Dell™ OpenManage™ Server Administrator: Benutzerhandbuch Version 5.2

Notizen und Hinweise

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

HINWEIS: Ein HINWEIS warnt vor möglichen Beschädigungen der Hardware oder Datenverlust und zeigt, wie diese vermieden werden können.

Dezember 2006

Zurück zum Inhaltsverzeichnis

Fehlerbehebung

Dell™ OpenManage™ Server Administrator: Benutzerhandbuch Version 5.2

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

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

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

ANMERKUNG: Auf einem SUSE Linux Enterprise Server (Version 9) werden Meldungen, die von **wall** gesendet werden vom **xterm**-Terminalprogramm angezeigt aber nicht vom **Konsole**- Terminalprogramm.

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** bei der Angabe 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 setzen Sie den vollständigen Pfad zum Skript im Feld **Absoluter Pfad zur Anwendung** ein.

  Beispiel 1:

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

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

  Beispiel 2:

  ```
  mail -s "Serverwarnung" 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.

BMC-Plattformereignisfilter Warnungsmeldungen

Ein Liste aller möglichen Plattformereignisfilter-/(PEF-)Meldungen und die Beschreibung des jeweiligen Ereignisses finden Sie in Tabelle 11-1.

Tabelle 11-1. BMC-PEF-Warnungsereignisse

Ereignis	Beschreibung
Lüftersondenfehler	Der Lüfter läuft zu langsam oder gar nicht.
Spannungssondenfehler	Die Spannung reicht für einen ordnungsgemäßen Betrieb nicht aus.
Diskreter Spannungssondenfehler	Die Spannung reicht für einen ordnungsgemäßen Betrieb nicht aus.
Temperatursondenwarnung	Die Temperatur geht auf den oberen bzw. unteren Grenzwert zu.
Temperatursondenfehler	Die Temperatur ist für einen ordnungsgemäßen Betrieb zu hoch oder zu niedrig.
Gehäuseeingriff festgestellt	Das Systemgehäuse wurde geöffnet.
Redundanz (Netzteil oder Lüfter) herabgesetzt	Redundanz der Lüfter bzw. Netzteile wurde herabgesetzt.

Redundanz (Netzteil oder Lüfter) verloren	Keine Redundanz mehr für die Lüfter bzw. Netzteile des Systems vorhanden.
Prozessorwarnung	Ein Prozessor läuft unter seiner Spitzenleistung bzw. Taktrate.
Prozessor-Fehler	Ein Prozessor ist fehlerhaft.
PPS/VRM/DCtoDC-Warnung	Das Netzteil, das Spannungsreglermodul oder DC/DC-Konverter steht vor einem Ausfall.
Netzteil/VRM/D2D-Fehler	Netzteil, 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.

Service-Namen verstehen

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

Tabelle 11-2. Service-Namen

Zweck	Service-Name	Vorhergehende Version	Aktuelle Version
Web-Server			
	Anzeigename	Secure Port-Server	DSM SA-Verbindungsdienst
	Name der ausführbaren Datei	Omaws [32|64]	dsm_om_connsvc [32|64]
			dsm_om_connsvc
Planen oder Benachrichtigung			
	Anzeigename	OM Common Services	DSM SA Freigegebene Services
	Name der ausführbaren Datei	Omsad [32|64]	dsm_om_shrsvc[32|64]
			dsm_om_shrsvc

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

Sie können eine fehlerhafte Installation reparieren, indem Sie eine Neuinstallation erzwingen und eine Deinstallation von Server Administrator ausführen.

So erzwingt man eine Neuinstallation:

1. Finden Sie heraus, welche Version von Server Administrator vorher installiert wurde
2. Laden Sie das Installationspaket für diese Version von der Dell™ Support-Website unter **support.dell.com** herunter
3. Machen Sie **SysMgmt.msi** vom 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 wählen Sie alle Funktionen, die ursprünglich installiert wurden. Wenn Sie nicht sicher sind, welche Funktionen installiert wurden, wählen Sie alle Funktionen aus und führen Sie die Installation aus.

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

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

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Glossar

Dell™ OpenManage™ Server Administrator: Benutzerhandbuch Version 5.2

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

A

Abkürzung für Ampere.

AC

Abkürzung für Alternating Current (Wechselstrom).

ACL

Abkürzung für Access Control List (Zugangskontrollliste). Bei ACL-Dateien handelt es sich um Textdateien mit Listen, in denen festgelegt wird, wer Zugang zu auf einem Novell® Web Server gespeicherten Ressourcen erhält.

Adapterkarte

Eine Erweiterungskarte, die in den Erweiterungskartensteckplatz auf der Systemplatine des Systems gesteckt wird. Eine Adapterkarte erweitert das System um Spezialfunktionen, indem sie eine Schnittstelle zwischen dem Erweiterungsbus und einem Peripheriegerät bereitstellt. Beispiele für Adapterkarten sind Netzwerkkarten, Sound-Karten und SCSI-Adapter.

ADB

Abkürzung für Assign Database (Datenbank zuweisen).

AGP

Abkürzung für Advanced Graphics Port (Erweiterte Graphikschnittstelle).

Anbieter

Ein Anbieter ist eine Erweiterung eines CIM-Schemas, das mit verwalteten Objekten kommuniziert und auf Daten und Ereignisbenachrichtigungen von einer Anzahl von Quellen zugreift. Anbieter senden diese Informationen an den CIM-Objektmanager zur Integration und Interpretation.

ASCII

Akronym für American Standard Code for Information Interchange (Amerikanischer Standardcode für Informationsaustausch). Eine Textdatei, die nur Zeichen aus der ASCII-Zeichensatztabelle enthält (normalerweise mit einem Texteditor, wie z. B. dem Programm Notepad in Microsoft® Windows®, erstellt), wird als ASCII-Datei bezeichnet.

ASIC

Akronym für Application-Specific Integrated Circuit (Anwendungsspezifische integrierte Schaltung).

ASPI

Akronym für Advanced SCSI Programming Interface (Erweiterte SCSI-Programmierschnittstelle).

Attribut

Ein Attribut oder eine Eigenschaft enthält eine bestimmte Information über eine verwaltbare Komponente. Attribute können zu Gruppen zusammengefügt werden. Handelt es sich um ein Lese-Schreib-Attribut, kann es durch ein Verwaltungsprogramm definiert werden.

Authentisierung

Der Server Administrator Remote Access Controller besitzt zwei Methoden um Benutzerzugriff zu authentifizieren:

RAC-Authentifizierung und Authentifizierung des lokalen Betriebssystems. RAC-Authentifizierung ist immer aktiviert. Administratoren können spezifische Benutzerkonten und Kennwörter aufstellen, die Zugriff auf den RAC zulassen.

Betriebssysteme erfordern auch, dass Administratoren verschiedene Stufen von Benutzern und Benutzerkonten definieren; jede Benutzerebene hat verschiedene Berechtigungen. Die Authentifizierung des lokalen Betriebssystems auf dem RAC ist eine Option für Administratoren, die nicht einen Satz von Berechtigungen für Benutzer im Betriebssystem und einen anderen Satz von Benutzern und Konten für den RAC definieren wollen. Wenn Sie die Authentifizierung des lokalen Betriebssystems für den RAC aktivieren, berechtigen Sie jeden Benutzer mit Administratorstatus auf dem Betriebssyst m sich bei RAC anzumelden.

autoexec.bat-Datei

Die **autoexec.bat**-Datei wird ausgeführt, wenn das System gestartet wird (nach der Ausführung jeglicher Befehle in der **config.sys**-Datei). Diese Startdatei enthält Befehle, die die Merkmale der einzelnen am System angeschlossenen Geräte definieren und führt Programme aus, die nicht im aktiven Verzeichnis gespeichert sind.

Baudrate

Maß für Datenübertragungsgeschwindigkeit. Ein Modem überträgt Daten beispielsweise mit einer oder mehreren festgelegten Baudraten über den COM-Anschluss (die serielle Schnittstelle) des Systems.

Bedienungsfeld

Der Teil des Systems, der die Anzeigen und Bedienelemente enthält; wie z. B. den Netzschalter, die Festplattenlaufwerkzugriffsanzeige und die Betriebsanzeige.

BGA

Abkürzung für Ball Grid Array (Ballnetz-Array), eine integrierte Schaltung (IC), die ein Array von Lötkugeln anstelle von Stiften zum Anschluss an eine Systemplatine verwendet.

Bildschirmadapter

Siehe Videoadapter.

Bildwiederholfrequenz

Die Frequenz, mit der der Bildschirm das Videobild auf dem Monitorbildschirm neu zeichnet. Genauer gesagt ist die Bildwiederholfrequenz die in Hz gemessene Frequenz, mit der die horizontalen Bildschirmzeilen neu aufgeladen werden (manchmal auch als Vertikalfrequenz bezeichnet). Je höher die Bildwiederholfrequenz, desto weniger Bildflimmern kann vom menschlichen Auge wahrgenommen werden. Die höheren Bildwiederholfrequenzen werden auch zeilensprungfrei ausgeführt.

Binär

Ein Zahlensystem, das die Ziffern 0 und 1 zur Wiedergabe von Informationen verwendet. Das System führt Vorgänge basierend auf der Anordnung und Berechnung dieser zwei Ziffern durch.

BIOS

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

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

Bit

Die kleinste Informationseinheit, die vom System verarbeitet wird.

BMC

Abkürzung für Baseboard-Verwaltungs-Controller, der Controller in dem die Intelligenz des IPMI sitzt.

bpi

Abkürzung für Bits per Inch (Bit pro Zoll).

bps

Abkürzung für Bits per Second (Bit pro Sekunde).

BTU

Abkürzung für British Thermal Unit (Britische Wärmemengeneinheit).

Bus

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

Byte

Ein Byte besteht aus acht zusammenhängenden Bits, der kleinsten Einheit, mit der das System arbeitet.

C

Abkürzung für Celsius.

CA

Abkürzung für Certification Authority (Zertifizierungsstelle).

Cache

Ein schneller Speicherbereich, der eine Kopie von Daten oder Anleitungen enthält, um die Zugriffszeiten auf Daten zu verkürzen. So könnte z. B. das BIOS des Systems den ROM-Code in einem schnelleren RAM-Speicher ablegen. Oder ein Festplatten-Cache-Dienstprogramm könnte RAM-Speicher reservieren, in dem häufig benutzte Informationen der Festplatte des Systems abgelegt werden. Wenn ein Programm Daten von einem Festplattenlaufwerk anfordert, die sich auch im Cache befinden, kann das Festplatten-Cache-Dienstprogramm die Daten aus dem RAM schneller aufrufen als vom Festplattenlaufwerk.

CDRAM

Abkürzung für Cache-DRAM, ein von Mitsubishi entwickelter Hochgeschwindigkeits-DRAM-Speicherchip, der einen kleinen SRAM-Cache enthält.

CD-ROM

Abkürzung für Compact Disc Read-Only Memory (CD mit Nur-Lese-Speicher). CD-Laufwerke verwenden optische Technologie um Daten von CDs zu lesen. CDs sind Nur-Lese-Speichergeräte; mit Standard-CD-Laufwerken können keine neuen Daten auf einer CD gespeichert werden.

CHAP

Akronym für Challenge-Handshake Authentication Protocol, ein Authentisierungsprotokoll, das von PPP-Servern verwendet wird, um die Identität des Einleiters einer Verbindung bei deren Erstellung oder zu einem beliebigen späteren Zeitpunkt zu bestätigen.

Chip

Ein Satz von mikroskopisch kleinen elektronischen Schaltkreisen, die zur Verwendung als Prozessoren und als Speicher in Systemen ausgelegt sind. Kleine Chips können zwischen einer Handvoll und Zehntausenden von Transistoren enthalten. Sie sehen wie kleine Aluminiumchips aus und haben eine Fläche von maximal 15 mm2 und eine Dicke von 0,8 mm, woher auch der Name "Chip" kommt. Große Chips mit einer Fläche von über 1,3 cm2 enthalten Millionen Transistoren. Die Schaltkreise befinden sich in Wirklichkeit nur in den oberen 2-hundertstel Millimetern der Chipoberfläche. Der Rest des Chips dient nur als Basis.

CI/O

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

CIM

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

CIMOM

Akronym für Common Information Model Object Manager (Objektmanager für allgemeines Informationsmodell).

CLI

Abkürzung für Command Line Interface (Befehlszeilenschnittstelle.)

cm

Abkürzung für Zentimeter.

CMOS

Akronym für Complimentary Metal-Oxide Semiconductor (Komplementär-Metalloxidhalbleiter). In Systemen werden CMOS-Speicherchips häufig zur NVRAM-Speicherung eingesetzt.

COM*n*

Die Gerätenamen für die erste bis zur vierten seriellen Schnittstelle auf dem System sind COM1, COM2, COM3 und COM4. Der Standard-Interrupt für COM1 und COM3 ist IRQ4, der Standard-Interrupt für COM2 und COM4 ist IRQ3. Daher müssen Sie vorsichtig vorgehen, wenn Sie Software konfigurieren, die ein serielles Gerät steuert, damit Sie keinen Interrupt-Konflikt hervorrufen.

config.sys-Datei

Die **config.sys**-Datei wird ausgeführt, wenn das System gestartet wird (vor der Ausführung etwaiger Befehle in der **autoexec.bat**-Datei). Diese Startdatei enthält Befehle, die festlegen, welche Geräte zu installieren und welche Treiber zu verwenden sind. Weitere Befehle der Datei legen fest, wie das Betriebssystem den Speicher verwendet und Dateien verwaltet.

ConsoleOne

Novell ConsoleOne ist eine Java-basierte Grundlage für Graphikdienstprogramme, die Netzwerkressourcen von verschiedenen Standorten und Plattformen managen und verwalten. ConsoleOne enthält einen einzelnen Steuerungspunkt für alle Novell- und externen Produkte.

Controller

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

COO

Abkürzung für Cost of Ownership (Betriebskosten).

Coprozessor

Ein Chip, der dem Mikroprozessor des Systems bestimmte Verarbeitungsaufgaben abnimmt. Ein mathematischer Coprozessor erledigt z. B. die Arithmetikprozesse. Ein graphischer Coprozessor unterstützt die Videoausgabe. Der Intel® Pentium®-Mikroprozessor z. B. besitzt einen integrierten mathematischen Coprozessor.

cpi

Abkürzung für Characters per Inch (Zeichen pro Zoll).

CPU

Abkürzung für Central Processing Unit (Zentrale Verarbeitungseinheit). Siehe auch Mikroprozessor.

CRC

Abkürzung für Cyclic Redundancy Code (Zyklischer Redundanzcode), eine Zahl, die zur Feststellung von Schäden von einem Datenblock errechnet und mit diesem gespeichert und übertragen wird. Durch Neuberechnung des CRC und Vergleich mit dem ursprünglich übertragenen Wert kann der Empfänger einige Arten von Übertragungsfehlern feststellen.

CSR

Abkürzung für Certificate Signing Request (Zertifikatsignierungsanforderung).

Cursor

Ein Markierungszeichen, z. B. ein Block, ein Unterstreichungszeichen oder ein Zeiger, der die Position angibt, an der die nächste Tastatur- oder Mausmaßnahme vorgenommen wird.

DAT

Akronym für Digital Audio Tape (Digitalaudioband).

dB

Abkürzung für Dezibel.

dBA

Abkürzung für angepasste Dezibel.

DBS

Abkürzung für bedarfsbezogene Schalter. DBS ist eine Stromverwaltung, die zu einem niedrigeren Stomzustand schaltet (Frequeny und Spannung), wenn die Prozessornutzung niedrig ist. Sie erhält die Anwendungsleistung während der durchschnittliche Systemstrom abgesenkt wird.

DC

Abkürzung für Direct Current (Gleichstrom).

Auch eine Abkürzung für Dual Channel (Zweikanal).

DHCP

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

Dienstprogramm

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

Dienstprogramm-Partition

Eine startfähige Partition auf der Festplatte, die Dienstprogramme und Diagnosen für Hard- und Software enthält. Wenn sie aktiviert wird, startet die Partition und stellt eine ausführbare Umgebung für die Dienstprogramme auf der Partition bereit.

DIMM

Akronym für Dual In-Line Memory Module [Speichermodul mit zwei Kontaktanschlussreihen] Eine kleine Platine, die DRAM-Chips enthält und an die Systemplatine angeschlossen ist.

DIN

Akronym für Deutsche Industrie-Norm, die Organisation, die in Deutschland für die Bestimmung von Normen verantwortlich ist. Ein DIN-Anschluss ist ein Stecker, der einer der vielen von DIN definierten Normen entspricht. DIN-Anschlüsse werden häufig in Personalcomputern verwendet. Zum Beispiel ist der Tastaturanschluss für Personalcomputer ein DIN-Anschluss.

DIP

Akronym für Dual In-Line Package (Chips mit zwei Kontaktanschlussreihen). Auf einer Platine (z. B. einer Systemplatine oder Erweiterungskarte) können sich DIP-Schalter befinden, die zum Konfigurieren der Platine dienen. DIP-Schalter sind immer Kippschalter mit einer EIN- und einer AUS-Position.

DKS

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

DMA

Abkürzung für Direct Memory Access (Direkter Speicherzugriff). Ein DMA-Kanal erlaubt bestimmte Datenübertragungen zwischen RAM und einem Gerät, ohne den Mikroprozessor zu adressieren.

DMTF

Abkürzung für Distributed Management Task Force (Dezentrale Verwaltungs-Taskforce), ein Firmenkonsortium, das aus Hardware- und Softwareherstellern besteht.

dpi

Abkürzung für Dots per Inch (Punkte pro Zoll).

DPMS

Abkürzung für Display Power Management Signaling (Anzeigenstromverwaltungssignale). Ein Standard, der von der Video Electronics Standards Association (VESA®) entwickelt wurde und Hardwaresignale definiert, die vom Video-Controller gesendet werden, um in einem Monitor die verschiedenen Stromverwaltungszustände zu aktivieren. Ein Monitor wird als DPMS-kompatibel bezeichnet, wenn er nach Empfang des entsprechenden Signals vom Video-Controller des Systems in den jeweiligen Energiesparzustand wechselt.

DRAC 4

Akronym für Dell™ Remote Access Controller.

DRAC 5

Akronym für Dell Remote Access Controller.

DRAC II

Akronym für Dell OpenManage™ Remote Assistant Card II.

DRAC III

Akronym für Dell Remote Access Card III (Dell Remote-Zugriffskarte III).

DRAC III/XT

Akronym für Dell Remote Access Card III/XT (Dell Remote-Zugriff-Karte III/XT).

DRAM

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

DSM SA-Verbindungsdienst

