmen festlegen, die ausgeführt werden sollen, wenn ein Systemstrom einen Warnungs- oder Ausfallwert sendet.
- Plattformereignis-Warnungsziele für IPv6-Adressen konfigurieren.

- Die derzeitigen SNMP-Trap-Warnungsschwellenwerte anzeigen und die Warnungsschwellenwerte für Systemleistung (Watt) festlegen. Die ausgewählten Traps werden ausgelöst, wenn das System bei dem ausgewählten Schweregrad ein entsprechendes Ereignis erzeugt.

**ANMERKUNG:** Der Trap für den Spitzenstrom des Systems erzeugt nur Ereignisse für die Schweregradstufe „Zur Information".

#### *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 **Prozessor**-Objekts kann die folgenden Register aufweisen, abhängig von den Gruppenberechtigungen des Benutzers: **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**

Im Register **Warnungsverwaltung** können Sie die aktuellen Warnungsmaßnahmen-Einstellungen sehen und die Warnungsmaßnahmen festlegen, die ausgeführt werden sollen, wenn ein Prozessor einen Warnungs- oder Ausfallwert sendet.

#### *Remote-Zugriff*

Klicken Sie auf das Objekt **Remote-Zugriff**, um die BMC-Funktionen Baseboard Management Controller) oder iDRAC-Funktionen (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 nur auf Dell PowerEdge *x9xx*-Systemen und iDRAC nur auf Dell PowerEdge *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.

Mit DRAC können Sie auf die Remote System Management-Fähigkeiten des Systems zugreifen. Der Server Administrator DRAC bietet Remote-Zugriff auf nicht arbeitsfähige Systeme, Warnungsmeldungen, wenn ein System außer Betrieb ist, und die Möglichkeit, ein System neu zu starten.

Das Maßnahmenfenster des **Remote-Zugriff-**Objekts kann, abhängig von den Gruppenberechtigungen des Benutzers, folgende Register aufweisen: **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 **Auf Standardeinstellungen zurücksetzen**, 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.

**ANMERKUNG:** Das Register **Zusätzliche Konfiguration** steht nur auf Systemen mit iDRAC zur Verfügung.

Wenn DRAC konfiguriert ist, können Sie auf der Registerkarte **Konfiguration** Netzwerkeinstellungen konfigurieren.

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

Im Register „Zusätzliche Konfiguration" können Sie IPv4/IPv6-Eigenschaften 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 angezeigt werden.

**ANMERKUNG:** Auf Dell PowerEdge *x9xx*-Systemen:
– Zehn Benutzer-IDs werden angezeigt. Wenn eine DRAC-Karte installiert wird, werden sechzehn Benutzer-IDs angezeigt.
– Die Spalte „Seriell über LAN-Nutzlast" wird angezeigt.

***Wechselbarer Flash-Datenträger***

Klicken Sie auf das Objekt **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 **Eigenschaften**.

**Eigenschaften**

**Unterregister: Informationen**

Im Register **Eigenschaften** können Sie Informationen zu den wechselbaren Flash-Datenträgern und internen SD-Modulen anzeigen. Dies schließt Details zum Konnektornamen, dessen Zustand sowie seiner Speichergröße ein.

**Warnungsverwaltung**

**Unterregister: Warnungsmaßnahmen | SNMP-Traps**

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

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

Interne SD-Module und vFlash nutzen die Warnungsverwaltung gemeinsam. Durch die Konfiguration von Warnungsmaßnahmen/SNMP/PEF für die SD-Module oder für vFlash werden diese automatisch für die jeweils andere Option konfiguriert.

### *Steckplätze*

Klicken Sie auf das Objekt **Steckplätze**, um die Anschlüsse oder Sockel auf der Hauptplatine zu verwalten, die gedruckte Leiterplatinen, wie z. B. Erweiterungskarten, aufnehmen. Das Maßnahmenfenster **Steckplätze**-Objekts enthält das Register **Eigenschaften**.

**Eigenschaften**

**Unterregister: Informationen**

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

### *Temperatures (Temperaturen)*

Klicken Sie auf das Objekt **Temperaturen**, um die Systemtemperatur zu verwalten und 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 hoch sind. Das Maßnahmenfenster des **Lüfter**-Objekts kann die folgenden Register aufweisen, abhängig von den Gruppenberechtigungen des Benutzers: **Eigenschaften** und **Warnungsverwaltung**.

**Eigenschaften**

**Unterregister: Temperatursonden**

Auf der Registerkarte **Eigenschaften** können Sie die Strommesswerte und den Status der Temperatursonden des Systems abrufen und Minimal- und Maximalwerte für den Schwellenwert der Temperatursonden-Warnung angeben.

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

**Warnungsverwaltung**

**Unterregister: Warnungsmaßnahmen | SNMP-Traps**

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

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

**ANMERKUNG:** Sie können minimale und maximale Schwellenwerte der Temperatursonde für ein externes Gehäuse nur in Ganzzahlen angeben. Wenn Sie versuchen, den minimalen oder maximalen Schwellenwert der Temperatursonde auf einen Dezimalwert zu setzen, wird nur die Ganzzahl vor dem Komma als Schwellenwerteinstellung 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 **Spannungen**-Objekts kann die folgenden Register aufweisen, abhängig von den Gruppenberechtigungen des Benutzers: **Eigenschaften** und **Warnungsverwaltung**.

**Eigenschaften**

**Unterregister: Spannungssonden**

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

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

**Warnungsverwaltung**

**Unterregister: Warnungsmaßnahmen | SNMP-Traps**

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

- Die aktuellen Warnungsmaßnahmen-Einstellungen sehen und die Warnungsmaßnahmen festlegen, die ausgeführt werden sollen, wenn ein Systemspannungssensor einen Warnungs- oder Ausfallwert sendet.
- Die derzeitigen SNMP-Trap-Warnungsschwellenwerte anzeigen und die Warnungsschwellenwerte für Spannungssensoren festlegen. Die ausgewählten Traps werden ausgelöst, wenn das System bei dem ausgewählten Schweregrad ein entsprechendes Ereignis 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 **Software**-Objekts kann, abhängig von den Gruppenberechtigungen des Benutzers, das folgende Register aufweisen: **Eigenschaften**.

**Eigenschaften**

**Unterregister: Zusammenfassung**

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

#### *Betriebssystem*

Klicken Sie auf das Objekt **Betriebssystem**, um grundlegende Informationen über das jeweilige Betriebssystem anzuzeigen. Das Maßnahmenfenster des **Betriebssystem**-Objekts kann das folgende Register aufweisen, abhängig von den Gruppenberechtigungen 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-Dienst:

Der Storage Management-Dienst enthält Funktionen für die Konfiguration der Speichergeräte. In den meisten Fällen wird der Storage Management-Dienst unter Verwendung des **typischen Setups** installiert. Der Storage Management-Dienst ist auf den Betriebssystemen Microsoft Windows, Red Hat Enterprise Linux und SUSE Linux Enterprise Server verfügbar.

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

Beim Storage Management-Dienst hat das Maßnahmenfenster des **Speichermedien**-Objekts, je nach Gruppenberechtigungen 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.

Die verfügbaren Konfigurationsoptionen der Einstellungen-Startseite sind:

- 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 **Allgemeine Einstellungen**-Objekts kann die folgenden Register aufweisen, abhängig von den Gruppenberechtigungen des Benutzers: **Benutzer** und **Web Server**.

### Benutzer

**Unterregister: Eigenschaften**

Im Register **Benutzer** können Sie Benutzereinstellungen festlegen z. B. die Startseite-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:

- DSM SA-Verbindungsdiensteinstellungen festlegen. Anweisungen zum Konfigurieren von Servereinstellungen finden Sie unter „Dell Systems Management Server Administration-Verbindungsdienst und Sicherheits-Setup“.
- Konfigurieren Sie die SMTP-Serveradresse und die Bind-IP-Adresse entweder im IPv4- oder IPv6-Adressierungsmodus.

- 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“ auf Seite 70.

## Server Administrator

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

### Einstellungen

**Unterregister: Zugriffskonfiguration | SNMP-Konfiguration**

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

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

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

- 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.

# 5

# Arbeiten mit dem Remote Access Controller

**ANMERKUNG:** Der *Baseboard-Verwaltungs-Controller (BMC)* wird auf den Dell PowerEdge *x9xx*-Systemen unterstützt und der *Integrierte Dell Remote Access Controller (iDRAC)* auf den Dell-Systemen *xx*0x und xx1x.

## Übersicht

Dieses Kapitel bietet Informationen über die Verfügbarkeit und Verwendung der Remote-Zugriffsfunktionen von BMC/iDRAC und DRAC.

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 von Intelligent Platform Management Interfaces (IPMI), sodass Sie Systeme im Remote-Zugriff konfigurieren, überwachen und wiederherstellen können.

Der DRAC ist eine Hardware- und Softwarelösung zur Systemverwaltung und bietet Remote-Verwaltung, Wiederherstellung eines abgestürzten Systems sowie 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 auf Systemen verfügbar, die das Betriebssystem Microsoft Windows ausführen), um Ihnen bei der Diagnose der wahrscheinlichen Ursache eines Systemabsturzes 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 bietet darüber hinaus Warnungsbenachrichtigung, wenn ein System ausgefallen ist, und ermöglicht den Neustart eines Systems im Remote-Zugriff. Darüber hinaus protokolliert der Remote Access Controller die wahrscheinliche Ursache von Systemabstürzen und speichert den *letzten Bildschirm vor dem Absturz*.

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

Bei der Verwendung des Remote Access Controllers können Sie 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 finden Sie im Benutzerhandbuch zu den Dienstprogrammen des *Dell OpenManage Baseboard-Verwaltungs-Controllers*.

**ANMERKUNG:** Weitere Informationen zur Verwendung von DRAC 5 finden Sie im *D*ell 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 |
| `Servermodule` | Modulares System |
| `Hauptsystem` | Modulares System |
| `System` | Nicht-modulares System |
| `Hauptsystemgehäuse` | Nicht-modulares System |

Die *Dell Systems Software Support Matrix*, die unter **support.dell.com** verfügbar ist, bietet weitere Informationen zur Systemunterstützung für Remote-Zugriffsgeräte.

Server Administrator ermöglicht den bandinternen Remote-Zugriff auf Ereignisprotokoll-, Stromsteuerungs- und Sensorstatusdaten und die Konfiguration 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, das eine Unterkomponente der Gruppe **Hauptsystemgehäuse/Hauptsystem** ist.

Sie können folgende Aufgaben ausführen:

- Grundlegende Informationen anzeigen
- Das Remote-Zugriffsgerät auf einer LAN-Verbindung konfigurieren
- Das Remote-Zugriffsgerät auf einer Seriell-über-LAN-Verbindung konfigurieren
- Das Remote-Zugriffsgerät auf einer seriellen Schnittstellenverbindung konfigurieren
- Zusätzliche Eigenschaften des Remote-Zugriffsgeräts konfigurieren
- Benutzer auf dem Remote-Zugriffsgerät konfigurieren
- Plattformereignisfilter-Warnungen einrichten

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

Berichterstattung und Konfiguration von BMC/iDRAC und DRAC können auch mit Hilfe 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 *x*9xx-Systemen anzeigen.