Akronym für Dell Systems Management Server Administration. Eine Anwendung, mit der Webseiten mit Hilfe von Web-Browsern unter Verwendung des HTTPS-Protokolls angezeigt werden können. Siehe Web-Server.

DTE

Abkürzung für Data Terminal Equipment (Datenterminalausrüstung). Jedes Gerät (z. B. ein Computersystem), das Daten in digitaler Form über ein Kabel oder eine Kommunikationsleitung senden kann. Das DTE ist über eine Datenkommunikationsausrüstung (DCE), z. B. ein Modem, an das Kabel oder die Kommunikationsleitung angeschlossen.

E/A

Abkürzung für Eingabe/Ausgabe. Die Tastatur ist ein Eingabegerät und der Drucker ist ein Ausgabegerät. Im allgemeinen kann man zwischen E/A-Aktivitäten und Rechneraktivitäten unterschieden. Beispiel: Wenn ein Programm ein Dokument zu einem Drucker sendet, unternimmt es eine Ausgabeaktivität; wenn das Programm eine Liste mit Begriffen sortiert, unternimmt es eine Rechneraktivität.

ECC

Abkürzung für Error Checking and Correction (Fehlerkorrekturcode).

ECP

Abkürzung für Extended Capabilities Port (Anschluss mit erweiterter Funktionalität).

EDO

Akronym für Extended Data Output Dynamic Random Access Memory (Dynamischer Speicher mit wahlfreiem Zugriff mit erweitertem Datenausgang), ein schnellerer DRAM als der herkömmliche DRAM. EDO-RAM kann mit dem Abruf des nächsten Speicherblocks beginnen, während er noch den vorherigen Block an den Mikroprozessor sendet.

EEPROM

Akronym für Electrically Erasable Programmable Read-Only Memory (Elektrisch lösch- und programmierbarer, Nur-Lese-Speicher).

EIDE

Abkürzung für Enhanced Integrated Drive Electronics (Erweiterte integrierte Laufwerkelektronik). EIDE-Geräte zeichnen sich gegenüber traditionellen IDE-Geräten durch ein oder mehrere der folgenden zusätzlichen Merkmale aus:

- Datentransferraten von bis zu 16 MB/Sek
- Unterstützung sowohl von Festplattenlaufwerken als auch anderen Laufwerken, z. B. CD- oder Bandlaufwerken
- Unterstützung von Festplattenlaufwerken mit einer Kapazität von mehr als 528 MB
- Unterstützung von bis zu zwei Controllern, an denen maximal je zwei Geräte angeschlossen sind.

Einstellungen

Einstellungen sind Bedingungen eines verwaltbaren Objekts, die bei der Bestimmung helfen, wie vorzugehen ist, wenn ein bestimmter Wert in einer Komponente festgestellt wird. So kann beispielsweise ein Benutzer die kritische Obergrenze einer Temperatursonde auf 75 Grad Celsius einstellen. Wenn die Sonde diese Temperatur erreicht, wird durch die Einstellung das Senden einer Warnungsnachricht an die Verwaltungskonsole veranlasst, so dass der Benutzer eingreifen kann. Einige Einstellungen können, wenn sie erreicht werden, das System herunterfahren oder eine andere Reaktion auslösen, die Schäden am System verhindern können.

EISA

Akronym für Extended Industry-Standard Architecture (Erweiterte Industriestandardarchitektur), ein 32-Bit-Erweiterungsbus-Design. Die Erweiterungskartensteckplätze in einem EISA-System sind mit 8- und 16-Bit- ISA-Erweiterungskarten kompatibel.

Um beim Einbau einer EISA-Erweiterungskarte einen Konfigurationskonflikt zu vermeiden, muss das EISA-Konfigurationsprogramm aufgerufen werden. Über dieses Dienstprogramm können Sie angeben, in welchem Erweiterungssteckplatz sich die Karte befindet; außerdem erhält es Informationen über die erforderlichen Systemressourcen der Karte von einer entsprechenden EISA-Konfigurationsdatei.

EMI

Abkürzung für Electromagnetic Interference (Elektromagnetische Interferenz).

EMM

Abkürzung für Expanded Memory Manager (Expansionsspeicher-Manager). Ein Dienstprogramm, das Erweiterungsspeicher verwendet, um auf Systemen mit einem Intel386™ oder schnelleren Mikroprozessor einen Expansionsspeicher zu emulieren.

EMS

Abkürzung für Expanded Memory Specification (Spezifikationen für den Expansionsspeicher).

EMV

Abkürzung für Elektromagnetische Verträglichkeit.

EPP

Abkürzung für Enhanced Parallel Port (Erweiterte parallele Schnittstelle), die verbesserte bidirektionale Datenübertragung leistet. Viele Geräte sind auf die Nutzung des EPP-Standards ausgelegt, insbesondere Geräte, z. B. Netzwerk- oder SCSI-Adapter, die an die parallele Schnittstelle eines portablen Computers angeschlossen werden.

EPROM

Akronym für Erasable Programmable Read-Only Memory (Lösch- und programmierbarer, Nur-Lese-Speicher).

ERA

Abkürzung für Embedded Remote Access (Eingebetteter Fernzugriff).

ERA/MC

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

ERA/O

Abkürzung für Embedded Remote Access/Option (Integrierte Remote-Zugriff-Option).

Erweiterungsbus

Das System besitzt einen Erweiterungsbus, über den der Mikroprozessor direkt mit den Controllern der Peripheriegeräte (z. B. einer Netzwerkkarte oder einem internen Modem) Daten austauschen kann.

Erweiterungskartensteckplatz

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

Erweiterungsspeicher

RAM oberhalb der 1 MB-Grenze. Die meisten Softwareprogramme, die diesen Speicher benutzen können (z. B. das Windows-Betriebssystem), erfordern, dass

sich ein Erweiterungsspeicher unter der Kontrolle eines XMM befindet.

ESD

Abkürzung für Electrostatic Discharge (Elektrostatische Entladung).

ESM

Abkürzung für Embedded Systems Management (Integrierte Systemverwaltung).

Expansionsspeicher

Ein Verfahren, um den RAM oberhalb von 1 MB zu adressieren. Der Expansionsspeicher auf dem System kann nur mit Hilfe eines EMM genutzt werden. Sie sollten das System nur dann für einen Expansionsspeicher konfigurieren, wenn Sie Anwendungsprogramme ausführen werden, die Expansionsspeicher benutzen können (oder erfordern).

Externer Cache-Speicher

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

F

Abkürzung für Fahrenheit.

Fähigkeit

Bezieht sich auf die Vorgänge, die ein Objekt ausführen kann, oder Maßnahmen, die an einem verwalteten Objekt durchgeführt werden können. Wenn eine Platine z. B. hot-plug-fähig ist, kann sie ersetzt werden, während das System eingeschaltet ist.

FAT

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

- **FAT** - Ein von MS-DOS, Windows 3.*x* , Windows 95 und Windows 98 verwendetes Dateisystem. Windows NT® und Windows 2000 können ebenfalls das FAT-Dateisystem verwenden. Das Betriebssystem verwaltet eine Tabelle zur Beobachtung des Status verschiedener Segmente der Festplatte, die zum Speichern von Dateien verwendet werden.
- **FAT32** - Abgeleitet vom FAT-Dateisystem. FAT32 unterstützt kleinere Cluster-Formate als FAT und sorgt dadurch für effizientere Kapazitätsausnutzung auf FAT32-Laufwerken.

FCC

Abkürzung für Federal Communications Commission, die amerikanische Bundesbehörde für das Kommunikationswesen.

FEPROM

Akronym für Flash Erasable Programmable Read-Only Memory (Flash-lösch- und programmierbarer, Nur-Lese-Speicher). Ein Flash-Speicher ist eine Art nicht-flüchtiges Speichergerät, einem EEPROM ähnlich; das Löschen jedoch wird blockweise oder für den gesamten Chip durchgeführt.

Fibre Channel

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

Firmware

Software (Programme oder Daten), die in den Nur-Lese-Speicher (ROM) geschrieben wurde. Firmware kann ein Gerät starten und betreiben. Jeder Controller enthält Firmware, die hilft, die Funktionalität des Controllers bereit zu stellen.

Flash-BIOS

Ein BIOS, das im Flash-Speicher anstatt im ROM gespeichert wird. Ein Flash-BIOS-Chip kann am Einbauort aktualisiert werden, ein ROM BIOS muss jedoch durch einen neueren Chip ersetzt werden.

Flash-Speicher

Eine Art von EEPROM-Chip, der mittels eines auf Diskette befindlichen Dienstprogramms neu programmiert werden kann, während er im System installiert ist. Die meisten EEPROM-Chips können nur mit Hilfe spezieller Programmiergeräte neu beschrieben werden.

Formatieren

Der Vorgang, mit dem eine Festplatte oder Diskette auf die Dateienspeicherung vorbereitet wird. Ein uneingeschränkter Formatierungsbefehl löscht alle Daten vom Datenträger.

FPBGA

Abkürzung für Field Programmable Gate Array (Feldprogrammierbares Gate-Array), ein Programmierbarer Logikchip (PLD) mit einer hohen Gate-Dichte.

FRU

Abkürzung für Field Replaceable Unit (Austauschbare Funktionseinheit).

ft

Abkürzung für das Längenmaß Fuß

FTP

Abkürzung für File Transfer Protocol (Dateiübertragungsprotokoll).

g

Abkürzung für Gramm.

G

Abkürzung für Gravität.

GB

Abkürzung für Gigabyte. Ein Gigabyte entspricht 1 024 Megabyte oder 1 073 741 824 Byte.

gcc

Abkürzung für gnu-C-Compiler.

Gerätetreiber

Ein Programm, mit dem das Betriebssystem oder ein anderes Programm mit einem Peripheriegerät, wie z. B. einem Drucker, korrekt kommunizieren kann. Einige Geräteteiber - z. B. Netzwerktreiber - müssen von der config.sys-Datei (mit einer device=Anweisung) oder als speicherresidente Programme (gewöhnlich von der autoexec.bat-Datei) geladen werden. Andere, z. B. Videotreiber, müssen jeweils bei Aufruf des Programms, für das sie entwickelt wurden, geladen werden.

Graphik-Coprozessor

Siehe Coprozessor.

Graphikmodus

Ein Videomodus, der durch x horizontale mal y vertikale Pixel mal z Farben definiert werden kann.

Grenzwerte

Systeme werden gewöhnlich mit verschiedenen Sensoren ausgestattet, die Temperatur, Spannung, Strom und Lüftergeschwindigkeit überwachen. Die Schwellenwerte der Sensoren legen die Bereiche (Mindest- und Höchstwerte) fest, um zu bestimmen, ob der Sensor unter normalen, nichtkritischen, kritischen oder gefährlichen Bedingungen arbeitet. Server Administrator-unterstützte Schwellenwerte sind

- UpperThresholdFatal (Oberer Schwellenwert - Gefahr)
- UpperThresholdCritical (Oberer Schwellenwert - kritisch)
- UpperThresholdNoncritical
- Normal
- LowerThresholdNoncritical
- LowerThresholdCritical (Unterer Schwellenwert - kritisch)
- LowerThresholdFatal (Unterer Schwellenwert - Gefahr)

GUI

Akronym für Graphical User Interface (Graphische Benutzeroberfläche).

h

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

HBA

Abkürzung für Host Bus Adapter (Host-Bus-Adapter). Eine PCI-Adapterkarte im System, deren einzige Funktion es ist, Datenbefehle vom PCI-Busformat in das Speicherverbindungsformat umzuwandeln (Beispiele: SCSI, Fibre Channel) und direkt mit Festplattenlaufwerken, Bandlaufwerken, CD-Laufwerken oder anderen Speichergeräten zu kommunizieren.

HMA

Abkürzung für High Memory Area (Hoher Speicherbereich). Die ersten 64 KB des Erweiterungsspeichers oberhalb von 1 MB. Eine XMS-gestützte Speicherverwaltung kann HMA als direkte Erweiterung des konventionellen Speichers ausweisen. Siehe auch XMM.

Host-Adapter

Ein Host-Adapter implementiert die Kommunikation zwischen dem Bus des Systems und dem Controller eines Peripheriegerätes. (Festplatten-Controller-Subsysteme umfassen eine integrierte Host-Adapterschaltung.) Um einen SCSI-Erweiterungsbus im System hinzuzufügen, muss der entsprechende Host-Adapter installiert oder angeschlossen werden.

Hot-plug-fähig

Die Fähigkeit, ein redundantes Teil bei laufendem System aus- und einzubauen. Auch "Ersatzgerät" genannt.

HPFS

Abkürzung für die High Performance File System (Hochleistungs-Dateisystem)-Option des Betriebssystems Windows NT.

http

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

HTTPS

Abkürzung für Hypertext Transmission Protocol, Secure (Sicheres Hypertextübertragungsprotokoll). HTTPS ist eine Variation von HTTP, das von Web-Browsern zur Abwicklung gesicherter Transaktionen verwendet wird. HTTPS ist ein einzigartiges Protokoll, das eigentlich von SSL unterlegtes HTTP ist. Sie müssen "https://" für HTTP-URLs mit SSL verwenden, jedoch weiterhin "http://" für HTTP-URLs ohne SSL verwenden.

Hz

Abkürzung für Hertz.

ICES

Abkürzung für Interference Causing Equipment Standard (in Canada) (Schnittstellenverursachender Gerätestandard, in Kanada).

ICMP

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

ICU

Abkürzung für ISA Configuration Utility (ISA-Konfigurationsdienstprogramm)

ID

Abkürzung für Identifikation (Kennung).

IDE

Abkürzung für Integrated Drive Electronics (Integrierte Laufwerkelektronik). IDE ist eine Computersystemschnittstelle, die hauptsächlich für Festplattenlaufwerke und CDs verwendet wird.

IHV

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

Infodatei

Eine Textdatei, die mit einem Softwarepaket oder einem Hardwareprodukt ausgeliefert wird und ergänzende oder aktualisierende Informationen zur Dokumentation der Soft- bzw. Hardware enthält. Lies-mich-Dateien erklären die Installation der Software, beschreiben neue Produktverbesserungen oder Korrekturen, die noch nicht in der Dokumentation erfasst sind, und weisen auf Probleme und andere Dinge hin, die beim Einsatz der Software oder Hardware zu beachten sind.

Interlacing

Ein Verfahren zur Erhöhung der Bildschirmauflösung, indem die horizontalen Zeilen nur abwechselnd aufgefrischt werden. Da Interlacing zu sichtbarem Bildschirmflimmern führen kann, bevorzugen die meisten Benutzer zeilensprungfreie Bildschirmauflösungen.

Interner Mikroprozessor-Cache

Ein Instruktions- und Daten-Cache, der im Mikroprozessor realisiert ist. Der Intel Pentium-Mikroprozessor z. B. besitzt einen internen 16-KB-Cache, der als 8-KB-Nur-Lese-Instruktions-Cache und als 8-KB-Lese-Schreib-Daten-Cache arbeitet.

IP-Adresse

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

IPMI

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

IPX

Abkürzung für Internetwork Packet Exchange (Internetzwerk-Paketaustausch).

IRQ

Abkürzung für Interrupt Request (Unterbrechungsaufforderung). Dieses Signal gibt an, dass Daten an ein Peripheriegerät auszugeben oder von ihm zu empfangen sind und über eine IRQ-Leitung zum Mikroprozessor geleitet werden. Jeder Peripherieverbindung muss eine separate IRQ-Nummer zugewiesen werden. Beispiel: Die erste serielle Schnittstelle des Systems (COM1) ist standardmäßig IRQ4 zugewiesen. Zwei Geräte können sich die gleiche IRQ-Zuweisung teilen, dann aber nicht gleichzeitig verwendet werden.

ISA

Akronym für Industry-Standard Architecture (Industriestandardarchitektur). Eine 16-Bit-Erweiterungsbus-Architektur. Die Erweiterungskartensteckplätze in einem ISA-System sind auch mit 8-Bit-ISA-Erweiterungskarten kompatibel.

ISV

Abkürzung für Independent Software Vendor (Unabhängiger Softwareanbieter).

ITE

Abkürzung für Information Technology Equipment (Informationstechnologiegeräte).

Java

Eine plattformübergreifende Programmiersprache, die von Sun Microsystems entwickelt wurde.

JSSE

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

Jumper

Jumper sind kleine Blöcke auf einer Platine mit zwei oder mehr herausragenden Stiften. Jumper-Stecker aus Plastik mit eingeschweißtem Draht passen auf diese Stifte. Der Draht verbindet die Stifte und stellt einen Schaltkreis her. Jumper sind eine einfache Methode, den Schaltkreis auf einer Platine temporär zu ändern.

K

Abkürzung für kilo- (gibt 1000 an).

Kb

Abkürzung für Kilobyte, 1024 Byte.

KB/Sek

Abkürzung für Kilobyte pro Sekunde.

Kbit(s)

Abkürzung für Kilobit, 1024 Bit.

Kbit(s)/s

Abkürzung für Kilobit pro Sekunde.

Kerberos

Ein Netzwerk-Authentifizierungsprotokoll. Es ist dafür vorgesehen, eine starke Authentifizierung für Client/Server-Anwendungen dadurch anzubieten, dass geheime Schlüsselkryptographie verwendet wird.

kg

Abkürzung für Kilogramm, 1000 Gramm.

kHz

Abkürzung für Kilohertz, 1000 Hertz.

Konventioneller Speicher

Die ersten 640 KByte des RAM. Alle Systeme enthalten einen konventionellen Speicher. Falls sie nicht speziell dafür entworfen wurden, sind die MS-DOS®-Programme auf den konventionellen Speicherbereich beschränkt.

Kühlkörper

Eine Metallplatte mit Stiften oder Rippen, die der Wärmeableitung dient. Die meisten Mikroprozessoren besitzen integrierte Kühlkörper.

Kühlung

Batterien von Lüftern oder anderen Kühlvorrichtungen in einem Systemgehäuse.

LAN

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

Laufwerktypennummer

Das System kann eine Anzahl bestimmter Festplattenlaufwerke identifizieren. Jedes trägt eine Laufwerktypennummer, die im NVRAM abgespeichert ist. Die im System-Setup-Programm angegebenen Festplattenlaufwerke müssen mit den im System installierten Festplatten übereinstimmen. Über das System-Setup-Programm können außerdem für die Festplatten, die nicht in der Tabelle der in NVRAM gespeicherten Laufwerktypen angeführt sind, physikalische Parameter (logische Zylinder, logische Köpfe, Zylinderanzahl und logische Sektoren pro Paket) angegeben werden.

lb

Abkürzung für amerikanische Pfund.

LCC

Englische Abkürzung für Chipträger mit oder ohne Anschlüsse.

LDAP

Das Akronym für Lightweight Directory Access Protocol. Ein Netzwerkprotokoll, um Verzeichnisdienste, die über TCP-IP ausgeführt werden, abzufragen und zu modifizieren.

LED

Abkürzung für Light-Emitting Diode (Leuchtdiode). Ein elektronisches Gerät, das aufleuchtet, wenn es Strom empfängt.

LIF

Akronym für Low Insertion Force (Niedrige Einsatzkraft). Einige Systeme besitzen LIF-Sockel und Anschlüsse, mit denen Bauteile wie der Mikroprozessor mit minimaler Kraftaufwendung ein- und ausgebaut werden können.

Local Bus

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

LPT*n*

Die Gerätebezeichnungen für die erste bis einschließlich dritte Druckerschnittstelle des Systems sind LPT1, LPT2 und LPT3.

LRA

Abkürzung für Local Response Agent (Lokaler Antwortagent).