# Anzeigen grundlegender Informationen

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

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

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

Die Seite **Remote-Zugriff** zeigt folgende grundlegende Informationen für den System-BMC an:

**Remote-Zugriffsgerät**

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

**IPv4-Adresse**

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

**IPv6-Adresse**

- IP-Adressen-Quelle
- IPv6-Adresse 1
- Standard-Gateway
- IPv6-Adresse 2
- Lokale Adresse verbinden

- DNS-Adressenquelle
- Bevorzugter DNS-Server
- Alternativer DNS-Server

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

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

So konfigurieren Sie das Remote-Zugriffsgerät für die Kommunikation über eine LAN-Verbindung:

1. Klicken Sie auf das Objekt **Modulares Gehäuse→ System/ Servermodul→ Hauptsystemgehäuse/Hauptsystem→ Remote-Zugriff**.
2. Klicken Sie auf die Registerkarte **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 kombiniert wird.

4. Konfigurieren Sie die folgenden NIC-Konfigurationsdetails:
   - 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.

– NIC-Auswahl

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

**ANMERKUNG:** Die Option NIC-Auswahl ist nur auf Systemen bis Version „yx1x" verfügbar.

– Primär- und Failover-Netzwerkoptionen

  Bei yx2x-Systemen lauten die **Primärnetzwerk**optionen für die Remote Management (iDRAC7)-NIC wie folgt: LOM1, LOM2, LOM3, LOM4 und Dezidiert. Die **Failover-Netzwerk**optionen lautet wie folgt: LOM1, LOM2, LOM3, LOM4, All LOMs und Kein/e.

  Die dedizierte Option ist verfügbar, wenn die iDRAC7-Unternehmenslizenz vorhanden und gültig ist.

**ANMERKUNG:** Die Anzahl der LOMs richtet sich nach der System- und Hardware-Konfiguration.

– IPMI-über-LAN aktivieren

– IP-Adressen-Quelle

– IP-Adresse

– Subnetzmaske

– Gateway-Adresse

– Beschränkung der Kanalberechtigungsebene

– Neuer Verschlüsselungsschlüssel (Diese Option ist auf Dell PowerEdge *x*9*xx*-Systemen verfügbar.)

**5** Konfigurieren Sie die folgenden optionalen VLAN-Konfigurationsdetails:

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

– VLAN-ID aktivieren

– VLAN ID

– Priorität

6 Konfigurieren Sie die folgenden IPv4-Eigenschaften:
   – IP-Adressen-Quelle
   – IP-Adresse
   – Subnetzmaske
   – Gateway-Adresse
7 Konfigurieren Sie die folgenden IPv6-Eigenschaften:
   – IP-Adressen-Quelle
   – IP-Adresse
   – Präfixlänge
   – Standard-Gateway
   – DNS-Adressenquelle
   – Bevorzugter DNS-Server
   – 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 einer seriellen Schnittstellenverbindung

So konfigurieren Sie den BMC für die Kommunikation über eine serielle Schnittstellenverbindung:

1 Klicken Sie auf **Modulares Gehäuse→ System/Servermodul→ Hauptsystemgehäuse/Hauptsystem→ Remote-Zugriff**.
2 Klicken Sie auf die Registerkarte **Konfiguration**.
3 Klicken Sie auf **Serielle Schnittstelle**.
   Das Fenster **Konfiguration der seriellen Schnittstelle** wird angezeigt.
4 Konfigurieren Sie folgende Details:
   – Verbindungsmoduseinstellung
   – Baudrate
   – Flusskontrolle
   – 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 IPMI-Meldungen (Intelligent Plattform Schnittstellenmanagement) über die serielle Schnittstelle unter Verwendung von druckbaren ASCII-Zeichen benutzt. Der Terminalmodus unterstützt auch eine begrenzte Zahl an Textbefehlen für die Unterstützung herkömmlicher textbasierter 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:

- Zeilenbearbeitung
- Löschsteuerung
- Echo-Steuerung
- Handshaking-Steuerung
- Neue Zeilenreihenfolge
- 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

So konfigurieren Sie den BMC/iDRAC für Datenübertragung einer Seriell-über-LAN-Verbindung (SOL):

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

2 Klicken Sie auf die Registerkarte **Konfiguration**.

3 Klicken Sie auf **Seriell über LAN**.

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

4 Konfigurieren Sie folgende Details:
   – Seriell über LAN aktivieren
   – Baudrate
   – 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:
   – Intervall der Zeichenakkumulation
   – 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

So konfigurieren Sie die IPv4- und IPv6-Eigenschaften unter Verwendung der Registerkarte **Zusätzliche Konfiguration**:

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

Weitere Informationen zur Lizenzverwaltung finden Sie im *Dell License Manager-Benutzerhandbuch* unter **support.dell.com**.

# Konfigurieren der Benutzer von Remote-Zugriffsgeräten

So konfigurieren Sie Benutzer von Remote-Zugriffsgeräten über die Seite **Remote-Zugriff**:

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:
   - Zur Aktivierung eines Benutzers wählen Sie **Benutzer aktivieren**.
   - Geben Sie einen Namen für den Benutzer in das Feld **Benutzername** ein.
   - Wählen Sie das Kontrollkästchen **Kennwort ändern** aus.
   - Geben Sie ein neues Kennwort in das Feld **Neues Kennwort** ein.
   - Geben Sie das gleiche Kennwort in das Bestätigungsfeld **Neues Kennwort bestätigen** ein.
5. Legen Sie folgende Benutzerberechtigungen fest:
   - Wählen Sie die maximalen Beschränkungen für LAN-Benutzerberechtigungsebenen aus.
   - Wählen Sie maximal gewährte serielle Schnittstellen-Benutzerberechtigung aus.
   - Wählen Sie auf Dell PowerEdge *x9xx*-Systemen **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 ergibt insgesamt 16 Benutzer. Dieselben Benutzername- und Kennwortregeln gelten für BMC/iDRAC- und RAC-Benutzer. Wenn DRAC/iDRAC6 installiert ist, werden alle 16 Benutzereinträge DRAC zugewiesen.

# Plattformereignisfilter-Warnungen einstellen

So konfigurieren Sie die wichtigsten BMC-Funktionen, darunter die Parameter für Plattformereignisfilter (PEF) und -Warnungsziele, über den Server Administrator-Instrumentierungsdienst:

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 Administratorberechtigungen angemeldet sein, um die BMC-PEF-Warnungen konfigurieren zu können.

**ANMERKUNG:** Mit der Einstellung **Plattformereignisfilter-Warnungen aktivieren** kann das Erzeugen von PEF-Warnungen deaktiviert oder aktiviert werden. Diese Einstellungen sind unabhängig von den einzelnen Plattformereignis-Warnungseinstellungen.

**ANMERKUNG:** **Systemstromsondenwarnungen** und **Systemstromsondenfehler** werden auf Dell PowerEdge-Systemen ohne PMBus-Unterstützung nicht unterstützt, obwohl Server Administrator die Konfiguration zulässt.

**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, wenn das System aufgrund eines Plattformereignisses heruntergefahren werden soll.

5 Wählen Sie eine der folgenden Maßnahmen:

- **Keine**
  Führt keine Aktion durch, wenn das Betriebssystem gesperrt oder abgestürzt ist.
- **System neu starten**
  Fährt das Betriebssystem herunter und leitet einen Systemstart ein, wobei BIOS-Überprüfungen durchgeführt werden und das Betriebssystem neu geladen wird.
- **System aus- und wieder einschalten (Power Cycle)**
  Die Stromversorgung des Systems wird 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.
- **System ausschalten**
  Unterbricht die Stromzufuhr zum System.
- **Stromverminderung**
  Drosselt die CPU.

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

**ANMERKUNG:** Stromverminderung wird nicht auf allen Systemen unterstützt. Die Funktionen für die Netzteil- und die Stromversorgungsüberwachung sind nur auf Systemen verfügbar, die mit mindestens zwei redundanten, im laufenden Betrieb austauschbaren Netzteilen ausgerüstet sind. Diese Funktionen sind für dauerhaft installierte, nicht-redundante Netzteile, die keine Energieverwaltungsschaltung aufweisen, nicht verfügbar.

6 Wählen Sie das Kontrollkästchen **Warnung generieren** für 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 gesendet, 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 Managed Station und einem verwalteten System hin- und hergesendet werden. Die Community-Zeichenkette (auch Community-Name genannt) wird mit jedem Paket mitgesendet, das zwischen der Managed Station und einem verwalteten System übertragen wird.

6 Klicken Sie auf **Änderungen übernehmen**.

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

# 6

# Server Administrator-Protokolle

## Übersicht

Server Administrator ermöglicht die Anzeige und Verwaltung von Hardware-, Warnungs- und Befehlsprotokollen. Alle Benutzer können entweder von der Startseite von Server Administrator oder von dessen 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 zum Erstellen von Berichten über die Befehlszeile finden Sie im *Dell OpenManage Server Administrator-Benutzerhandbuch für die Befehlszeilenschnittstelle* unter **support.dell.com**.

Beim Anzeigen der Server Administrator-Protokolle können Sie 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

- Klicken Sie auf **Drucken**, um eine Kopie des Protokolls auf dem Standarddrucker auszugeben.
- Klicken Sie auf **Exportieren**, um eine Textdatei mit den Protokolldaten (in der die Werte aller Datenfelder durch ein benutzerdefiniertes Begrenzungszeichen getrennt sind) an einem von Ihnen festgelegten Ort zu speichern.

- Klicken Sie auf **E-Mail**, um eine E-Mail-Nachricht zu erstellen, die den Inhalt des Protokolls als Anhang einschließt.
- Klicken Sie auf **Protokoll löschen**, um alle Ereignisse aus dem Protokoll zu löschen.
- Klicken Sie auf **Speichern unter**, um den Protokollinhalt in einer **ZIP**-Datei zu speichern.
- Klicken Sie auf **Aktualisieren**, um den Protokollinhalt wieder in den Datenbereich des Maßnahmenfensters zu laden.

Unter „Task-Schaltflächen“ finden Sie weitere Informationen über die Task-Schaltflächen.

# Server Administrator-Protokolle

Server Administrator enthält die folgenden Protokolle:

- Hardware-Protokoll
- Warnungsprotokoll
- Befehlsprotokoll

## Hardware-Protokoll

Verwenden Sie das Hardware-Protokoll, um nach potenziellen Problemen bei den Hardwarekomponenten des Systems zu suchen. Auf den Dell PowerEdge *x*9xx- *und* xx1x-Systemen wechselt die Hardwareprotokoll-Statusanzeige zum kritischen Status (), wenn die Protokolldatei 100 Prozent der 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 integrierter Anweisungen, die Hardwarestatusmeldungen an 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 eine Aufmerksamkeit 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:

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

#### Unterhalt des Hardwareprotokolls

Das Statusanzeigesymbol neben dem Protokollnamen auf der Server Administator-Startseite wechselt vom normalen Status ( ) zum nicht-kritischen Status ( ), wenn die Protokolldatei 80 Prozent der Kapazität erreicht. Stellen Sie sicher, dass Sie das Hardwareprotokoll löschen, wenn 80 Prozent der Kapazität erreicht sind. Wenn dem Protokoll erlaubt wird, 100 Prozent der Kapazität zu erreichen, werden die letzten Ereignisse vom Protokoll verworfen.

Klicken Sie zum Löschen eines Hardware-Protokolls auf der Seite **Hardware-Protokoll** auf die Verknüpfung **Protokoll löschen**.

### Warnungsprotokoll

**ANMERKUNG:** Falls das Warnungsprotokoll ungültige XML-Daten anzeigt (wenn zum Beispiel die für die Auswahl generierten XML-Daten nicht angemessen formatiert sind), klicken Sie auf **Protokoll löschen** und zeigen Sie die Protokolldaten noch einmal an.