m

Abkürzung für Meter.

mA

Abkürzung für Milliampere.

mAh

Abkürzung für Milliamperestunde.

Mathematischer Coprozessor

Siehe Coprozessor.

Maus

Ein Zeigegerät, das die Cursor-Bewegungen auf dem Bildschirm steuert. Mit mausorientierter Software können Sie Befehle aufrufen, indem Sie den Zeiger auf das dargestellte Objekt bewegen und eine Maustaste klicken.

MB

Abkürzung für Megabit.

MB

Abkürzung für Megabyte. Der Begriff Megabyte steht für 1 048 576 Bytes. Im Zusammenhang mit der Speicherkapazität einer Festplatte wird der Begriff jedoch häufig abgerundet und steht dann generell für 1 000 000 Bytes.

MB/Sek

Abkürzung für Megabytes per Second (Megabytes pro Sekunde).

Mbps

Abkürzung für Megabits per Second (Megabits pro Sekunde).

MBR

Abkürzung für Master Boot Record (Master-Startverzeichnis).

MCA

Abkürzung für Micro Channel Architecture (Mikrokanalarchitektur), die auf Multiprozessoren ausgelegt ist. MCA verhindert eventuelle Konflikte, die bei der Installation neuer Peripheriegeräte entstehen können. MCA ist nicht kompatibel mit EISA- bzw. XT-Busarchitektur, weswegen ältere Karten nicht damit verwendet werden können.

MHz

Abkürzung für Megahertz.

MIB

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

MIDI

Akronym für Musical Instrument Digital Interface (Digitale Musikinstrumenten-Schnittstelle).

Mikroprozessor

Der primäre Rechnerchip im Innern des Systems, der die Auswertung und Ausführung von arithmetischen und logischen Funktionen steuert. Eine für einen bestimmten Mikroprozessor geschriebene Software muss normalerweise revidiert werden, damit sie sich auch für einen anderen Mikroprozessor eignet. CPU ist ein Synonym für Mikroprozessor.

mm

Abkürzung für Millimeter.

Modem

Ein Gerät, das die Kommunikation des Systems mit anderen Systemen über eine Telefonleitung ermöglicht.

modulares System

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

MOF

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

MPEG

Akronym für Motion Picture Experts Group (Filmexpertengruppe). MPEG ist ein digitales Videodateienformat.

ms

Abkürzung für Millisekunde.

MS-DOS

Akronym für Microsoft Disk Operating System (Microsoft-Festplattenbetriebssystem).

MTBF

Abkürzung für Mean Time Between Failures (Durchschnittszeit zwischen Ausfällen).

Multifrequenzmonitor

Ein Monitor, der mehrere Videostandards unterstützt. Er kann sich auf den Frequenzbereich des Signals verschiedener Videoadapter einstellen.

mV

Abkürzung für Millivolt.

Name

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

NDIS

Abkürzung für Network Driver Interface Specification (Netzwerktreiber-Schnittstellenspezifikation).

Netzstromschalter

Ein Schalter mit zwei Wechselstromeingängen, der für Wechselstromredundanz sorgt, indem er auf einen Bereitschafts-Wechselstromeingang umschaltet, wenn der primäre Wechselstromeingang ausfällt.

Netzteil

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

NIC

Akronym für Network Interface Controller (Netzwerkschnittstellen-Controller).

NIF

Akronym für Network Interface Function (Netzwerkschnittstellen-Funktion). Dieser Ausdruck entspricht dem Akronym NIC.

NIS

Abkürzung für das Netzwerkinformationssystem. NIS ist ein Netzwerknamensgebungs- und Verwaltungssystem für kleinere Netzwerke. Benutzer an beliebigen Hosts können Zugriff auf Dateien oder Anwendungen auf beliebigen Hosts im Netzwerk mit einer Einzelbenutzer-Identifizierung und -Kennwort erhalten.

NMI

Abkürzung für Nonmaskable Interrupt (Nichtmaskierbare Unterbrechung). Ein Gerät gibt ein NMI an den Mikroprozessor aus, um Hardwarefehler (z. B. Paritätsfehler) anzuzeigen.

Non-Interlaced

Ein Verfahren, um Bildschirmflimmern durch sequenzielles Auffrischen jeder horizontalen Zeile zu vermindern.

ns

Abkürzung für Nanosekunde, ein Milliardstel einer Sekunde.

NTFS

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

NTLM

Abkürzung für Windows NT LAN Manager. NTLM ist das Sicherheitsprotokoll für das Windows NT-Betriebssystem.

NuBus

Proprietärer Erweiterungsbus, der in Apple Macintosh-Personalcomputern verwendet wird.

Nur-Lese-Datei

Eine Nur-Lese-Datei kann weder bearbeitet noch gelöscht werden. Eine Datei kann unter folgenden Bedingungen Nur-Lese-Status haben:

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

NVRAM

Akronym für Nonvolatile Random-Access Memory (Nicht-flüchtiger Speicher mit wahlfreiem Zugriff). Dabei handelt es sich um einen Speicher, dessen Inhalt beim Abschalten des Systems nicht verloren geht. NVRAM wird benutzt, um das Datum, die Uhrzeit und die Systemkonfigurationsdaten zu speichern.

oberer Speicherbereich

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

OID

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

Online-Zugangsdienst

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

OTP

Abkürzung für One-Time Programmable (Einmal programmierbar).

PAM

Akronym für Pluggable Authentication Modules (Steckbare Authentisierungsmodule). PAM ermöglicht es System-Administratoren, eine Authentisierungsregelung zu erstellen, ohne Authentisierungsprogramme neu kompilieren zu müssen.

Parallele Schnittstelle

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

Parameter

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

Partition

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

PCI

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

PC-Karte

Ein kreditkartengroßes, herausnehmbares Modul für portable Computer, standardisiert durch PCMCIA. PC-Karten werden auch "PCMCIA-Karten" genannt. PC-Karten sind 16-Bit- Geräte zum Anschließen von Modems, Netzwerkadaptern, Sound-Karten, Funkempfängern, Festkörperplatten und Festplattenlaufwerken an einen portablen Computer. Die PC-Karte ist ein "Plug-and-Play"-Gerät, das automatisch von der Kartendienst-Software konfiguriert wird.

PCMCIA

Personal Computer Memory Card International Association (Internationale Vereinigung für Personalcomputer-Speicherkarten). Eine internationale Industrie-Vereinigung, die Normen für Geräte wie Modems und externe Festplattenlaufwerke entwickelt hat, die an portable Computer angeschlossen werden können.

PERC

Akronym für Dell PowerEdge™ Expandable RAID Controller (Erweiterbarer RAID-Controller).

Peripheriegerät

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

PGA

Abkürzung für Pin Grid Array (Stiftnetz-Array), eine Art Mikroprozessorsockel, der das Entnehmen des Mikroprozessors ermöglicht.

Physikalischer Speicher-Array

Der physikalische Speicher-Array umfasst den gesamten physikalischen Speicher eines Systems. Variablen für den physikalischen Speicher sind Höchstumfang, Gesamtanzahl an Speichersteckplätzen auf der Hauptplatine und Gesamtanzahl der belegten Steckplätze.

PIC

Akronym für Programmable Interrupt Controller (Programmierbarer Interrupt-Controller).

PIP

Akronym für Peripheral Interchange Program (Peripherie-Austauschprogramm).

Pixel

Ein einzelner Punkt auf einem Bildschirm. Pixel sind in Zeilen und Spalten angeordnet und erzeugen so ein Bild. Bildschirmauflösungen (z. B. 640 x 480) werden durch Anzahl der horizontalen und vertikalen Pixel ausgedrückt.

PKCS #7

Abkürzung für Public Key Cryptography Standard #7 (Öffentlicher Schlüssel-Kryptographiestandard Nr. 7). PKCS #7 ist ein Standard von RSA Data Security, Inc. zum Einkapseln signierter Daten wie z. B. einer Zertifikatskette.

PKIS

Abkürzung für Novell Public Key Infrastructure Services (Öffentlicher Novell Schlüssel-Infrastrukturdienst).

PLCC

Abkürzung für Kunststoff-Chipträger mit Anschlüssen.

Plug-and-Play

Ein Industriestandard, mit dem Hardware-Geräte leichter an Personalcomputer angeschlossen werden können. Plug-and-Play bietet automatische Installation und Konfiguration, Kompatibilität mit bereits vorhandener Hardware, sowie dynamische Unterstützung mobiler Computerumgebungen.

PME

Abkürzung für Power Management Event (Stromverwaltungsereignis). Ein PME ist ein Stift auf einer Verbindung peripherer Geräte, der es einem PCI- Gerät ermöglicht, ein Aktivierungsereignis zu bestätigen.

POST

Akronym für Power-On Self-Test (Einschalt-Selbsttest). Nach dem Einschalten des Systems wird zunächst ein POST durchgeführt, der Systemkomponenten wie RAM, Laufwerke und Tastatur testet, bevor das Betriebssystem geladen werden kann.

ppm

Abkürzung für Pages Per Minute (Seiten pro Minute).

PPP

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

PQFP

Abkürzung für Plastic Quad Flat Pack, eine Art Mikroprozessorsockel, in den der Mikroprozessor-Chip permanent eingebaut ist.

Programmdiskettensatz

Der Diskettensatz, mit dem die vollständige Installation eines Betriebssystems oder eines Anwendungsprogramms durchgeführt werden kann. Wenn ein Programm neu konfiguriert wird, ist oft der Programmdiskettensatz erforderlich.

PS

Abkürzung für Stromversorgung.

PS/2

Abkürzung für Personal System/2.

PXE

Abkürzung für Pre-Boot eXecution Environment (Pre-Boot Ausführungsumgebung).

QFP

Abkürzung für Quad Flat Pack.

RAC

Akronym für Remote Access Controller.

RAID

Akronym für Redundant Array of Independent Disks (Redundantes Array unabhängiger Festplatten).

RAM

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

RAMDAC

Akronym für Random-Access Memory Digital-to-analog Converter (Zufallszugriffspeicher Digital-Analog-Wandler).

RAW

Nicht verarbeitet. Der Ausdruck bezieht sich auf Daten, die ohne Interpretation an ein E/A-Gerät weitergeleitet werden. Im Gegensatz dazu bezieht sich "bearbeitet" auf Daten, die vor der Weiterleitung an das E/A-Gerät verarbeitet werden. Gemeint ist oft unkomprimierter Text, der nicht in einem proprietären Format gespeichert wird. Der Ausdruck entstammt UNIX, das bearbeitete und nicht verarbeitete Modi für die Datenausgabe an einen Terminal unterstützt.

RBAC

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

RDRAM

Akronym für Rambus DRAM. Dynamische RAM-Chip-Technologie von Rambus, Inc. Direkt-RDRAMs werden in Systemen verwendet. Direkt-RDRAM-Chips sind in RIMM-Modulen untergebracht, die DIMMs ähnlich sind, aber unterschiedliche Stiftbelegungen aufweisen. Die Chips können mit Doppelkanälen gebaut werden, wodurch die Übertragungsrate auf 3,2 GB/s verdoppelt wird.

Realmodus

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

Remote-Verwaltungssystem

Ein Remote-verwaltetes System ist ein beliebiges System, das von einem entfernten Standort aus mit Hilfe eines unterstützten Web-Browsers auf die Server Administrator-Homepage auf einem verwalteten System zugreift. Siehe verwaltetes System.

RFI

Abkürzung für Radio Frequency Interference (Hochfrequenzinterferenz).

RGB

Abkürzung für rot/grün/blau.

RIMM

Akronym für Rambus In-Line Memory Module (Rambus-Speichermodul mit einer Kontaktanschlussreihe), der Rambus-Version eines DIMM-Moduls.

RMI

Akronym für den Remote-Methodenaufruf. RMI ist ein Teil der Java Programmiersprachen-Bibliothek, die ein Java Programm ermöglicht, das auf einem System läuft, auf die Gegenstände und Methoden eines anderen Javanischen Programms zuzugreifen, das auf einem verschiedenen System läuft.

ROM

Akronym für Read-Only Memory (Nur-Lese-Speicher). Einige der für den Einsatz des Systems wesentlichen Programme sind in ROM-Code. Im Gegensatz zum

RAM geht der Inhalt des ROM-Chips beim Ausschalten des Systems nicht verloren. Beispiele von Code in ROM schließen das Programm mit ein, das die Startroutine des Systems und den POST einleitet.

RPM

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

RTC

Abkürzung für Real-Time Clock (Echtzeituhr). Eine von der Stützbatterie gespeiste Uhr im Innern des Systems, die bei ausgeschaltetem System Datum und Uhrzeit beibehält.

SAN

Akronym für Storage Area Network (Speicherbereichsnetzwerk).

SAS

Akronym für Secure Authentication Services oder serial-attached SCSI. Wenn es sich um Sicherheitsprotokolle oder Authentifizierung handelt, ist SAS Secure Authentication Services. Wenn es sich um Computerperipheriegeräte handelt, die serielle (ein Bit auf einmal) Mittel zur Digitaldatenübertragung über dünne Kabel verwenden, ist SAS Serial-attached SCSI.

SCA

Abkürzung für Single Connector Attachment (Einzelanschluss-Anlage).

Schalter

Schalter kontrollieren verschiedene Schaltkreise auf der Systemplatine bzw. steuern verschiedene Funktionen im Computersystem. Diese Schalter werden auch als DIP-Schalter bezeichnet. Sie sind normalerweise zu Gruppen von zwei oder mehreren Schaltern in einem Kunststoffgehäuse zusammengefasst. Zwei Sorten von DIP-Schaltern sind auf Systemplatinen gebräuchlich: Schiebeschalter und Kippschalter. Die Bezeichnungen der Schalter beziehen sich auf die Weise, mit der die Stellungen (ein und aus) verändert werden.

Schema

Eine Sammlung von Klassendefinitionen, die verwaltete Objekte in einer bestimmten Umgebung beschreibt. Ein Schema ist eine Sammlung von Klassendefinitionen zur Repräsentation verwalteter Objekte, die für jede Verwaltungsumgebung allgemein gleich sind, weshalb CIM Allgemeines Informationsmodell genannt wird.

Schreibgeschützt

Nur-Lese-Dateien sind schreibgeschützt. Eine 3,5-Zoll-Diskette kann durch Verschieben der Schreibschutzkerbe in die offene oder durch Einstellen der Schreib-Schutz-Funktion im System-Setup-Programm Position, schreibgeschützt werden.

Schutzmodus

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

- Einen Speicheradressbereich von 16 MB (80286er Mikroprozessoren) bis 4 GB (Intel386 oder höher)
- Multitasking
- Virtueller Speicher, ein Verfahren, um den adressierbaren Speicherbereich durch Verwendung des Festplattenlaufwerks zu vergrößern

Die 32-Bit Betriebssysteme Windows NT, OS/2® und UNIX® werden im Schutzmodus betrieben. MS-DOS kann nicht im Schutzmodus arbeiten; einige Programme, die unter MS-DOS ausgeführt werden, z. B. Windows, können jedoch das System in den Schutzmodus versetzen.

SCSI

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

SDMS

Abkürzung für SCSI Device Management System (SCSI-Geräteverwaltungssystem).

SEC

Abkürzung für Single-Edge Contact (Einseitiger Anschluss).

Sek

Abkürzung für Sekunden.

SEL

Akronym für System Event Log (Systemereignisprotokoll).

Serielle Schnittstelle

Eine E/A-Schnittstelle, die meistens dazu verwendet wird, ein Modem an ein System anzuschließen. Sie können eine serielle Schnittstelle normalerweise an ihrem 9-poligen Anschluss erkennen.

Servermodul

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

Service-Tag-Nummer

Ein Strichcode-Etikett, das jedes System kenntlich macht, wenn man sich an den Kundendienst oder den technischen Support wenden muss.

SGRAM

Akronym für synchrones Graphik-RAM.

Shadowing

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

Sicherungskopie

Eine Kopie eines Programms oder einer Datendatei. Vorsichtshalber sollten Sie regelmäßig Sicherungskopien der Festplattenlaufwerke des Systems anlegen. Bevor Sie Änderungen an der Systemkonfiguration vornehmen, sollten Sie von den wichtigsten Systemstartdateien des Betriebssystems Sicherungskopien anfertigen.

Signaltoncode

Eine diagnostische Meldung in Form einer Serie von Signaltonmustern, die über den Lautsprecher des Systems ausgegeben wird. Ein Signaltoncode gefolgt von einem zweiten und dann von drei kurz aufeinander folgenden Signaltönen ist z. B. der Signaltoncode 1-1-3.

SIMD

Abkürzung für Single Instruction Multiple Data (Einzelanweisung/Mehrfachdaten).

SIMM

Akronym für Single In-Line Memory Module [Speichermodul mit einer Kontaktanschlussreihe] Eine kleine Platine, die DRAM-Chips enthält und an die Systemplatine angeschlossen ist.

SIP

Akronym für Single On-Line Package (Paket mit einer Kontaktanschlussreihe), ein Gehäusetyp für elektronische Komponenten, bei denen die Anschlussstifte auf einer Seite hervorstehen. Ein SIP wird auch Stiftpaket mit einer Kontaktanschlussreihe (SIPP) genannt .

SKU

Akronym für Stock Keeping Unit (Inventarüberwachungseinheit).

SMART

Akronym für Self-Monitoring Analysis Reporting Technology (Selbstüberwachende Analyse- und Berichtstechnologie). Eine Technologie, mit der Festplattenlaufwerke Fehler und Ausfälle an das System-BIOS melden können, das dann eine entsprechende Fehlermeldung auf dem Bildschirm anzeigt. Um von dieser Technologie Gebrauch machen zu können, müssen Sie über ein SMART-kompatibles Festplattenlaufwerk und die entsprechende Unterstützung im System-BIOS verfügen.

SMBIOS

Akronym für Systemverwaltungs-BIOS.

SMD

Abkürzung für Surface Mount Device (Oberflächenmontierte Geräte).

SMTP

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

SNMP

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

SODIMM

Akronym für DIMM mit kleinem Profil. Ein DIMM-Modul mit einem dünneren Profil aufgrund der Verwendung von TSOP Chip-Paketen. SODIMMs werden gewöhnlich in portablen Computern verwendet.

SOIC

Abkürzung für Small Outline IC, ein kleines, rechteckiges, oberflächenmontiertes Chip-Paket aus Kunststoff, das nach außen stehende Flügelstifte verwendet.

SOJ

Abkürzung für Small Outline Package J-Lead, einem kleines, rechteckiges, oberflächenmontiertes Chip-Paket aus Kunststoff mit J-förmigen Stiften an den beiden Längsseiten.

Speicher

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