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:

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

**ANMERKUNG:** Der Protokollverlauf wird später u. U. zur Behebung von Fehlern oder für Diagnosezwecke benötigt. Es wird deshalb empfohlen, die Protokolldateien zu speichern.

Weitere Informationen zu Warnmeldungen finden Sie im *Server Administrator-Meldungs-Referenzhandbuch* unter **support.dell.com**.

## Befehlsprotokoll

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

Verwenden Sie das Befehlsprotokoll zur Überwachung aller vom Server Administrator ausgegebenen Befehle. Das Befehlsprotokoll verzeichnet An- und Abmeldungen, Systemverwaltungssoftware-Initialisierungen und ein von der Systemverwaltungssoftware eingeleitetes Herunterfahren und protokolliert den Zeitpunkt, an dem das Protokoll zuletzt gelöscht wurde. Die Größe der Befehlsprotokolldatei kann gemäß 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:

- Das Datum und die Uhrzeit, zu der der Befehl gegeben wurde
- Der Benutzer, der derzeit auf der Server Administrator-Startseite oder der CLI angemeldet ist
- Eine Beschreibung des Befehls und der zugehörigen Werte

**ANMERKUNG:** Der Protokollverlauf wird später u. U. zur Behebung von Fehlern oder für Diagnosezwecke benötigt. Es wird deshalb empfohlen, die Protokolldateien zu speichern.

# 7

# Warnungsmaßnahmen einstellen

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

Wenn Sie Warnungsmaßnahmen für ein Ereignis einstellen, können Sie die Maßnahme Warnung auf dem Server anzeigen **festlegen.** Um diese Maßnahme auszuführen, sendet Server Administrator eine Meldung an **/dev/console**. Wenn auf dem Server Administrator-System ein X Window System ausgeführt wird, wird diese Meldung standardmäßig nicht angezeigt. Um die Warnungsmeldung 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 die Warnungsmeldung 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-Übertragung einer 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 Meldungserlaubnis auf **Ja** eingestellt ist. Wenn auf dem Server Administrator-System ein 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 Server Administrator ausführen kann, gelten Einschränkungen. Folgen Sie diesen Richtlinien, um eine ordnungsgemäße Ausführung zu gewährleisten:

- Geben Sie keine X Window System-basierten Anwendungen an, da Server Administrator solche Anwendungen nicht ordnungsgemäß ausführen kann.
- Geben Sie keine Anwendungen an, bei denen Eingaben durch den Benutzer erforderlich sind, da Server Administrator solche Anwendungen nicht ordnungsgemäß ausführen kann.

- Leiten Sie **stdout** und **stderr** beim Festlegen der Anwendung in eine Datei um, sodass Ausgaben oder Fehlermeldungen angezeigt werden.
- Wenn mehrere Anwendungen (oder Befehle) für eine Warnung ausgeführt werden sollen, erstellen Sie ein Skript, das diese Aufgabe übernimmt, und geben Sie den vollständigen Pfad zum Skript in das 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.

## Warnungsmaßnahmen in Microsoft Windows Server 2003 und Windows Server 2008 einstellen

Beim Festlegen von Warnungsmaßnahmen werden Visual Basic-Skripts nicht automatisch von der Funktion „Anwendung 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 Befehlsprozessor `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, die eine grafische Benutzeroberfläche hat oder Anwendereingaben erfordert) im Feld „Absoluter Pfad zur Anwendung“ ein. Die interaktive Anwendung kann bei einigen Betriebssystemen unerwartete Ergebnisse erzeugen.

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

**ANMERKUNG:** Microsoft Windows 2003 wird auf yx2x-Systemen nicht unterstützt.

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

Aus Sicherheitsgründen ist Windows Server 2008 so konfiguriert, dass keine interaktiven Dienste möglich sind. Wenn ein Dienst als interaktiver Dienst auf 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 zum *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 eine Weise wie der Befehl *pause* in einer Batch-Datei zu einer Eingabe auffordern.

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 sind, 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 zur Ermittlung interaktiver Dienste (Interactive Services Detection) gestartet wurde. Das Register **Prozessse** 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 und interaktive Dienst aktivieren kann.

So erlauben Sie die Interaktion mit dem Desktop:

1. Klicken Sie mit der rechten Maustaste auf den DSM SA-Datenverwaltungsservice im Fenster **Dienstesteuerung**, und wählen Sie **Eigenschaften** aus.
2. Aktivieren Sie auf der Registerkarte **Anmelden** die Option **Interagieren von Service zu Desktop erlauben**, und klicken Sie auf OK.
3. Starten Sie den DSM SA-Datenverwaltungsservice neu, damit die Änderung wirksam wird.
4. Stellen Sie sicher, dass der Dienst **zur Ermittlung interaktiver Dienst** ausgeführt wird.

Wenn der DSM SA-Datenverwaltungsservice mit dieser Änderung neu gestartet wird, generiert der Manager für die Dienstesteuerung die folgende Fehlermeldung im Systemprotokoll:

```
Der DSM SA-DSM SA-Datenverwaltungsservice wird als
interaktiver Dienst gekennzeichnet. Durch die
Aktivierung des Dienstes zur Ermittlung von
interaktiven Diensten kann der DSM SA-
Datenverwaltungsservice interaktive Anwendungen für
eine Warnungsmaßnahme ordnungsgemäß ausführen.
```

Sobald diese Änderungen durchgeführt sind, wird das Dialogfeld **Interaktive Dienste-Dialogerkennung** durch das Betriebssystem angezeigt, um Zugriff auf die interaktive Anwendungsschnittstelle/Eingabeaufforderung zu ermöglichen.

# Warnungsmeldungen der BMC/iDRAC-Plattformereignisfilter

In der folgenden Tabelle werden alle möglichen Meldungen für Plattformereignisfilter mit einer Beschreibung des entsprechenden Ereignisses angezeigt.

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

| Ereignis | Beschreibung |
|---|---|
| Lüftersondenfehler | Der Lüfter läuft zu langsam oder überhaupt nicht. |
| Spannungssondenfehler | Die Spannung reicht für einen ordnungsgemäßen Betrieb nicht aus. |
| Batteriesondenwarnung | Die Batterie läuft derzeit unterhalb des empfohlenen Ladezustands. |
| Batteriesondenfehler | Die Batterie ist ausgefallen. |
| Diskreter Spannungssondenfehler | Die Spannung reicht für einen ordnungsgemäßen Betrieb nicht aus. |
| Temperatursondenwarnung | Die Temperatur nähert sich dem oberen bzw. unteren Grenzwert. |
| 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. |
| Prozessor nicht vorhanden | Ein Prozessor wurde entfernt. |
| PS/VRM/D2D Warnung | Das Netzteil, das Spannungsreglermodul oder der DC/DC-Konverter steht vor einem Ausfall. |
| PS/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. |

**Tabelle 7-1. PEF-Warnungsereignisse *(fortgesetzt)***

| Ereignis | Beschreibung |
|---|---|
| Systemstromsondenwarnung | Die Leistungsaufnahme nähert sich dem Fehlerschwellenwert. |
| Systemstromsondenfehler | Die Leistungsaufnahme hat die höchstzulässige Stufe überschritten, was zu einem Fehler führte. |
| Wechselbarer Flash Medien nicht vorhanden | Der wechselbare Flash-Datenträger wurde entfernt. |
| Wechselbarer Flash Datenträgerfehler | Für den wechselbaren Flash-Datenträger steht ein Fehlerzustand an. |
| Wechselbarer Flash Datenträgerwarnung | Für den wechselbaren Flash-Datenträger steht ein Fehlerzustand an. |
| Kritisch für interne zweifache SD-Modulkarte | Die interne zweifache SD-Modulkarte ist ausgefallen. |
| Warnung für interne zweifache SD-Modulkarte | Für die interne zweifache SD-Modulkarte steht ein Fehlerzustand an. |
| Redundanzverlust für interne zweifache SD-Modulkarte | Die interne zweifache SD-Modulkarte verfügt nicht über Redundanz. |
| Fehlen einer internen zweifachen SD-Modulkarte | Die interne zweifache SD-Modulkarte wurde entfernt. |

# A

# Fehlerbehebung

## Verbindungsdienstfehler

Auf Red Hat Enterprise Linux startet der DSM-SA-Verbindungsdienst (Dell Systems Management Server Administrator) nicht, wenn `SELinux` auf den Modus `Erzwungen` eingestellt ist. Führen einen der folgenden Schritte aus, und starten Sie die diesen Dienst:

- Stellen Sie `SELinux` auf den Modus `Deaktiviert` oder den Modus `Zulassen` ein.
- Ändern Sie die SELinux-Eigenschaft **allow_execstack** zum Zustand **EIN**. Führen Sie den folgenden Befehl aus:

  ```
  setsebool allow_execstack on
  ```

- Ändern Sie den Sicherheitskontext für den DSM-SA-Verbindungsdienst. Führen Sie den folgenden Befehl aus:

  ```
  chcon -t unconfined_execmem_t
  /opt/dell/srvadmin/sbin/dsm_om_connsvcd
  ```

## Anmeldefehler-Szenarien

Eine Anmeldung beim Managed System kann in folgenden Situationen fehlschlagen:

- Eingabe einer ungültigen/falschen IP-Adresse.
- Eingabe falscher Anmeldeinformationen (Benutzername und Kennwort).
- Das Managed System ist AUSgeschaltet.
- Das Managed System ist aufgrund einer ungültigen IP-Adresse oder eines DNS-Fehlers nicht erreichbar.
- Das Managed System weist ein nicht vertrauenswürdiges Zertifikat auf und Sie wählen auf der Anmeldeseite nicht **Zertifikatswarnung ignorieren** aus.

- Die Server Administrator-Dienste sind auf dem VMware ESX/ESXi-System nicht aktiviert. Im *Installationshandbuch zu Dell OpenManage Server Administrator* unter **support.dell.com/manuals** finden Sie Informationen darüber, wie Server Administrator-Dienste auf dem VMware ESX/ESXi-System aktiviert werden.
- Der SFCBD-Dienst (small footprint CIM broker daemon) des VMware ESX/ESXi-Systems wird nicht ausgeführt.
- Der Web Server-Verwaltungsdienst auf dem verwalteten System wird nicht ausgeführt.
- Wenn Sie das Kontrollkästchen **Zertifikatswarnung ignorieren** nicht aktivieren, geben Sie die IP-Adresse des verwalteten Systems und nicht den Host-Namen ein.
- Die WinRM-Berechtigungsfunktion (Remoteaktivierung) ist auf dem verwalteten System nicht konfiguriert. Informationen zu dieser Funktion finden Sie im *Dell OpenManage Server Administrator Installation Guide* (Dell OpenManage Server Administrator-Installationshandbuch) unter **support.dell.com/manuals**.
- Beim Versuch, eine Verbindung zu einem VMware ESXi 4.1/5.0-Betriebssystem herzustellen, tritt ein Authentifizierungsfehler auf, was sich möglicherweise auf einen der folgenden Gründe zurückführen lässt:
  - Der `Sperr`modus ist aktiviert, während Sie beim Server oder bei Server Administrator angemeldet sind. Weitere Informationen zum `Sperr`modus finden Sie in der VMware-Dokumentation.
  - Das Kennwort wird geändert, während Sie bei Server Administrator angemeldet sind.
  - Sie melden sich bei Server Administrator als normaler Benutzer ohne Administratorrechte an. Weitere Informationen zum Zuweisen der Rolle finden Sie in der VMware-Dokumentation.