Speicheradresse

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

Speichermodul

Eine kleine Platine mit DRAM-Chips, die an die Systemplatine angeschlossen ist.

Speicherverwalter

Ein Dienstprogramm, das die Implementierung des über den konventionellen Speicher hinausgehenden Speicherplatzes, wie z. B. Erweiterungs- oder Expansionsspeicher, regelt.

SRAM

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

SSL

Abkürzung für Secure Socket Layer (Sichere Sockelschicht).

Startfähige Diskette

Sie können das System von einer Diskette aus starten. Zum Erstellen einer startfähigen Diskette legen Sie eine Diskette in das Diskettenlaufwerk ein, geben Sie auf die Befehlseingabeaufforderung hin sys a:ein und drücken Sie <Eingabe>. Verwenden Sie diese startfähige Diskette, wenn Ihr System nicht von der Festplatte startet.

Startroutine

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

Status

Bezieht sich auf den Funktionszustand oder das Funktionieren eines Objekts. Beispiel: Eine Temperatursonde kann den Status "normal" haben, wenn die Sonde akzeptable Temperaturen misst. Wenn die Sonde Temperaturen liest, die die vom Benutzer gesetzten Grenzen überschreiten, meldet sie einen kritischen Status.

Stromversorgung

Ein Satz Netzteile in einem Systemgehäuse.

SVGA

Abkürzung für Super Video Graphics Array (Super-Video-Graphikanordnung). VGA und SVGA sind Standards für Videoadapter mit höherer Auflösung und besserer Farbanzeige als frühere Standards.

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

Syntax

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

system.ini-Datei

Eine Startdatei des Betriebssystems Windows. Beim Aufruf des Windows-Betriebssystems wird zuerst die Datei **system.ini** gelesen, um die verschiedenen Optionen für die Windows-Betriebsumgebung festzulegen. U. a. wird in der Datei **system.ini** fest gehalten, welche Video-, Maus- und Tastaturtreiber für Windows installiert sind.

Mit der Systemsteuerung oder dem Windows-Setup-Programm können Optionen in der Datei **system.ini** geändert werden. In anderen Fällen müssen eventuell mit einem Text-Editor (z. B. Notepad) Optionen für die Datei **system.ini** manuell geändert oder hinzugefügt werden.

Systemdiskette

Systemdiskette ist ein Synonym für startfähige Diskette.

System-Kennnummer-Code

Ein normalerweise von einem Systemadministrator individuell dem System zugewiesener Code für Sicherheit und Überwachung.

Systemkonfigurationsdaten

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

Systemplatine

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

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

Hauptplatine und Platine werden oft als Synonyme für Systemplatine verwendet.

System-Setup-Programm

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

Systemspeicher

Systemspeicher ist ein Synonym für RAM.

Tabelle

Bei SNMP-MIBs ist eine Tabelle ein zweidimensionaler Array, der die Variablen beschreibt, aus denen ein verwaltetes Objekt besteht.

Tastenkombination

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

TCP/IP

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

Terminierung

Einige Geräte (wie z. B. das letzte Gerät an jedem Ende eines SCSI-Kabels) müssen terminiert werden, um Reflexionen und unechte Signale im Kabel zu verhindern. Wenn mehrere dieser Geräte in Serie geschaltet sind, muss eventuell der Abschlusswiderstand an diesen Geräten aktiviert oder deaktiviert werden, indem Sie einen Jumper oder eine Schalterstellung am Gerät ändern oder die Einstellungen in der Konfigurationssoftware für das Gerät ändern.

Texteditor

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

Textmodus

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

TFTP

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

tpi

Abkürzung für Tracks per Inch (Spuren pro Zoll).

TQFP

Abkürzung für Thin Quad Flat Pack.

TSOP

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

TSR

Abkürzung für Terminate-and-Stay-Resident (Beenden und im Speicher verbleiben). Ein TSR-Programm wird "im Hintergrund" ausgeführt. " Die meisten TSR-Programme implementieren eine vorbestimmte Tastenkombination (die auch als Hot Key bezeichnet wird), mit der die Schnittstelle des TSR-Programms aktiviert werden kann, während ein anderes Programm ausgeführt wird. Nach Ausführung des TSR-Programms können Sie zum anderen Anwendungsprogramm zurückkehren, wobei das TSR-Programm im Speicher verbleibt und für spätere Einsätze abrufbar ist. Manchmal können TSR-Programme Speicherkonflikte verursachen. Bei der Fehlersuche kann diese Möglichkeit ausgeschlossen werden, indem das System ohne das Abrufen von TSR-Programmen neu gestartet wird.

U/min

Abkürzung für Umdrehungen pro Minute.

UART

Akronym für Universal Asynchronous Receiver Transmitter (Universeller asynchroner Sender/Empfänger), der elektronische Schaltkreis, aus dem die serielle Schnittstelle besteht.

UDP

Abkürzung für User Datagram Protocol (Protokoll für Benutzerdatagramme).

UL

Abkürzung für Underwriters Laboratories.

UMB

Abkürzung für Upper Memory Blocks (Obere Speicherblöcke).

Unicode

Ein Zeichencode mit fester Breite von 16 Bits, entwickelt und erhalten vom Unicode Consortium.

URL

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

USB

Abkürzung für Universal Serial Bus (Universeller serieller Bus). Ein USB-Anschluss stellt einen einzelnen Anschluss für mehrere USB-kompatible Geräte wie z. B. Mausgeräte, Tastaturen, Drucker oder Computerlautsprecher. USB-Geräte können außerdem auch während des Betriebs angeschlossen oder abgenommen werden.

USV

Abkürzung für Unterbrechungsfreie Stromversorgung. Ein batteriebetriebenes Gerät, das bei Stromausfall automatisch die Versorgung des Systems übernimmt.

UTP

Abkürzung für Unshielded Twisted Pair (Nicht abgeschirmtes verdrilltes Leiterpaar).

UUID

Abkürzung für Universal Unique Identification (Universelle eindeutige Kennung).

V

Abkürzung für Volt.

VAC

Abkürzung für Volt(s) Alternating Current (Volt Wechselstrom).

varbind

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

Variable

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

VCCI

Abkürzung für Voluntary Control Council for Interference (Freiwilliger Rat für Interferenz).

VDC

Abkürzung für Volt(s) Direct Current (Volt Gleichstrom).

Verwaltetes System

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

Verzeichnis

Mit Hilfe von Verzeichnissen können Dateien auf einer Festplatte in einer hierarchischen Struktur (ähnlich der eines umgekehrten Baumes) organisiert werden. Jede Festplatte hat ein "Stammverzeichnis"; z. B. zeigt eine **C:\>** -Eingabeaufforderung normalerweise an, dass man sich beim Stammverzeichnis der Festplatte C befindet. Weitere Verzeichnisse, die vom Stammverzeichnis abzweigen, werden Unterverzeichnisse genannt. Von Unterverzeichnissen können zusätzliche Verzeichnisse abzweigen.

VESA

Akronym für Video Electronics Standards Association (Vereinigung für Videoelektronik-Normung).

VGA

Abkürzung für Video Graphics Array (Video-Graphikanordnung). VGA und SVGA sind Standards für Videoadapter mit höherer Auflösung und besserer Farbanzeige als frühere Standards. Um ein Programm mit einer bestimmten Auflösung wiederzugeben, müssen die entsprechenden Videotreiber installiert sein und der Monitor muss die gewünschte Auflösung unterstützen. Die Anzahl der von einem Programm wiedergegebenen Farben hängt von den Fähigkeiten des Bildschirms, des Videotreibers und der Größe des für den Videoadapter installierten Videospeichers ab.

VGA-Funktionsanschluss

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

Videoadapter

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

Bei einigen Systemen ist der Videoadapter in die Systemplatine integriert. Gleichzeitig steht eine Vielzahl von Videoadapterkarten zur Verfügung, die in einem Erweiterungssteckplatz eingebaut werden können.

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

Videoauflösung

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

Videomodus

Videoadapter unterstützen normalerweise mehrere Text- und Graphikmodi. Zeichenbasierte Software zeigt die Zeichen in Textmodus wie folgt an: *x* Spalten mal *y* Zeilen. *Grafikbasierte Software zeigt Grafiken im Grafikmodus wie folgt an: x horizontale mal y vertikale Pixel mal z* Farben.

Videospeicher

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

Videotreiber

Graphikmodus-Anwendungsprogramme und -Betriebsumgebungen benötigen ein solches Programm, um die Anzeige mit einer bestimmten Auflösung und Farbenzahl darzustellen. Dabei kann ein Softwarepaket einige "generische" Videotreiber umfassen. Zusätzliche Videotreiber müssen in der Regel auf den im System installierten Videoadapter zugeschnitten sein.

Virtueller Speicher

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

Virus

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

- Führen Sie in regelmäßigen Abständen ein Dienstprogramm aus, das das Festplattenlaufwerk auf Viren überprüft.
- Führen Sie für alle Disketten (einschließlich der gewerblich erstandenen Software) vor deren Anwendung stets eine Virusüberprüfung durch.

VLSI

Abkürzung für Very-Large-Scale Integration (Hochintegration).

VLVESA

Akronym für Very Low Voltage Enterprise System Architecture (Extrem niederspannige Systemarchitektur).

Vpp

Abkürzung für Peak-Point Voltage (Spitzenpunktspannung).

VRAM

Akronym für Video Random-Access Memory (Videospeicher mit wahlfreiem Zugriff). Einige Videoadapter verwenden VRAM-Chips (oder eine Kombination von VRAM- und DRAM-Chips), um die Videoleistung zu steigern. VRAM-Speicher sind zweikanalig, sodass der Videoadapter gleichzeitig den Bildschirm auffrischen und neue Anzeigendaten empfangen kann.

VRM

Abkürzung für Spannungsregler.

W

Abkürzung für Watt.

Wake Up On LAN

Die Möglichkeit, die Spannung in einer Client-Station über das Netzwerk einzuschalten. Remote-Aktivierung ermöglicht die Durchführung von Tasks wie Softwareaktualisierung und anderen Verwaltungstasks auf Benutzerrechnern nach Ende des Arbeitstages. Es erlaubt auch Remote-Benutzern den Zugang zu ausgeschalteten Rechnern. Intel nennt die Remote-Aktivierung "Wake-on-LAN".

Web-Server

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

WH

Abkürzung für Wattstunde(n).

win.ini-Datei

Eine Startdatei des Betriebssystems Windows. Beim Start von Windows konsultiert das Programm die Datei **win.ini**, um verschiedene Optionen für die Windows-Betriebsumgebung festzulegen. Unter anderem wird in der Datei **win.ini** fest gehalten, welche Drucker und Schriftarten für Windows installiert wurden. Andere Teile der Datei **win.ini** enthalten optionale Einstellungen für auf der Festplatte installierte Windows-Anwendungen. Mit der Systemsteuerung oder dem Windows-Setup-Programm können Optionen in der Datei **system.ini** geändert werden. In anderen Fällen müssen eventuell mit einem Texteditor (z. B. Notepad) Optionen für die Datei **win.ini** geändert oder hinzugefügt werden.

Winbind

Ein Programm, das Benutzern in einem heterogenen Netzwerk erlaubt, die Verwendung von Workstationen anzumelden, die entweder UNIX oder Betriebssysteme von Windows NT besitzen. Das Programm macht Workstations, welche UNIX verwenden, in NT-Domänen funktionsfähig, indem es NT wie UNIX zu jeder Workstation von UNIX aussehen lässt.

Windows 95

Ein integriertes und vollständiges Microsoft Windows-Betriebssystem, das MS-DOS nicht erfordert und verbesserte Betriebsfunktionen, leichtere Bedienung, erweiterte Arbeitsgruppenfähigkeit und vereinfachte Dateiverwaltung und -einsicht bietet.

Windows NT

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

WMI

Akronym für Windows Management Instrumentation. WMI bietet CIM Objektverwalterdienste.

X Window System

Die graphische Benutzeroberfläche, die in der Red Hat Enterprise Linux® -Umgebung verwendet wird.

X.509-Zertifikat

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

Xen

Xen ist ein virtueller Computermonitor für x86-Systeme.

XMM

Englische Abkürzung für Erweiterungsspeicherverwalter, ein Dienstprogramm, das es Anwendungsprogrammen und Betriebssystemen ermöglicht, in Übereinstimmung mit dem XMS den Erweiterungsspeicher zu verwenden.

XMS

Abkürzung für eXtended Memory Specification (Spezifikationen für den Expansionsspeicher).

Zeitüberschreitung

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

ZIF

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

ZIP

Ein herausnehmbares 3,5-Zoll-Diskettenlaufwerk von Iomega. Ursprünglich enthielt es herausnehmbare 100 MB-Kassetten. Das Laufwerk verfügt über Software, die die Disketten katalogisieren und die Dateien zur Sicherheit sperren kann. Eine 250 MB-Version des Zip-Laufwerks kann auch die 100 MB-Zip-Kassetten lesen und beschreiben.

Zugewiesener physikalischer Speicher-Array

Der zugewiesene physikalische Speicher-Array bezieht sich auf die Methode der Aufteilung des physikalischen Speichers.

Zum Beispiel kann ein zugewiesener Bereich 640 KB und der andere zugewiesene Bereich zwischen 1 und 127 MB aufweisen.

Zugriff

Bezieht sich auf die Maßnahmen, die ein Benutzer an einem variablen Wert durchführen kann. Beispiele sind Nur-Lese- und Lese-Schreibvorgänge.

Zustand

Bezieht sich auf den Zustand eines Objekts, das mehr als einen Zustand aufweisen kann. Beispiel: Ein Objekt kann den Zustand "nicht bereit" aufweisen.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Server Administrator installieren

Dell™ OpenManage™ Server Administrator: Benutzerhandbuch Version 5.2

Überblick

Server Administrator kann auf verschiedene Arten installiert werden. Die CD *Dell™ PowerEdge™ Installation and Server Management* bietet ein Setup-Programm für die Installation, die Aktualisierung und die Deinstallation von Server Administrator und anderen Managed System- und Management Station Software-Komponenten auf Ihrem verwalteten System. Die CD *Dell Systems Management*-Konsolen bietet ein Setup-Programm zum Installieren, Erweitern und Deinstallieren von Management Station Software-Komponenten auf Ihrer Verwaltungsstation. Zusätzlich können Sie den Server Administrator mittels einer unbeaufsichtigten Installation über ein Netzwerk auf mehreren System installieren. Dell OpenManage™-Produkte werden mithilfe des Installationsverfahrens installiert, das dem Betriebssystem systemeigen ist. Folgen Sie den Anleitungen des Konfigurationsassistenten, um Server Administrator einzurichten. Details finden Sie im *Dell OpenManage-Installations- und Sicherheitsbenutzerhandbuch*.

CD Dell PowerEdge Installation and Server Management

Die CD *Dell PowerEdge Installation and Server Management* bietet ein Setup-Programm für die Installation, die Aktualisierung und die Deinstallation von Server Administrator und anderen Managed System- und Management Station Software-Komponenten auf Ihrem verwalteten System. Zusätzlich können Sie den Server Administrator mittels einer unbeaufsichtigten Installation über ein Netzwerk auf mehreren System installieren.

Mit dem Setup-Programm auf der CD *Dell PowerEdge Installation and Server Management* können Sie den Server Administrator auf Systemen installieren und erweitern, die alle unterstützte Betriebssysteme ausführen. Auf Systemen, auf denen unterstützte Microsoft® Windows®, Red Hat® Enterprise Linux® und SUSE® LINUX Enterprise Server-Betriebssysteme ausgeführt werden, kann der Server Administrator mit der CD *Dell Installation and Server Management* oder über das Betriebssystem deinstalliert werden. Weitere Details finden Sie im *Dell OpenManage-Installations- und Sicherheitsbenutzerhandbuch*.

ANMERKUNG: Nach dem Installieren oder Deinstallieren von Server Administrator auf Dell PowerEdge 4600 müssen Sie das System neustarten, damit die Änderungen wirksam werden.

Unbeaufsichtigte Installation ohne Eingaben durch den Benutzer

Sie können mithilfe der CD *Dell™ PowerEdge™ Installation and Server Management* unbeaufsichtigte Installationen und Deinstallationen von Server Administrator auf Systemen vornehmen, auf denen unterstützte Microsoft Windows-, Red Hat Enterprise Linux- und SUSE LINUX Enterprise Server-Betriebssysteme ausgeführt werden. Zusätzlich können Sie Server Administrator auch über die Befehlszeile auf Systemen installieren bzw. deinstallieren, die unterstützte Microsoft Windows-, Red Hat Enterprise Linux- und SUSE LINUX Enterprise Server-Betriebssysteme ausführen.

Server Administrator erweitern

Mit der Dell OpenManage Software können Sie die Version 4.3 oder höher auf Version 5.2 erweitern. Vor dem Upgrade müssen Sie die frühere Version von Server Administrator deinstallieren und dann die neueste Version installieren, die die CD *Dell PowerEdge Installation and Server Management* verwendet.

ANMERKUNG: Service Pack-Upgrade wird in Dell OpenManage 5.2 nicht unterstützt.

ANMERKUNG: Wenn Sie eine frühere Version von Dell OpenManage als 4.3, erweitern Sie zu Version 4.3 und installieren Sie Dell OpenManage 5.2. Weitere Informationen finden Sie im *Dell OpenManage-Installations- und Sicherheitsbenutzerhandbuch*.

Um von 4.*3* oder später auf Dell OpenManage 5.2 zu erweitern verwenden Sie **setup.exe** oder geben Sie Folgendes ein:

```
msiexec/i SysMgmt.msi/qn
```
(für neue Installationen oder wichtige Upgrades. Zum Beispiel von Dell OpenManage Version 4.3 auf Version 5.2 erweitern.)

Für kleinere Upgrades, z. B. um von Dell OpenManage Version 4.3 auf Version 4.4 zu erweitern, geben Sie Folgendes ein:

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

Erweitern von MSI Engine

Mit Dell OpenManage Software können Sie MSI Engine erweitern während interaktive Installationen ausgeführt werden. Für Silent Installs muss der entsprechende Befehl zu den Installations-Skripts hinzufügt werden.

Verwenden Sie den folgenden Befehl in Ihrem Bereitstellungsskript, um MSI Engine (falls erforderlich) zu erweitern und die Systemverwaltungssoftware zu installieren/erweitern.

ANMERKUNG: Für Dell OpenManage Systems Management und Management Station-Installationsprogramme ist MSI 3.1 oder höher erforderlich. Aktualisieren Sie die MSI Engine, wenn Sie ein System verwenden, das ein Windows Server® 2003 (ohne Service Pack), Windows 2000 Server oder Windows XP-Betriebssystem ausführt. Wenn Sie ein System verwenden, das ein Windows Server 2003 SP2- oder Windows Server 2003 x64-Betriebssystem ausführt, müssen Sie die MSI Engine nicht aktualisieren.