# Beheben 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. Prüfen Sie, welche Version von Server Administrator zuvor installiert war.
2. Laden Sie das Installationspaket für diese Version unter **support.dell.com** herunter.
3. Machen Sie **SysMgmt.msi** im Verzeichnis **srvadmin\windows\SystemsManagement** 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 Standardverzeichnis installiert haben, stellen Sie sicher, dass die Änderung auch in **Benutzerdefiniertes Setup** durchgeführt wird.

6. Sobald die Anwendung installiert ist, können Sie Server Administrator unter Verwendung von **Programme hinzufügen/entfernen** deinstallieren.

# OpenManage Server Administrator-Dienste

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

**Tabelle A-1. OpenManage Server Administrator-Dienste**

| Dienstname | Beschreibung | Fehlerwirkung | Wieder-herstellungs-mechanismus | Schweregrad |
|---|---|---|---|---|
| Windows: DSM SA-Verbindungsdienst<br>Linux: dsm_om_connsvc<br>(Dieser Dienst wird mit dem Server Administrator Web Server installiert.) | Bietet Remote-/lokalen Zugriff auf Server Administrator von beliebigen Systemen mit einem unterstützten Webbrowser und einer unterstützten Netzwerk-verbindung aus. | Benutzer können sich nicht bei Server Administrator anmelden, und keine Vorgänge über die Web-Benutzeroberfläche ausführen. CLI kann jedoch nach wie vor verwendet werden. | Dienst neu starten | Kritisch |

**Tabelle A-1. OpenManage Server Administrator-Dienste *(fortgesetzt)***

| Dienstname | Beschreibung | Fehlerwirkung | Wieder-herstellungs-mechanismus | Schweregrad |
|---|---|---|---|---|
| | | Allgemeiner Dienst | | |
| Windows: DSM SA-Dienste freigegeben<br>Linux: dsm_om_shrsvc<br>(Dieser Dienst wird auf dem Managed System ausgeführt.) | Legt beim Start eine Bestands-aufnahme der Systemsoftware an, über die SNMP- und CIM-Anbieter von Server Administrator eine Remote-Software-aktualisierung mithilfe der Dell System Management Console und des Dell IT Assistant (ITA) durchführen. | Software-aktualisierungen sind unter Verwendung des ITA nicht möglich. Jedoch können die Aktualisierungen lokal und außerhalb von Server Administrator mithilfe einzelner Dell Update-Pakete durchgeführt werden. Aktualisierungen können weiterhin über Drittanbieter-Tools (darunter MSSMS, Altiris und Novell ZENworks) vollzogen werden. | Dienst neu starten | Warnung |

**ANMERKUNG:** Wenn die 32-Bit-Kompatibilitätsbibliotheken nicht auf einem 64-Bit-Linux-System installiert sind, können die Freigabedienste den Bestandsaufnahmensammler nicht starten und zeigen die folgende Fehlermeldung an: `libstdc++.so.5 ist zum Ausführen des Bestandsaufnahmensammlers erforderlich.` srvadmin-cm.rpm bietet die Binärdateien für den Bestandsaufnahmensammler. Eine Liste der Geschwindigkeiten, nach denen srvadmin-cm sich richtet, finden Sie im *Dell OpenManage Server Administrator Installation Guide* (Dell OpenManage Server Administrator-Installationshandbuch) unter **support.dell.com/manuals**.

**Tabelle A-1. OpenManage Server Administrator-Dienste *(fortgesetzt)***

| Dienstname | Beschreibung | Fehlerwirkung | Wieder-herstellungs-mechanismus | Schweregrad |
|---|---|---|---|---|
| | | **Instrumentierungsdienst** | | |
| DSM SA-Datenmanager<br>Linux: dsm_sa_datamgrd<br>(im Dienst dataeng gehostet)<br>(Dieser Dienst wird auf dem Managed System ausgeführt.) | Überwacht das System, bietet schnellen Zugriff auf detaillierte Fehler- und Leistungs-informationen und erlaubt Remote-verwaltung überwachter Systeme, einschließlich Herunterfahren, Start und Sicherheit. | Wenn diese Dienste nicht ausgeführt werden, sind Benutzer nicht in der Lage, die Details der Hardware-Ebene auf der GUI/CLI zu konfigurieren/ anzuzeigen. | Dienst neu starten | Kritisch |
| DSM SA-Ereignismanager<br>Linux: dsm_sa_eventmgrd<br>(im Dienst dataeng gehostet)<br>(Dieser Dienst wird auf dem Managed System ausgeführt.) | Bietet einen Dienst zur Ereignis-protokollierung von Betriebssystemen und Dateien für die System verwaltung und wird auch von Ereignisprotokoll analysatoren verwendet. | Wenn dieser Dienst angehalten wird, werden die Funktionen der Ereignis-protokollierung nicht einwandfrei funktionieren. | Dienst neu starten | Warnung |

**Tabelle A-1. OpenManage Server Administrator-Dienste *(fortgesetzt)***

| Dienstname | Beschreibung | Fehlerwirkung | Wieder-herstellungs-mechanismus | Schweregrad |
|---|---|---|---|---|
| Linux: dsm_sa_snmpd<br>(im Dienst dataeng gehostet)<br>(Dieser Dienst wird auf dem Managed System ausgeführt.) | Data Engine-SNMP-Schnittstellte von Linux | SNMP Get/Set/Trap-Anforderung funktioniert nicht über eine Management Station. | Dienst neu starten | Kritisch |
| **Storage Management-Dienst** | | | | |
| Windows: mr2kserv (Dieser Dienst wird auf dem Managed System ausgeführt.) | Der Speicher verwaltungsdienst gibt Auskunft über die Speicher verwaltung und erweiterte Funktionen zur Konfiguration eines lokalen oder entfernten Speichers, der mit einem System verbunden ist. | Benutzer sind nicht in der Lage, Speicherfunktionen für alle unterstützten RAID- und Nicht-RAID-Controller auszuführen. | Dienst neu starten | Kritisch |

# B

# Häufig gestellte Fragen

In diesem Abschnitt sind die häufig gestellten Fragen zu Dell OpenManage Server Administrator aufgeführt:

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

1 **Warum scheitert die Host-Neustartfunktion für ESXi 4.x (4.0 U3) und ESXi 5.x unter OpenManage Server Administrator?**

Dieses Problem taucht auf Grund des VMware Stand-Alone License (SAL)-Schlüssels auf. Weitere Informationen finden Sie im Knowledge Base-Artikel unter **kb.vmware.com/kb/1026060**.