```
:retry
start /wait msiexec /i SysMgmt.msi /qn
if %errorlevel% == 1613 (
REM UPGRADE THE WINDOWS INSTALLER ENGINE
start /wait WindowsInstaller-KB893803-v2-x86.exe /quiet /norestart
goto retry
)
if %errorlevel% == 1638 (
REM THIS IS A MINOR UPGRADE
start /wait msiexec /i SysMgmt.msi REINSTALL=ALL REINSTALLMODE=vomus/qn
)
```

Informationen zu Installationsverfahren und schrittweisen Anleitungen zur Installation, Erweiterung und Deinstallation des Server Administrator auf allen unterstützten Betriebssystemen finden Sie im *Dell OpenManage-Installations- und Sicherheitsbenutzerhandbuch*.

Bevor Sie beginnen

- Lesen und befolgen Sie die entsprechenden Anweisungen unter "Setup und Administration."
- Lesen Sie die Installationsvoraussetzungen, um sicherzustellen, dass Ihr System die Mindestanforderungen erfüllt.
- Lesen Sie das *Dell OpenManage-Installations- und Sicherheitsbenutzerhandbuch*, um für alle unterstützten Betriebssysteme schrittweise Anleitungen zur Installation, Erweiterung und Deinstallation von Server Administrator zu erhalten.
- Lesen Sie das *Server Administrator: Kompatibilitätshandbuch*. Dieses Dokument enthält Kompatibilitätsinformationen zu Server Administrator-Installation und -Betrieb auf verschiedenen Hardwareplattformen (oder Systemen) unter unterstützten Microsoft Windows-, Red Hat Enterprise Linux- und SUSE LINUX Enterprise Server-Betriebssystemen.
- Lesen Sie die Dell OpenManage-Installations-Infodatei auf der CD *Dell PowerEdge Installation and Server Management*. Die Datei enthält die neusten Informationen über neue Funktionen zusätzlich zu Informationen über bekannte Probleme.
- Lesen Sie die Server Administrator-Infodatei auf der CD *Dell PowerEdge Installation and Server Management*. Die Datei enthält die neuesten Informationen über Software-, Firmware- und Treiberversionen sowie Informationen über bekannte Probleme.
- Lesen Sie die Installationsanweisungen für Ihr Betriebssystem.

Installationsvoraussetzungen

In den folgenden Abschnitten werden die allgemeinen Voraussetzungen für den Server Administrator beschrieben. Betriebssystemspezifische Installationsvoraussetzungen werden als Teil der Installationsverfahren aufgelistet.

Unterstützte Betriebssysteme

Server Administrator unterstützt die folgenden Betriebssysteme:

- Microsoft Windows 2000 Server-Familie (Intel x86) (einschließlich Windows 2000 Server SP4 oder höher und Windows 2000 Advanced Server SP4 oder höher)
- Microsoft Windows Server 2003-Familie (32-Bit x86) (einschließlich SP1 mit Web, Standard und Enterprise Editionen) und Microsoft Windows Small Business Server [SBS] 2003 SP1
- Microsoft Windows Server 2003-Familie (x86_64) (einschließlich SP2 mit Standard und Enterprise Editionen), Microsoft Windows SBS 2003 SP1 und Microsoft Windows SBS 2003 R2
- Microsoft Windows Server 2003-Familie (mit R2) (einschließlich Standard und Enterprise Edition)
- Microsoft Windows Server 2003 (x86_64) R2 (einschließlich Standard und Enterprise Edition)
- Microsoft Windows Server 2003 R2 Standard, Enterprise und Datacenter x64 Editions mit SP2
- Microsoft Windows Storage Server 2003 R2 (einschließlich Express, Standard, Workgroup und Enterprise Editions)
- Red Hat Enterprise Linux AS, ES und WS, (Version 4) (x86) Update
- Red Hat Enterprise Linux AS, ES und WS, (Version 4) (x86_64) Update
- Red Hat Enterprise Linux 4 (ia64)
- Red Hat Enterprise Linux Server 5 (x86)
- Red Hat Enterprise Linux Server 5 (x86_64)

  ANMERKUNG: Die Unterstützung für aktualisierte Kernel, die von Red Hat freigegeben wurden bzw. für spätere Versionen von Red Hat Enterprise Linux freigegeben wurden, kann die Verwendung der Dynamischen Kernel-Unterstützung erfordern (eine Beschreibung dieser Funktion finden Sie unter "*Installations- und Sicherheitsbenutzerhandbuch*").

- SUSE Linux Enterprise Server (Version 9) (SP3 für x86_64)
- SUSE Linux Enterprise Server (Version 10) (x86_64)

ANMERKUNG: In der Infodatei von Server Administrator auf der *Dell PowerEdge Installations- und Server Management* oder der *Support-Matrix* auf der CD *Dell PowerEdge Documentation* befindet sich die neueste detaillierte Liste der Server Administrator-Dienste, die auf jedem unterstützten Betriebssystem unterstützt werden.

Systemanforderungen

Server Administrator muss auf jedem zu verwaltenden System installiert werden. Dann können Sie jedes System verwalten, indem Sie Server Administrator lokal oder entfernt über einen unterstützten Web-Browser ausführen.

Die Voraussetzungsprüfung (**setup.exe**) auf der CD *Dell PowerEdge Installation and Server Management* wird Ihr System automatisch analysieren, um zu bestimmen, ob die Systemanforderungen erfüllt wurden. Weitere Informationen erhalten Sie unter "Voraussetzungsprüfung für Windows".

Anforderungen für das verwaltete System

- Eines der unterstützten Betriebssysteme.
- Mindestens 128 MB RAM.
- Mindestens 256 MB an freier Festplattenspeicherkapazität.
- Administratorrechte.
- Eine TCP/IP-Verbindung zum überwachten System und zum Remote-System zur Vereinfachung der Verwaltung des Remote-Systems.
- Einer der unterstützten Web-Browser.
- Einer der "unterstützten Systemverwaltungsprotokoll-Standards".
- Maus, Tastatur und Monitor zur lokalen Verwaltung eines Systems. Für den Monitor ist eine Mindestauflösung von 800 x 600 erforderlich. Die empfohlene Bildschirmauflösung ist 1024 x 768.
- Der Server Administrator Remote Access Controller erfordert, dass ein DRAC (Dell Remote Access Controller) auf dem zu verwaltenden System installiert wird. Entsprechende Dell Remote Access Controller-Benutzerhandbücher für vollständige Software- und Hardwareanforderungen erhalten Sie unter "Remote Access Controller" und "Weitere nützliche Dokumente".

  ANMERKUNG: Die DRAC-Software wird als Teil der Installationsoptionen von **Typisches Setup** und **Benutzerdefiniertes Setup** installiert, wenn Managed System Software von der CD *Dell PowerEdge Installation and Server Management* installiert wird, vorausgesetzt, dass das verwaltete System alle Voraussetzungen zur DRAC-Installation erfüllt. Entsprechende Dell Remote Access Controller-Benutzerhandbücher für vollständige Software- und Hardwareanforderungen erhalten Sie unter "Remote Access Controller" und "Weitere nützliche Dokumente".

- Der Storage Management-Service wird standardmäßig unter Verwendung von **Typisches Setup** auf Systemen installiert, die unterstützte Windows-Betriebssysteme ausführen.

  ANMERKUNG: Auf Red Hat Enterprise Linux- und SUSE LINUX Enterprise Server-Systemen können Sie entweder den Storage Management-Service über Red Hat Package Manager (RPM) installieren oder verwenden Sie das Skript `srvadmin-install.sh` - ein menügesteuertes Skript, welches die entsprechenden RPMs basierend auf den ausgewählten Optionen installiert.

Remote-Verwaltungssystem - Anforderungen

- Einer der unterstützten Web-Browser zur Remote-Verwaltung eines Systems von der Server Administrator-Startseite aus.
- Eine TCP/IP-Verbindung zum verwalteten System und zum Remote-System zur Vereinfachung der Verwaltung des Remote-Systems.
- Mindestbildschirmauflösung von 800 x 600. Die empfohlene Bildschirmauflösung ist 1024 x 768.

Unterstützte Web-Browser

Zur lokalen Verwaltung eines Systems von der Server Administrator-Homepage aus ist ein unterstützter Web-Browser erforderlich. Unterstützte Browser:

- Internet Explorer 7.0 und 6.0 SP2 (Nur für Microsoft Windows)
- Mozilla FireFox 2.0 (Für Microsoft Windows Server 2003, Windows XP, Red Hat Enterprise Linux, und SUSE Linux Enterprise Server)
- Mozilla FireFox 1.5 (Für SUSE Linux Enterprise Server und Red Hat Enterprise Linux)

ANMERKUNG: In der Infodatei von Server Administrator auf der *Dell PowerEdge Installations- und Server Management* oder der *Support-Matrix auf der CD Dell PowerEdge Documentation* befindet sich die neueste detaillierte Liste der Server Administrator-Dienste, die auf jedem unterstützten Webbrowser unterstützt werden.

Unterstützte Systemverwaltungsprotokoll-Standards

Ein unterstützter Systems Management-Protokollstandard muss vor der Installation des Server Administrators auf dem verwalteten System installiert sein. Auf unterstützten Microsoft Windows-Betriebssystemen unterstützt Server Administrator diese beiden Systemverwaltungsstandards: Allgemeines Informationsmodell/Windows Management Instrumentation (CIM/WMI) und Einfaches Netzverwaltungsprotokoll (SNMP). Auf unterstützten Red Hat Enterprise Linux und SUSE Linux Enterprise Server-Betriebssystemen unterstützt Server Administrator den SNMP-Systemmanagementstandard.

ANMERKUNG: Informationen über die Installation eines Verwaltungsprotokollstandards für unterstützte Systeme auf Ihrem verwalteten System entnehmen Sie der Dokumentation Ihres Betriebssystems.

Tabelle 4-1 zeigt die Verfügbarkeit der Systemverwaltungsstandards für jedes unterstützte Betriebssystem.

Tabelle 4-1. Verfügbarkeit des Systemverwaltungsprotokolls nach Betriebssystemen

Betriebssystem	SNMP	CIM/WMI
Unterstützte Microsoft Windows-Betriebssysteme	Verfügbar auf den Installationsdatenträgern für das Betriebssystem.	Immer installiert
Unterstützte Red Hat Enterprise Linux-Betriebssysteme	Das mit dem Betriebssystem gelieferte ucd-snmp-Paket muss installiert werden.	Nicht verfügbar.
SUSE Linux Enterprise Server-Betriebssysteme	Das mit dem Betriebssystem gelieferte ucd-snmp-Paket muss installiert werden.	Nicht verfügbar.

Voraussetzungsprüfung für Windows

Das Voraussetzungsprüfungsprogramm setup.exe im Windows-Verzeichnis auf der CD *Dell Installation and Server Management* bietet die Fähigkeit, den erforderlichen Status für Softwarekomponenten zu untersuchen, ohne die eigentliche Installation zu starten. Dieses Programm zeigt ein Statusfenster an, das Informationen über die Systemhardware bietet, die für den Betrieb einiger Softwarekomponenten eventuell erforderlich ist.

Die Voraussetzungsprüfung kann unter Verwendung von **runprereqcheck.exe /s** automatisch ausgeführt werden.

Installationsverfahren

Informationen zu Installationsverfahren und schrittweisen Anleitungen zur Installation, Erweiterung und Deinstallation des Server Administrator auf allen unterstützten Betriebssystemen finden Sie im *Dell OpenManage-Installations- und Sicherheitsbenutzerhandbuch*.

Installieren des Server Administrator mit Citrix

Wenn Sie Server Administrator mit Citrix installieren wollen, müssen Sie die Installation in der folgenden Reihenfolge durchführen:

1. Installieren Sie das Betriebssystem mithilfe der CD *Dell PowerEdge Installation and Server Management*.

   ANMERKUNG: Installieren Sie Server Administrator oder andere Systemverwaltungssoftware nicht, bis Sie die Citrix Software installiert haben .

2. Installieren Sie die Citrix Software. Um vollständige Informationen über das Installieren und das Konfigurieren der Citrix Software zu erhalten, lesen Sie die Citrix-Dokumentation.

3. Installieren Sie Server Administrator mithilfe der CD *DellPowerEdge Installation and Server Management*.

Alle Anwendungen (einschließlich des Server Administrator) funktionieren ordnungsgemäß, wenn sie **nach** der Installation von Citrix installiert werden. Citrix weist bei der Installation alle Laufwerkbuchstaben neu zu.

Wenn Sie z. B. Server Administrator auf dem Laufwerk C: installieren und dann Citrix installieren, ändert dies den Laufwerkbuchstaben C: zu M:. Hieraus folgt, dass Server Administrator nicht ordnungsgemäß funktioniert, wenn Sie Citrix nach der Installation von Server Administrator installieren. Server Administrator kann repariert werden, indem Folgendes eingegeben wird:
`msiexec.exe/fa SysMgmt.msi`

Überlegungen vor der Installation des Storage Management Service

Storage Management ist mit Server Administrator integriert. Der Dell OpenManage Storage Management ist ein Ersatz für Array Manager.

Wenn Sie den Storage Management Service 2.0 installieren, wird eine vorherige Installation von Storage Management deinstalliert.

PERC-Konsole und FAST-Kompatibilität bei der Installation des Storage Management Service

Die Installation des Storage Management auf einem System, auf dem FAST oder die PERC-Konsole installiert ist, ist eine nicht unterstützte Konfiguration. Insbesondere werden Sie bemerken, dass der Storage Management Service oder die FAST-Funktionen während der Laufzeit deaktiviert sind, wenn Sie den Storage Management Service auf einem System nutzen, auf dem ebenfalls FAST installiert ist. Deshalb ist es erforderlich, dass Sie FAST und die PERC-Konsole deinstallieren, bevor Sie den Storage Management Service installieren.

Dell OpenManage Storage Management ersetzt alle Funktionen zur Speicherverwaltung die von FAST und der PERC-Konsole angeboten wurden. Außerdem ersetzt der Storage Management Service die Funktionen, die von FAST und der PERC-Konsole angeboten wurden.

Kompatibilität mit Linux-Dienstprogrammen bei der Installation des Storage Management Service

Es ist erforderlich, den erweiterten Storage Management Service auf einem Linux-System nicht zu installieren, das mit RAID-Speicherverwaltungsdienstprogrammen von Dell oder anderen Anbietern ausgerüstet ist. Sie sollten diese Dienstprogramme deinstallieren, bevor Sie den Storage Management Service installieren. Der Storage Management Service ersetzt die Funktionen zur Speicherverwaltung die von diesen Dienstprogrammen angeboten wurden. Beispiele für die Linux-Dienstprogramme von Dell oder anderen Anbietern:

- LinFlash
- DellMgr

- DellMON
- LINLib
- MegaMgr
- MegaMON

Vorausgesetzte Treiber und Firmware für Linux und den Storage Management Service

Unter Linux ist die Installation des Storage Management nicht in der Lage, zu entdecken ob die Treiber und die Firmware auf dem System die Anforderungen für die Installation und den Einsatz von Storage Management erfüllen. Bei der Installation unter Linux sind sie in der Lage, die Installation zu beenden, unabhängig davon, ob die Treiber- und die Firmware-Versionen die Anforderungen erfüllen. Wenn die Treiber- und die Firmware-Versionen die Anforderungen nicht erfüllen, haben Sie unter Umständen nicht den Zugriff auf alle Funktionen des Storage Management. Überprüfen Sie während der Laufzeit des Storage Management Service die Anwendungsprotokolldateien für Meldungen über veraltete Firmware-Versionen. Eine vollständige Liste der unterstützten Controller-Firmware- und Treiberversionen finden Sie in der Infodatei (readme_sm.txt) des Storage Management.

Filesystem Hierarchy Standard v2.3 Support

File Hierarchy System (FHS) ist eine Komponente der größeren Linux Standards Base-Definition. In dieser Version unterstützt Server Administrator die Verschiebung von Dateien.

Eine typische Installation platziert alle Dateien in: **/opt/dell/srvadmin**

Die entsprechenden betroffenen Verzeichnisse:

- Gemeinsam nutzbare (statische) Dateien in: **/opt/dell/srvadmin**
- Host-spezifische Dateien (benutzermodifizierbar): **/etc/opt/dell/srvadmin** und **/etc/opt//srvadmin**
- Dynamische (Protokoll-) Dateien: **/var/tmp/dell/srvadmin**, **/var/tmp//srvadmin** und **/var/log/dell/srvadmin /var/log//srvadmin**

Weitere Informationen finden Sie im *Dell OpenManage-Installations- und Sicherheitsbenutzerhandbuch*.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Instrumentation Service

Dell™ OpenManage™ Server Administrator: Benutzerhandbuch Version 5.2

Überblick

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

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

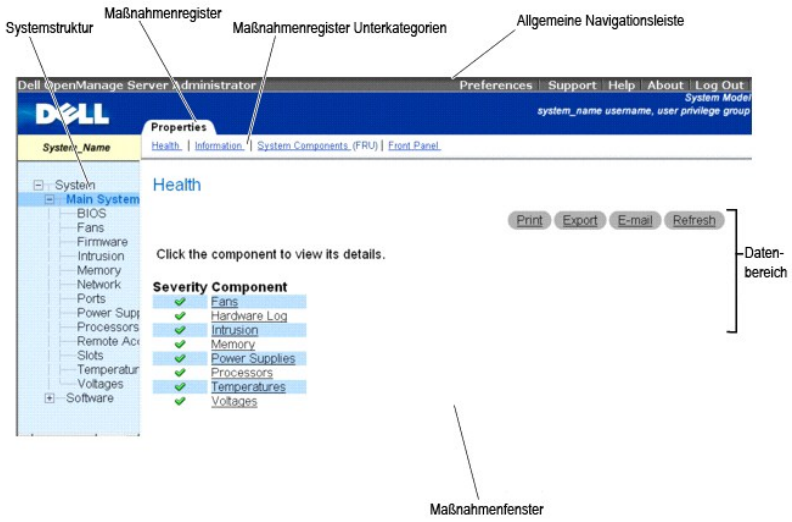
- Festlegung der Höchst- und Mindestwerte für bestimmte kritische Komponenten. Diese Werte, Schwellenwerte genannt, bestimmen den Bereich, in dem ein Warnungsereignis für die betreffende Komponente auftritt (Mindest- und Höchstausfallwerte werden vom Hersteller des Systems festgelegt).
- Festlegung der Systemreaktion bei Auftreten eines Warnungs- oder Ausfallereignisses. Benutzer können die Maßnahmen konfigurieren, die ein System als Reaktion auf Benachrichtigungen über Warnungs- und Ausfallereignisse ergreift. Andererseits können Benutzer mit permanenter Überwachung festlegen, dass keine Maßnahmen zu ergreifen sind, und sich auf das menschliche Urteil über die beste Reaktion auf ein Ereignis verlassen.
- 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 sowohl für verwaltete Systeme als auch Verwaltungsstationen, auf denen Microsoft® Windows Server® 2003 ausgeführt wird, konfigurieren, um SNMP-Pakete zu akzeptieren. Um Einzelheiten zu erhalten, lesen Sie "SNMP-Agenten für Systeme konfigurieren, auf denen unterstützte Windows-Betriebssysteme ausgeführt werden".

Systemverwaltung

Die Homepage des Server Administrators wird automatisch auf der Ansicht des **System**objekts der Systemstrukturansicht geöffnet. Die Standardeinstellung für das **System**objekt öffnet die **Zustands**komponenten im Register **Eigenschaften**.

Abbildung 6-1. Beispiel-Server Administrator-Homepage



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

ANMERKUNG: Viele der Systemstrukturobjekte, Systemkomponenten, Maßnahmenregister, Unterkategorien der Maßnahmenregister oder Datenbereichsfunktionen sind für einen Benutzer nicht verfügbar, der mit Benutzer-Zugriffsrechten angemeldet ist. Administrator- oder Hauptbenutzer-Zugriffsrechte sind zur Ansicht vieler der konfigurierbaren Systemstrukturobjekte, Systemkomponenten, Maßnahmenregister oder

Datenbereichsfunktionen erforderlich. Darüber hinaus haben nur Benutzer, die mit Administrator-Rechten angemeldet sind, Zugriff auf kritische Systemfunktionen wie die Herunterfahren-Funktion im Register **Herunterfahren** .

Die Voreinstellungen-Homepage zeigt standardmäßig auf die Seite **Zugriffs-Konfiguration** im Register **Voreinstellungen**.

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

Verwaltung von Systemstrukturobjekten

Die Systemstruktur des Server Administrator zeigt alle sichtbaren Systemobjekte basierend auf den Software- und Hardwaregruppen an, die der Server Administrator auf dem verwalteten System feststellt, und auf den Zugriffsrechten der Benutzer. Die Systemkomponenten werden nach Komponententyp kategorisiert. Wenn das Hauptobjekt - **System** - erweitert wird, sind die Hauptkategorien der Systemkomponenten, die erscheinen können "**Hauptsystemgehäuse**," "**Software**" und "**Speicher**."

Wenn der Storage Management Service installiert ist - abhängig vom Controller und Speicher, der dem System hinzugefügt wurde - erweitert sich das Speicherstrukturobjekt, um die folgenden Objekte anzuzeigen:

- Controller
- Batterie
- Konnektor
- Gehäuse oder Rückwandplatine
- Physische Festplatten
- EMMs
- Lüfter
- Netzteile
- Temperaturen
- Virtuelle Festplatten
- Firmware-/Treiberversion

Server Administrator-Homepage-Systemstrukturobjekte

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

System

Das **System**objekt enthält drei Hauptsystem-Komponentengruppen: Hauptsystemgehäuse , Software und Speicher. Die Homepage des Server Administrators wird automatisch auf der Ansicht des **System**objekts der Systemstrukturansicht geöffnet. Die meisten Verwaltungsfunktionen können vom Maßnahmenfenster des **System**objekts getätigt werden. Das Maßnahmenfenster des Objekts **System** kann die folgenden Register aufweisen, abhängig von den Gruppenzugriffsberechtigungen des Benutzers: **Eigenschaften**, **Herunterfahren**, **Protokolle**, **Warnungsverwaltung**, **Sitzungsverwaltung** und **Diagnose**.

ANMERKUNG: Aktualisierungsfunktionalität wird auf Versionen früher als Server Administrator-Version 2.0 unterstützt. Die Dell™ Server Update Utility und Dell Update Packages können von der Dell Support-Webseite unter **support.dell.com** heruntergeladen werden. Diese werden auf den Betriebssystemen Microsoft Windows ®, Red Hat® Enterprise Linux® und SUSE ® LINUX Enterprise Server unterstützt.

ANMERKUNG: Das Server-Aktualisierungsdienstprogramm von Dell oder Aktualisierungspakete von Dell müssen von dem System gestartet werden, das Sie aktualisieren möchten.

Eigenschaften

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

Im Register **Eigenschaften** können Sie:

- Sehen Sie nach dem aktuellen Warnungsfunktionszustand für Hardware- und Softwarekomponenten im Objekt **Hauptsystemgehäuse**, den verbundenen Speicherkomponenten.
- Die detaillierten Zusammenfassungen für alle Komponenten im überwachten System anzeigen.
- Die Bestandsinformationen für das überwachte System anzeigen und konfigurieren.
- Die automatischen Systemwiederherstellungsmaßnahmen (Watchdog-Zeitgeber) für das überwachte System anzeigen und einstellen.

  ANMERKUNG: Automatische Systemwiederherstellungsmaßnahmen werden eventuell nicht genau pro 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 und *h* das Heartbeat-Intervall darstellt. Der Wert des Heartbeat-Intervalls beträgt 7 Sekunden, wenn *n* <= 30 ist und 15 Sekunden, wenn *n* > 30 ist.

ANMERKUNG: Die Funktionalität der Watchdog-Zeitgeberfunktion kann in einem Fall, wo ein unbehebbares Speicherereignis im System DRAM Bank_1 auftritt, nicht garantiert werden. Wenn an diesem Ort ein unbehebbares 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 Herunterfahr- oder Neustartverhalten zu beeinflussen, funktioniert die Funktion eventuell nicht richtig. Wenn dies eintritt, müssen Sie das System manuell neu starten.

Herunterfahren

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

Im Register **Herunterfahren** können Sie:

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

ANMERKUNG: Ein temperaturbedingtes Herunterfahren erfolgt nur dann, wenn die vom Sensor gemeldete Temperatur über dem Temperaturschwellenwert liegt. Ein temperaturbedingtes Herunterfahren erfolgt nicht, wenn die vom Sensor gemeldete Temperatur unter dem Temperaturschwellenwert liegt.

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

ANMERKUNG: Server Administrator auch dann noch verfügbar und verwendet die Befehlszeilenoberfläche (CLI), wenn der DSM SA-Verbindungsdienst heruntergefahren ist. Die CLI-Funktionen erfordern keinen DSM SA-Verbindungsdienst.

ANMERKUNG: Der DSM SA-Verbindungsdienst fängt automatisch nach einem Neustart an, deshalb muss der DSM SA-Verbindungsdienst jedes Mal heruntergefahren werden, wenn ein System startet.

Protokolle

Unterregister: Hardware | **Warnung** | **Befehl**

Im Register **Protokolle** können Sie:

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

ANMERKUNG: Es wird empfohlen, dass Sie das Hardwareprotokoll löschen, wenn es 80-Prozent-Kapazität erreicht. Wenn dem Protokoll erlaubt wird, 100-Prozent-Kapazität zu erreichen, werden die spätesten Ereignisse vom Protokoll abgelegt.

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

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

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

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

Warnungsverwaltung

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

Im Register **Warnungsverwaltung** können Sie:

- Die aktuellen Warnungsmaßnahmen-Einstellungen sehen und die Warnungsmaßnahmen festlegen, die ausgeführt werden sollen, wenn ein Systemkomponentensensor einen Warnungs- oder Ausfallwert sendet.
- Die aktuellen Plattformereignisfilter-Einstellungen sehen 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, an das eine Warnung über ein Plattformereignis gesendet werden soll.
- Prüfen Sie die derzeitigen SNMP-Trap-Warnungsgrenzwerte und setzen Sie die Warnungsgrenzwerte für instrumentierte Systemkomponenten. Die ausgewählten Traps werden ausgelöst, wenn das System ein entsprechendes Ereignis bei dem ausgewählten Schweregrad erzeugt.

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

Sitzungsverwaltung

Unterregister: Sitzung

Im Register **Sitzungsverwaltung** können Sie:

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

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

Diagnose

Diagnose ist nicht mehr über den Server Administrator verfügbar. Um eine Systemdiagnose durchzuführen, installieren Sie Dell PowerEdge Diagnostics von Ihrer *Dell PowerEdge Service and Diagnostic Utilities*-CD oder laden Sie die Dell PowerEdge Diagnostics von der Dell Support-Webseite unter **support.dell.com** herunter und installieren dieses. Dell PowerEdge Diagnostics ist eine eigenständige Anwendung, die ohne die Installation des Server Administrators ausgeführt werden kann. Weitere Informationen finden Sie im *Dell PowerEdge Diagnostics-Benutzerhandbuch*.

Hauptsystemgehäuse

Durch Klicken auf das Objekt **Hauptsystemgehäuse** können Sie die wichtigen Hardware- und Softwarekomponenten des Systems verwalten. Die verfügbaren Komponenten sind:

- Netzstromschalter
- Batterien (verfügbar nur auf PowerEdge 1950-, 1955-, -, 2900- und 2950-Systemen)
- BIOS
- Lüfter
- Firmware
- Eingriff
- Speicher
- Netzwerk
- Schnittstellen
- Netzteile
- Prozessoren
- Remote-Zugriff
- Steckplätze
- Temperaturen
- Spannungen

ANMERKUNG: Netzstromschalter und werden nur in beschränkten Systemen angezeigt.

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

Eigenschaften

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

Im Register **Eigenschaften** können Sie:

- Den Zustand oder Status von Hardwarekomponenten und Sensoren anzeigen. Jede verzeichnete Komponente hat ein Symbol "Statusanzeigen der Systemkomponente" 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 Ausfall- (kritische) Bedingung für eine Komponente an, die einen sofortigen Eingriff erfordert. Eine Leerstelle ( ) bedeutet, dass der Zustand der Komponente unbekannt ist. Die verfügbaren überwachten Komponenten umfassen:
  - Netzstromschalter
  - Batterien (verfügbar nur auf PowerEdge 1950-, 1955-, -, 2900- und 2950-Systemen)
  - Stromzufuhr
  - Lüfter
  - Hardware-Protokoll
  - Eingriff
  - Speicher
  - Netzwerk
  - Netzteile
  - Prozessoren
  - Temperaturen
  - Spannungen

ANMERKUNG: Netzstromschalter und werden nur in beschränkten Systemen angezeigt.

- Informationen über die Attribute des Hauptsystemgehäuses anzeigen
- Detaillierte Informationen über die in Ihrem System eingebauten vor Ort austauschbaren Einheiten (FRUs) anzeigen (im Unterregister **Systemkomponenten (FRU)**). Bemerken Sie, dass nur die FRUs, die elektronische Teile-IDs besitzen, aufgeführt werden.
- Aktivieren oder deaktivieren Sie die Schaltflächen auf der Vorderseite des verwalteten Systems, und zwar den Netzschalter bzw. die Schaltfläche nicht-maskierbarer Interrupt (NMI) (falls in Ihrem System vorhanden).

Netzstromschalter

Durch das Klicken auf das Objekt **Netzstromschalter** können Hauptfunktionen des Netzstrom-Failover-Schalters des Systems angezeigt werden. Das Maßnahmenfenster des Objekts **Netzstromschalter** kann das folgende Register aufweisen, abhängig von den Gruppenzugriffsrechten des Benutzers: **Eigenschaften**.

Eigenschaften

Unterregister: Informationen

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

Batterien

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

Eigenschaften

Unterregister: Informationen

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

Warnungsverwaltung

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

BIOS

Durch Klicken auf das Objekt **BIOS** können Sie Schlüsselfunktionen des BIOS Ihres Systems 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 andere verschiedene Funktionen, wie z. B. Systemmeldungen, steuern. Das Maßnahmenfenster des **BIOS**-Objekts kann die folgenden Register aufweisen, abhängig von den Gruppenzugriffsrechten des Benutzers: **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.

ANMERKUNG: Durch das Einstellen der Startsequenz auf **Geräteliste** im Register **Setup** erfolgt die Startsequenz folgendermaßen: Diskette, IDE-CD-Laufwerk, Festplattenlaufwerk, optionale ROMs (wenn die Geräte zur Verfügung stehen).

Sie können den Zustand von vielen BIOS-Setup-Funktionen modifizieren, einschließlich, aber nicht beschränkt auf, die serielle Schnittstelle, Dual-Netzwerkschnittstellen-Controller-Karten, Startsequenz, benutzerzugängliche USB-Schnittstellen, CPU Virtualization Technology, CPU-Hyperthreading, Netzstromwiederherstellungsmodus, Integrierter SATA-Controller, Konsolenumleitung und Failsafe-BAUD-Rate der Konsolenumleitung.

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.

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

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

Stromzufuhr

Durch Klicken auf das Objekt **Stromzufuhr** können Sie die Stromzufuhrniveaus im System regeln. Der Server Administrator überwacht die Stromzufuhr in kritischen Komponenten an verschiedenen Gehäusestellen im überwachten System. Das Maßnahmenfenster des Objektes **Stromzufuhr** kann die folgenden Register aufweisen, abhängig von den Gruppenzugriffsrechten des Benutzers: **Eigenschaften** und **Warnungsverwaltung**.

Eigenschaften

Unterregister: Stromsonden

Im Register **Eigenschaften** können Sie:

- Die aktuellen Messungen und Status der Stromsonden des Systems anzeigen.
- Stromsonden-Warnungsschwellenwerte konfigurieren.
- Warnungsmaßnahmen einstellen, falls eine Stromsonde eine Warnung oder einen Fehlerwert zurückgeben sollte.

ANMERKUNG: Beim Zuweisen von Sondenschwellenwerten rundet Server Administrator die von Ihnen eingegebenen Mindest- oder Maximalwerte manchmal zu den am nächsten zuweisbaren Werten.

Warnungsverwaltung

Unterregister: Warnungsmaßnahmen | **SNMP-Traps**

Im Register **Warnungsverwaltung** können Sie:

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

Lüfter

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

Eigenschaften

Unterregister: Lüftersonden | **Lüftersteuerung**

Im Register **Eigenschaften** können Sie:

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

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

- Lüftersteuerungsoptionen auswählen.

Warnungsverwaltung

Unterregister: Warnungsmaßnahmen | **SNMP-Traps**

Im Register **Warnungsverwaltung** können Sie:

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

Firmware

Durch Klicken auf das Objekt **Firmware** können Sie die System-Firmware verwalten. Firmware besteht aus Programmen oder Daten, die in den ROM geschrieben wurden. Firmware kann ein Gerät starten und betreiben. Jeder Controller enthält Firmware, die hilft, die Funktionalität des Controllers bereit zu stellen. Das Maßnahmenfenster des **Firmware**-Objekts kann das folgende Register aufweisen, abhängig von den Gruppenzugriffsrechten des Benutzers: **Eigenschaften**

Eigenschaften

Unterregister: Informationen

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

Eingriff

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

Eigenschaften

Unterregister: Eingriff

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

Warnungsverwaltung

Unterregister: Warnungsmaßnahmen | **SNMP-Traps**

Im Register **Warnungsverwaltung** können Sie:

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

Speicher

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

Eigenschaften

Unterregister: Speicher

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

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

Warnungsverwaltung

Unterregister: Warnungsmaßnahmen | **SNMP-Traps**

Im Register **Warnungsverwaltung** können Sie:

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

Netzwerk

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

Eigenschaften

Unterregister: Informationen

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

Schnittstellen

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

Eigenschaften

Unterregister: Informationen

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

Netzteile

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

Eigenschaften

Unterregister: Elemente

Im Register **Eigenschaften** können Sie:

- Informationen über die Attribute der Netzteilredundanz anzeigen.
- Den Status der einzelnen Netzteilelemente prüfen.

Warnungsverwaltung

Unterregister: Warnungsmaßnahmen | **SNMP-Traps**

Im Register **Warnungsverwaltung** können Sie:

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

Prozessoren

Durch Klicken auf das Objekt Prozessoren können Sie den/die Mikroprozessor(en) des Systems verwalten. Ein Prozessor ist der primäre Rechenchip im Innern eines Systems, der die Auswertung und Ausführung von arithmetischen und logischen Funktionen steuert. Das Maßnahmenfenster des Objekts **Prozessor** kann die folgenden Register aufweisen, abhängig von den Gruppenzugriffsrechten 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 | **SNMP-Traps**

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

Remote-Zugriff

Durch Klicken auf das Objekt **Remote-Zugriff** können Sie die Baseboard-Verwaltungs-Controller (BMC)-Funktionen und Remote Access Controller-Funktionen verwalten.

Durch das Auswählen von BMC können Sie die BMC-Funktionen, wie z. B. allgemeine Informationen, über den BMC verwalten. Sie können auch die Konfiguration des BMC in einem LAN-Netzwerk, die serielle Schnittstelle für den BMC, Terminalmoduseinstellungen für die serielle Schnittstelle, BMC seriell über LAN und BMC-Benutzer verwalten.

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

Durch das Auswählen von DRAC können Sie auf die Remote-Systemverwaltungsfähigkeiten Ihres Systems zuzugreifen. Der Server Administrator DRAC gewährt Remote-Zugriff auf nicht arbeitsfähige Systeme, auf Warnungsmeldungen, wenn ein System außer Betrieb ist, und die Möglichkeit, ein System neu zu starten.

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

Eigenschaften

Unterregister: Informationen

Im Register **Eigenschaften** können Sie allgemeine BMC oder DRAC-Informationen anzeigen. Klicken Sie auf **Wieder auf Standardeinstellung stellen**, um alle Attribute wieder auf ihre Standardeinstellungen zurück zu stellen.

Konfiguration

Unterregister: LAN | **Serielle Schnittstelle** | **Seriell über LAN**

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

Unter dem Register **Konfiguration** kann Folgendes ausgeführt werden, wenn DRAC konfiguriert wird:

- Netzwerkeigenschaften konfigurieren.
- SNMP-Traps konfigurieren.

- Einträge für Wählen nach Bedarf konfigurieren.
- Einwählbenutzer konfigurieren.
- Konfigurieren Sie Remote-Eigenschaften wie Remote-Startparameter.
- Modemeigenschaften konfigurieren.

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

Benutzer

Unterregister: Benutzer

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

ANMERKUNG: Auf Dell PowerEdge *x9xx*-Systemen:

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

Steckplätze

Durch Klicken auf das Objekt **Steckplätze** können Sie die Anschlüsse oder Sockel auf der Hauptplatine verwalten, die gedruckte Leiterplatinen, z. B. Erweiterungskarten, aufnehmen. Das Objektmaßnahmenfenster **Steckplätze** befindet sich auf der Registerkarte **Eigenschaften**.

Eigenschaften

Unterregister: Informationen

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

Temperaturen

Durch Klicken auf das Objekt **Temperaturen** können Sie die Systemtemperatur regeln, um Hitzeschäden an den internen Systemkomponenten zu vermeiden. Der Server Administrator überwacht die Temperatur an verschiedenen Stellen im Systemgehäuse, um sicherzustellen, dass die Temperaturen im Gehäuse nicht zu hoch steigen. Das Maßnahmenfenster des **Temperatur**objekts kann die folgenden Register aufweisen, abhängig von den Gruppenzugriffsrechten des Benutzers: **Eigenschaften** und **Warnungsverwaltung**.

Eigenschaften

Unterregister: Temperatursonden

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

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

Warnungsverwaltung

Unterregister: Warnungsmaßnahmen | **SNMP-Traps**

Im Register **Warnungsverwaltung** können Sie:

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

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

Spannungen

Durch Klicken auf das Objekt **Spannungen** können Sie die Spannungsniveaus im System regeln. Der Server Administrator überwacht die Spannungen in kritischen Komponenten an verschiedenen Gehäusestellen im überwachten System. Das Maßnahmenfenster des **Spannungs**objekts kann die folgenden Register aufweisen, abhängig von den Gruppenzugriffsrechten des Benutzers: **Eigenschaften** und **Warnungsverwaltung**.

Eigenschaften

Unterregister: Spannungssonden

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

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

Warnungsverwaltung

Unterregister: Warnungsmaßnahmen | **SNMP-Traps**

Im Register **Warnungsverwaltung** können Sie:

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

Software

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

Eigenschaften

Unterregister: Zusammenfassung

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

Betriebssystem

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

Eigenschaften

Unterregister: Informationen

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

Speicher

Server Administrator enthält den Storage Management-Service:

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

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

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

Eigenschaften

Unterregister: Funktionszustand

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

Storage Management Service

Im Falle des Storage Management Service können Sie durch Klicken auf das Objekt **Speichermedien** den Status und die Einstellungen für die an das System angeschlossenen unterstützten Controller anzeigen. Das Controller-Objekt wird erweitert, um das an den Controller angeschlossene Speichergerät anzuzeigen.

Abhängig von den an das System angeschlossenen Controllern und Speichergeräten zeigt das erweiterte Objekt **Speichermedien** die folgenden Objekte niedriger Ebene:

- Controller
- Batterie
- Konnektor
- Gehäuse oder Rückwandplatine
- Physische Festplatten
- EMMs

- Lüfter
- Netzteile
- Temperaturen
- Virtuelle Festplatten
- Firmware-/Treiberversion

Das Maßnahmenfenster des Objekts **Speichermedien** kann die folgenden Register aufweisen, abhängig von den Gruppenzugriffsrechten des Benutzers: **Eigenschaften**

Eigenschaften

Unterregister: Funktionszustand

Im Fenster **Funktionszustand** des Registers **Eigenschaften** können Sie den aktuellen Funktionszustand oder den Status der angeschlossenen Speicherkomponenten anzeigen. Dieses Fenster zeigt den Status aller Objekte einer niedrigeren Ebene.

Ein schneller Weg, den Status aller Speicherkomponenten anzuzeigen, ist die Auswahl des Objekts **Speichermedien** und die Anzeige des Fensters **Funktionszustand** im Register **Eigenschaften**. Klicken Sie auf die erforderlichen Speicherkomponenten im Fenster **Funktionszustand**, um detaillierte Informationen über den Funktionszustand oder Status der Komponente anzuzeigen.

Unterregister: Informationen/Konfiguration

Im Fenster **Informationen/Konfiguration** des Registers **Eigenschaften** können Sie die Eigenschaften der an das System angeschlossenen Controller anzeigen. Sie können außerdem globale Tasks ausführen, die auf alle Controller angewendet werden.

Controller

Durch Klicken auf das Objekt **Controller** können Sie Informationen über die Controller und die verschiedenen, an den Controller angeschlossenen Komponenten anzeigen. Die an den Controller angeschlossenen Komponenten umfassen Batterien, virtuelle Laufwerke und so weiter. Das Maßnahmenfenster des Objekts **Controller** kann die folgenden Register aufweisen, abhängig von den Gruppenzugriffsrechten des Benutzers: **Funktionszustand** und **Informationen/Konfiguration**.

Funktionszustand

Im Register **Funktionszustand** können Sie den aktuellen Status der Batterie, der virtuellen Festplatten und anderer an den Controller angeschlossenen Speicherkomponenten anzeigen. Der Status wird mit Symbolen angezeigt, die in "Speicherkomponenten - Schweregrad " beschrieben werden.

Informationen/Konfiguration

Im Register **Informationen/Konfiguration** können Sie Eigenschaftsinformationen über den Controller und die an den Controller angeschlossenen Speicherkomponenten anzeigen. Sie können außerdem in diesem Register Controller-Tasks ausführen.

Konnektor

Durch klicken auf das Objekt **Kanal** können Sie Informationen über den an den Konnektor angeschlossenen Konnektor und das Gehäuse oder die Rückwandplatinen anzeigen. Das Maßnahmenfenster des Objekts **Konnektor** kann die folgenden Register aufweisen, abhängig von den Gruppenzugriffsberechtigungen des Benutzers: **Funktionszustand** und **Informationen/Konfiguration**

Funktionszustand

Im Register **Funktionszustand** können Sie den aktuellen Status der an den Konnektor angeschlossenen Gehäuse oder Rückwandplatinen anzeigen. Der Status wird mit Symbolen angezeigt, die in "Speicherkomponenten - Schweregrad " beschrieben werden.

Informationen/Konfiguration

Im Register **Konfiguration/Informationen** können Sie Eigenschaftsinformationen über den an den Konnektor angeschlossenen Konnektor und das Gehäuse oder die Rückwandplatinen anzeigen. Sie können außerdem in diesem Register Konnektor-Tasks ausführen.

Gehäuse oder Rückwandplatine

Durch klicken auf das Objekt **Gehäuse oder Rückwandplatine** können Sie Informationen über die physischen Festplatten, Temperatursonden und andere an das Gehäuse oder die Rückwandplatine angeschlossene Komponenten anzeigen. Das Maßnahmenfenster des Objekts **Gehäuse oder Rückwandplatine** kann die folgenden Register aufweisen, abhängig von den Gruppenzugriffsrechten des Benutzers: **Funktionszustand** und **Informationen/Konfiguration**

Funktionszustand

Im Register **Funktionszustand** können Sie den aktuellen Status der physischen Festplatten und andere an das Gehäuse oder die Rückwandplatine angeschlossenen Komponenten anzeigen. Ein Beispiel: Der Status eines Gehäuselüfters, des Netzteils, der Temperatursonden usw. werden in diesem Register angezeigt. Der Status der an die Rückwandplatine angeschlossenen physischen Festplatten wird hier ebenfalls angezeigt. Der Status wird mit Symbolen angezeigt, die in "Speicherkomponenten - Schweregrad " beschrieben werden.

Informationen/Konfiguration

Durch Klicken auf das Objekt **Informationen/Konfiguration** können Sie Informationen über die physischen Festplatten, EMMs (Gehäuseverwaltungs-Module) und andere an das Gehäuse oder die Rückwandplatine angeschlossenen Komponenten anzeigen. Bei Gehäusen können Sie außerdem in diesem Register Gehäuse-Tasks ausführen.

Physische Festplatten

Durch Klicken auf das Objekt **Physische Festplatten** können Sie Informationen über die an den Kanal angeschlossenen physischen Festplatten anzeigen. Das Maßnahmenfenster des Objekts **Physische Festplatten** kann die folgenden Register haben, abhängig von den Gruppenzugriffsrechten des Benutzers: **Informationen/Konfiguration**

Informationen/Konfiguration