2 **Welche Aufgaben müssen ausgeführt werden, nachdem ein VMware ESX 4.0 U3- und ESX 4.1 U2-Betriebssystem zur Active Directory-Domäne hinzugefügt wurde?**

Nach dem Hinzufügen eines VMware ESX 4.0 U3- und ESX 4.1 U2-Betriebssystems zur Active Directory-Domäne muss ein Active Directory-Benutzer die folgenden Schritte ausführen:

- Melden Sie sich während der Verwendung des VMware ESX 4.1- und des ESX 4.1 U2-Betriebssystems als Server-Administrator bei Server Administrator an, und starten Sie den DSM-SA-Verbindungsdienst neu.
- Melden Sie sich als Remote Enablement Agent beim Remote-Knoten an, während Sie das VMware ESX 4.0 U3- oder das ESX 4.1 U2-Betriebssystem verwenden. Warten Sie ungefähr 5 Minuten, bis der sfcbd-Ablauf die Berechtigung für den neuen Benutzer hinzugefügt hat.

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

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

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

Bei Systemen mit Server Administrator in Version 4.3 müssen Sie eine Aktualisierung auf eine 6.x -Version und anschließend auf eine 7.x-Version durchführen. Bei Systemen mit einer Version unterhalb von Version 4.3 müssen Sie zunächst eine Aktualisierung auf Version 4.3, dann auf eine 6.x-Version und dann auf eine 7.x-Version durchführen. Das x steht hier für die Version von Server Administrator, auf die Sie aktualisieren möchten).

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

Melden Sie sich an: **support.dell.com→ Enterprise IT→ Manuals→ Software→ Systems Management→ Dell OpenManage Server Administrator**

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

**6 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 **Eigenschaften→ Zusammenfassung**. Die auf Ihrem System installierte Version von Server Administrator wird in der Spalte **Systemverwaltung** angezeigt.

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

Ja, Sie können Ihre bevorzugte https-Schnittstelle einstellen. Navigieren Sie zu **Einstellungen→ Allgemeine Einstellungen→ Web Server→ HTTPS-Schnittstelle**

Wählen Sie statt **Standardeinstellung verwenden** die Option **Optionsschaltfläche verwenden, um bevorzugte Schnittstelle festzulegen** aus.

**ANMERKUNG:** Die Änderung der Schnittstellennummer auf eine ungültige bzw. eine bereits belegte Schnittstellennummer kann andere Anwendungen oder Browser beim Zugriff auf Server Administrator auf dem verwalteten System beeinträchtigen. Eine Liste der Standardschnittstellen finden Sie im *Dell OpenManage-Installations- und Sicherheitsbenutzerhandbuch* unter **support.dell.com/manuals**.

**8 Kann ich Server Administrator auf Fedora, College Linux, Mint, Ubuntu, Sabayon oder PClinux installieren?**

Nein, Server Administrator unterstützt keines dieser Betriebssysteme.

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

Nein, Server Administrator ist nicht dafür ausgelegt, bei Problemen E-Mails zu senden.

**10 Ist SNMP für die ITA-Ermittlung, die Bestandsaufnahme und Softwareaktualisierungen 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 sicheres FTP vorgenommen. Für diese diskrete Maßnahme sind Berechtigungen/Anmeldeinformationen auf Stammebene erforderlich, die dann eingegeben werden müssen, wenn die Maßnahme eingerichtet bzw. angefordert wird. Anmeldeinformationen des Ermittlungsbereichs werden nicht vorausgesetzt.

ITA-*Kommunikation mit Windows-Systemen:*

Für Server (Systeme, die Windows Server-Betriebssysteme ausführen) kann das System entweder mit SNMP oder mit CIM oder mit beiden Protokollen 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 Speicherort (möglicherweise eine andere Netzwerkfreigabe) auf das Zielsystem kopiert. Daraufhin werden WMI-Funktionen aufgerufen, um die Softwareaktualisierung auszuführen.

Auf 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 (in erster Linie ermittelten) Gerät.

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.

**11 Gibt es Pläne für SNMP-v3-Unterstützung?**

Nein, es gibt keine Pläne für SNMP v3-Unterstützung.

**12 Verursacht ein Unterstreichungszeichen im Domänennamen Probleme bei der Anmeldung bei Server Admin?**

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

**13 Welchen Einfluss hat das Markieren/Aufheben der Markierung von 'Active Directory' auf der Anmeldungsseite von Server Administrator auf Berechtigungsebenen?**

Wenn Sie das Kontrollkästchen „Active Directory“ nicht markieren, haben Sie nur den Zugriff, der im Microsoft Active Directory konfiguriert ist. Sie können sich nicht unter Verwendung der erweiterten Schemalösung von Dell 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* unter support.dell.com/manuals.

**14 Welche Maßnahmen muss treffen, während ich eine Kerberos-Authentifizierung ausführe und eine Anmeldung über den Web Server versuche?**

Für Authentifizierungen müssen die Inhalte der Dateien **/etc/pam.d/openwsman** und **/etc/pam.d/sfcb** auf dem verwalteten Knoten durch Folgendes ersetzt werden:

Für 32-Bit:

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

Für 64-Bit:

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

# Stichwortverzeichnis

## T



## U



## V

## W



## Z