Im Register **Informationen/Konfiguration** können Sie aktuelle Status- und Eigenschaftsinformationen über die an die Gehäuse oder Rückwandplatinen angeschlossenen physischen Festplatten anzeigen. Der Status wird mit Symbolen angezeigt, die in "Speicherkomponenten - Schweregrad " beschrieben werden.

Eigenschaftsinformationen umfassen Name, Zustand, Kapazität, verwendeter und verfügbarer Festplattenspeicherplatz sowie andere Informationen. Sie können außerdem in diesem Register Tasks der physischen Festplatte ausführen.

EMMs

Durch Klicken auf das Objekt **EMMs** können Sie grundlegende Informationen über Gehäuseverwaltungs-Module (EMMs) anzeigen. Das Maßnahmenfenster des Objekts **EMMs** kann das folgende Register aufweisen, abhängig von den Gruppenzugriffsrechten des Benutzers: **Informationen/Konfiguration**

Informationen/Konfiguration

Im Register **Informationen/Konfiguration** können Sie aktuelle Status- und Eigenschaftsinformationen der EMMS anzeigen. Der Status wird mit Symbolen angezeigt, die in "Speicherkomponenten - Schweregrad " beschrieben werden.

Eigenschafteninformationen umfassen Name, Zustand, Teilenummer, Firmware-Version und SCSI-Geschwindigkeit.

Lüfter

Durch Klicken auf das Objekt **Lüfter** können Sie Informationen über die Gehäuselüfter anzeigen. Das Maßnahmenfenster des Objekts **Lüfter** kann das folgende Register aufweisen, abhängig von den Gruppenzugriffsrechten des Benutzers: **Informationen/Konfiguration**

Informationen/Konfiguration

Im Register **Informationen/Konfiguration** können Sie aktuelle Status- und Eigenschaftsinformationen der Lüfter anzeigen. Der Status wird mit Symbolen angezeigt, die in "Speicherkomponenten - Schweregrad " beschrieben werden.

Eigenschafteninformationen umfassen Name, Zustand, Teilenummer, Firmware-Version und Geschwindigkeit.

Netzteile

Durch Klicken auf das Objekt **Netzteil** können Sie grundlegende Informationen über die Gehäuse-Netzteile anzeigen. Das Maßnahmenfenster des Objekts **Netzteile** kann folgende Register aufweisen, abhängig von den Gruppenzugriffsrechten des Benutzers: **Informationen/Konfiguration**

Informationen/Konfiguration

Im Register **Informationen/Konfiguration** können Sie aktuelle Status- und Eigenschaftsinformationen der Gehäuse-Netzteile anzeigen. Der Status wird mit Symbolen angezeigt, die in "Speicherkomponenten - Schweregrad " beschrieben werden.

Eigenschaftsinformationen umfassen Name, Zustand und Teilenummer.

Temperaturen

Durch Klicken auf das Objekt **Temperaturen** können Sie Informationen über die Gehäuse-Temperatursonden anzeigen. Das Maßnahmenfenster des Objekts **Temperaturen** kann das folgende Register aufweisen, abhängig von den Gruppenzugriffsrechten des Benutzers: **Informationen/Konfiguration**

Informationen/Konfiguration

Im Register **Informationen/Konfiguration** können Sie aktuelle Status- und Eigenschaftsinformationen der Gehäuse-Temperatursonden anzeigen. Der Status wird mit Symbolen angezeigt, die in "Speicherkomponenten - Schweregrad " beschrieben werden.

Eigenschafteninformationen umfassen Name, Status und den Messwert (aktuelle Temperatur). Die Minimium- und Maximumwerte der Temperatursonden für die **Warnungs-** und **Fehler**schwellenwerte werden ebenfalls in diesem Register angezeigt.

Virtuelle Festplatten

Durch Klicken auf das Objekt **Virtuelle Festplatten** können Sie Informationen über die auf dem Controller konfigurierten virtuellen Festplatten anzeigen. Das Maßnahmenfenster des Objekts **Virtuelle Festplatten** kann die folgenden Register aufweisen, abhängig von den Gruppenzugriffsrechten des Benutzers: **Informationen/Konfiguration**

Informationen/Konfiguration

Im Register **Informationen/Konfiguration** können Sie Eigenschaftsinformationen der auf dem Controller konfigurierten virtuellen Festplatten anzeigen. Eigenschaftsinformationen umfassen Name, Status und das Layout (RAID-Stufe). Die Regeln für Lesen, Schreiben und Cache sowie die Stripe-Größe werden ebenfalls angezeigt. Sie können außerdem in diesem Register Tasks der virtuellen Festplatte ausführen.

Firmware- / Treiberversion

Durch Klicken des Objekts **Firmware- / Treiberversion** können die Informationen über die Version des Treibers und der Firmware,die zurzeit auf dem Controller installiert sind, angezeigt werden. Die Firmware- und Treibereigenschaften können sich abhängig vom Modell des Controller ändern.

Firmware- und Treibereigenschaften können folgendes enthalten:

- Firmware-Version
- Minimale erforderliche Firmware-Version
- Treiberversion
- Minimale erforderliche Treiberversion

Speicherkomponenten - Schweregrad

Der Status einer Komponente wird in abgestuften Schweregraden eingeteilt. Für jeden Schweregrad müssen Sie unterschiedliche Maßnahmen einleiten. Ein Beispiel: Sie müssen sofort Reparaturmaßnahmen als Reaktion auf den Status **Warnung** oder **Kritisch / Fehler** einleiten, um Datenverluste zu vermeiden.

Es kann sinnvoll sein, das Warnungsprotokoll anzuzeigen und Ereignisse zu suchen, die angeben, warum eine Komponente den Status **Warnung** oder **Kritisch** hat. Weitere Informationen zum Beheben von Störungen finden Sie in der Online-Hilfe des Storage Management Service.

ANMERKUNG: Der angezeigte Status entspricht dem Status zu der Zeit, zu der der Browser die Seite erstmals angezeigt hat. Wenn Sie vermuten, dass sich der Status geändert hat und Sie die angezeigten Informationen aktualisieren wollen, klicken Sie auf die Schaltfläche **Aktualisieren** in der rechten oberen Ecke des Maßnahmenfensters. Eine Konfigurationsänderungen kann nur entdeckt werden, wenn Sie ein **Neu scannen** des Controllers ausführen; klicken Sie auf das Register **Informationen / Konfiguration** für den entsprechenden Controller und klicken Sie auf **Neu scannen**.

Tabelle 6-1 erklärt die verschiedenen Schweregrade und den entsprechenden Komponentenstatus.

Tabelle 6-1. Schweregrade und Komponentenstatus

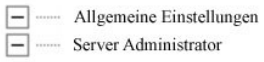
Schweregrad	Komponentenstatus
	**Normal / OK.** Die Komponente arbeitet wie erwartet.
	**Nichtkritisch / Warnung.** Eine Sonde oder ein anderes Überwachungsgerät hat einen Messwert für die Komponente erkannt, der sich über oder unter einem akzeptierten Wert befindet. Die Komponente wird noch funktionieren, kann aber ausfallen. Außerdem kann die Funktion der Komponente beeinträchtigt sein. Datenverluste sind möglich.
	**Kritisch / Fehlgeschlagen / Fehler.** Die Komponente hat bereits fehlerhaft gearbeitet oder ein Fehler steht unmittelbar bevor. Die Komponente benötigt sofortige Aufmerksamkeit und muss möglicherweise ersetzt werden. Es können bereits Datenverluste eingetreten sein.

Einstellungen verwalten: Konfigurationsoptionen der Homepage verwalten

Im linken Fenster der Startseite Einstellungen (in der die Systemstruktur auf der Startseite 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.

In Abbildung 6-2 werden verfügbare Konfigurationsoptionen der Einstellungen-Startseite dargestellt.

Abbildung 6-2. Konfigurationsoptionen der Voreinstellungen-Homepage verwalten



Allgemeine Einstellungen

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

Benutzer

Unterregister: Eigenschaften

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

Web-Server

Unterregister: Eigenschaften | X.509-Zertifikat

Im Register **Web Server** können Sie:

- DSM SA-Verbindungsdiensteinstellungen einstellen. Anleitungen zur Konfiguration Ihrer Servereinstellungen erhalten Sie unter "Dell Systems Management Server Administration-Verbindungsdienst und Sicherheitssetup".
- X.509-Zertifikatsverwaltung durchführen, indem Sie ein neues X.509-Zertifikat erstellen, ein vorhandenes X.509-Zertifikat wieder verwenden oder ein Stammzertifikat oder eine Zertifikatskette von einer Zertifizierungsstelle (CA) importieren. Weitere Informationen zur Zertifikatsverwaltung finden Sie unter "X.509-Zertifikatsverwaltung".

Server Administrator

Durch das Klicken auf das **Server Administrator**-Objekt kann der Zugriff von Benutzern mit Benutzer- oder Hauptbenutzerrechten aktiviert oder deaktivert und das SNMP-Stammkennwort konfiguriert werden. Das Maßnahmenfenster des Objekts **Server Administrator** kann die folgenden Register aufweisen, abhängig von den Gruppenzugriffsrechten des Benutzers: **Einstellungen**.

Einstellungen

Unterregister: Zugriffskonfiguration | SNMP-Konfiguration

Im Register **Einstellungen** können Sie:

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

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

- SNMP-Satzvorgänge konfigurieren.

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

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Einführung

Dell™ OpenManage™ Server Administrator: Benutzerhandbuch Version 5.2

Überblick

Der Server Administrator enthält eine umfassende 1:1-Systemverwaltungslösung auf zweierlei Art: von einer integrierten, Web-Browser-basierten graphischen Benutzeroberfläche (GUI) und von einer Befehlszeilenoberfläche (CLI) über das Betriebssystem. Der Server Administrator ist so ausgelegt, dass Systemadministratoren Systeme sowohl lokal als auch extern auf einem Netzwerk verwalten können. Server Administrator ermöglicht es den Systemadministratoren, sich auf die Verwaltung des gesamten Netzwerks zu konzentrieren, indem er eine umfassende 1:1-Systemverwaltung bietet.

ANMERKUNG: Für den Server Administrator kann ein System ein Stand-Alone-System, ein System mit verbundenen Netzwerkspeichereinheiten in einem separaten Gehäuse oder ein modulares System sein, das aus einem oder mehreren Servermodulen in einem Gehäuse besteht.

Der Server Administrator enthält Informationen über:

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

ANMERKUNG: Für die Remote-Wiederherstellung muss eine Dell™ Remote Access Controller-Karte installiert werden.

Integrierte Funktionen

Der Server Administrator bietet eine leicht anwendbare Verwaltung und Administration lokaler und Remote-Systeme über einen umfassenden Satz integrierter Verwaltungsdienste. Der Server Administrator ist die einzige Installation auf dem verwalteten System und ist sowohl lokal als auch extern über die Homepage des Server Administrators zugänglich. Zugriff auf entfernt überwachte Systeme kann über Einwählen, LAN oder drahtlose Verbindung erfolgen. Der Server Administrator gewährleistet die Sicherheit seiner Verwaltungsverbindungen über rollenbasierte Kontrolle (RBAC), Authentisierung und industriestandardmäßige sichere Sockelschichten-Verschlüsselung (SSL).

Installation

Server Administrator kann auf verschiedene Arten installiert werden. Die CD *Dell PowerEdge™ Installation and Server Management* bietet ein Setup-Programm für die Installation, die Aktualisierung und die Deinstallation von Server Administrator und anderen Managed System- und Management Station Software-Komponenten auf Ihrem verwalteten System. Die CD *Dell Systems Management*-Konsolen bietet ein Setup-Programm zum Installieren, Erweitern und Deinstallieren von Management Station Software-Komponenten auf Ihrer Verwaltungsstation. Zusätzlich können Sie den Server Administrator mittels einer unbeaufsichtigten Installation über ein Netzwerk auf mehreren System installieren.

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

ANMERKUNG: Weitere Informationen über die unbeaufsichtigte Server Administrator Installation/Deinstallation erhalten Sie im *Dell OpenManage™ Installations- und Sicherheitsbenutzerhandbuch*.

Um individuelle Systemkomponenten zu aktualisieren, verwenden Sie komponentenspezifische Dell Update Packages. Verwenden Sie die Anwendungs-CD Dell OpenManage Server Update Utility, um den vollständigen Versionsbericht einzusehen und das gesamte System zu aktualisieren. Server Update Utility ist eine CD-ROM-basierte Anwendung zur Identifizierung und Anwendung von Aktualisierungen für Ihren Server. Die Server Update Utility-Anwendung kann von **support.dell.com** heruntergeladen werden.

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

Server Administrator-Homepage

Die Startseite des Server Administrators bietet einfach einrichtbare und leicht anwendbare, Web-Browser-basierte Systemverwaltungs-Tasks vom verwalteten System oder von einem Remote-Host über ein LAN, einen DFÜ-Dienst oder ein drahtloses Netzwerk. Wenn der Dell Systems Management Server Administrator-Verbindungsdienst (DSM SA-Verbindungsdienst) installiert 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 Homepage des Server Administrators eine ausführliche, kontextabhängige Online-Hilfe.

Instrumentation Service

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

Remote Access Controller:

ANMERKUNG: Der Remote Access Controller ist auf modularen Systemen nicht verfügbar. Sie müssen direkt mit dem Dell Integrierten Remote-Zugriff-/Modularen Gehäuse-Controller (ERA/MC) auf einem modularen System verbinden. Weitere Informationen finden Sie im *Benutzerhandbuch für integrierten Dell Remote-Zugriff/MC*.

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

Storage Management Service

Der Storage Management Service enthält Speicherverwaltungsinformationen in einer integrierten Graphikansicht.

Der Storage Management Service von Server Administrator:

- Erlaubt die Anzeige des Status der lokalen und entfernten Speichermedien, die an das überwachte System angeschlossen sind.
- Unterstützt SCSI, SATA, ATA und SAS. Unterstützt keinen Fibre Channel.
- Das Ausführen von Controller- und Gehäusefunktionen bei allen unterstützten RAID- and Nicht-RAID-Controllern und -Gehäusen von einer einheitlichen graphischen oder Befehlszeilenoberfläche aus und ohne den Einsatz von BIOS-Dienstprogrammen.
- Schützt Daten durch das Konfigurieren von Datenredundanz, das Vergeben von Ersatzgeräten oder das Neu erstellen fehlerhafter Laufwerke.
- Enthält Funktionen zur Konfiguration des Speichers.

Auf unterstützten Microsoft® Windows®-Betriebssystemen wird Storage Management mithilfe des typischen Setups installiert.

Auf Systemen mit Red Hat® Enterprise Linux®- und SUSE® Linux Enterprise Server-Betriebssystemen können Sie entweder den Storage Management-Service über Red Hat Package Manager (RPM) installieren oder verwenden Sie das Skript `srvadmin-install.sh` - ein menügesteuertes Skript, welches die entsprechenden RPMs basierend auf den ausgewählten Optionen installiert.

Weitere Informationen über den Storage Management-Service erhalten Sie in der Storage Management-Onlinehilfe und dem *Dell OpenManage Server Administrator Storage Management-Benutzerhandbuch*. Informationen über das Starten der Online-Hilfe finden Sie unter "Anzeigen der Online-Hilfe."

HINWEIS: Dell OpenManage Array Manager wird nicht mehr unterstützt. Wenn Sie ein System (installiert mit Dell OpenManage 4.3 oder später) mit Array Manager installiert erweitern, wird Array Manager während des Upgrade-Verfahrens entfernt. Sie können stattdessen Storage Management verwenden.

ANMERKUNG: Installation von Storage Management ersetzt jede vorherige Installation des verwalteten Systems des Array Manager (Server-Software) und Konsole (Client-Software), die sich auf dem System befindet. Wenn nur die Array Manager-Konsole auf dem System installiert ist, dann ersetzt die Installation von Storage Management die Konsole von Array Manager nicht.

ANMERKUNG: Dell OpenManage Array Manager (für Management Station) ist unter Windows verfügbar, nur wenn vorherige Dell OpenManage Management Station Software (mit der installierten Array Manager-Konsole) entdeckt wird. Es ist nur für das Upgrade verfügbar.

Diagnostic Service

ANMERKUNG: Der Diagnose-Service steht nicht länger über den Server Administrator zur Verfügung.

Um eine Diagnose durchzuführen, installieren Sie Dell PowerEdge Diagnostics von der CD *Dell PowerEdge Service and Diagnostic Utilities* oder laden Sie die Dell PowerEdge Diagnostics von der Dell Support-Webseite unter **support.dell.com** herunter und installieren diese. Dell PowerEdge Diagnostics ist eine eigenständige Anwendung, die ohne die Installation des Server Administrators ausgeführt werden kann. Weitere Informationen finden Sie im *Dell PowerEdge Diagnostics-Benutzerhandbuch*.

Protokolle

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

Weitere nützliche Dokumente

Zusätzlich zu diesem *Benutzerhandbuch* können Sie die folgenden Handbücher entweder auf der Dell Support Website unter **support.dell.com** oder auf der *Dokumentations-CD* finden:

- Das *Dell OpenManage-Installations- und Sicherheitsbenutzerhandbuch* bietet vollständige Informationen über Installationsverfahren und schrittweise Anleitungen zur Installation, Erweiterung und Deinstallation von Server Administrator für alle unterstützten Betriebssysteme.
- Die *Installationsschnellanleitung für die Dell OpenManage-Software* enthält eine Übersicht der Anwendungen, die auf der Verwaltungsstation (Konsole) und auf den verwalteten Systemen installiert werden können, sowie Verfahren zur Installation von Konsolen- und verwalteten Systemen auf Systemen, die unterstützte Betriebssysteme ausführen.
- Das *Dell OpenManage Server Administrator-Kompatibilitätshandbuch* enthält Kompatibilitätsinformationen zu Server Administrator-Installation und -Betrieb

auf verschiedenen Hardwareplattformen (oder Systemen) unter unterstützten Microsoft Windows-, und Red HatEnterprise Linux- und SUSELINUX Enterprise Server-Betriebssystemen.

- Das *Dell OpenManage Server Administrator SNMP-Referenzhandbuch* enthält die SNMP-Verwaltungsinformations-Datenbank (MIB). Die SNMP-MIB definiert Variablen, die die Standard-MIB erweitern, so dass sie die Fähigkeiten von Systemverwaltungsagenten einschließt.
- Das *Dell OpenManage Server Administrator CIM-Benutzerhandbuch* dokumentiert den Allgemeines Informationsmodell (CIM)-Anbieter, eine Erweiterung der standardmäßigen Verwaltungsobjektformat (MOF)-Datei. Das CIM-Anbieter-MOF dokumentiert unterstützte Klassen von Verwaltungsobjekten.
- Das *Dell OpenManage Server Administrator Meldungs-Referenzhandbuch* enthält die Meldungen, die im Warnungsprotokoll auf der Homepage des Server Administrators oder auf der Ereignisanzeige des Betriebssystems angezeigt werden. Das Handbuch erklärt Text, Schweregrad und Ursache jeder Instrumentation Service-Warnmeldung, die vom Server Administrator ausgegeben wird.
- Das *Benutzerhandbuch für die Dell OpenManage Server Administrator Befehlszeilenschnittstelle* dokumentiert die gesamte Befehlszeilenschnittstelle (CLI) des Server Administrators, einschließlich einer Erklärung der CLI-Befehle zur Ansicht von Systemstatus, Zugriff auf Protokolle, Erstellen von Berichten, Konfigurieren verschiedener Komponentenparameter und Festlegen kritischer Schwellenwerte.
- Das *Dell PowerEdge Diagnostics-Benutzerhandbuch* bietet umfassende Informationen über die Installation und Verwendung von PowerEdge Diagnostics auf Ihrem System.
- Das *Dell OpenManage Baseboard-Verwaltungs-Controller-Dienstprogramm-Benutzerhandbuch* enthält zusätzliche Informationen über die Verwendung von Server Administrator zur Konfiguration und Verwaltung des System-BMC.
- Das *Benutzerhandbuch für Dell OpenManage Server Administrator Storage Management* ist ein umfassendes Nachschlagewerk für die Konfiguration und Verwaltung lokaler und externer, an ein System angeschlossener Speicherkomponenten.
- Das *Dell Remote Access Controller: Installations- und Setup-Handbuch* enthält vollständige Informationen über Installation und Konfiguration eines DRAC III-, DRAC III/XT- oder ERA/O-Controllers, Konfiguration eines ERA-Controllers und Verwendung eines RAC für Remote-Zugriff auf nicht betriebsfähige Systeme.
- Das *Benutzerhandbuch zum Dell Remote Access Controller / Racadm* finden Sie Informationen zur Verwendung des racadm-Befehlszeilen-Dienstprogramms.
- Das *Dell Remote Access Controller 4-Benutzerhandbuch* enthält vollständige Informationen über die Installation und Konfiguration eines DRAC 4-Controller und die Verwendung von DRAC 4 um im Remote-Zugriff auf ein inoperables System zuzugreifen.
- Das *Dell Remote Access Controller 5-Benutzerhandbuch* enthält vollständige Informationen über die Installation und Konfiguration eines DRAC 5-Controller und die Verwendung von DRAC 5 um im Remote-Zugriff auf ein inoperables System zuzugreifen.
- Das *Handbuch zum Dell integrierten Remote-Zugriff/MC-Controller* enthält vollständige Informationen zur Konfiguration und Verwendung des ERA/MC-Controllers zur Remote-Verwaltung und Überwachung des modularen Systems und seiner freigegebenen Ressourcen über ein Netzwerk.
- Das *Dell PowerEdge 1950 Systeme - Konfigurationshandbuch* enthält einen Überblick zur erstmaligen Einrichtung eines PowerEdge 1950-Systems.
- Das *Dell PowerEdge 1955 Systeme - Konfigurationshandbuch* enthält einen Überblick zur erstmaligen Einrichtung eines PowerEdge 1955-Systems.
- Das *Dell PowerEdge 2900 Systeme - Konfigurationshandbuch* enthält einen Überblick zur erstmaligen Einrichtung eines PowerEdge 2900-Systems.
- Das *Dell PowerEdge 2950 Systeme - Konfigurationshandbuch* enthält einen Überblick zur erstmaligen Einrichtung eines PowerEdge 2950-Systems.
- Das *Benutzerhandbuch zu Dell OpenManage Remote Install* enthält Informationen über unbeaufsichtigte, gleichzeitige Versorgungs- und Konfigurations-Lösungen über das Netzwerk durch Einsatz Image-basierter Technologie.
- Das *Benutzerhandbuch zu Dell Aktualisierungspaketen* enthält Informationen zum Erhalten und Verwenden von Dell Aktualisierungspaketen als Teil Ihrer Systemaktualisierungsstrategie.
- Das *Dell OpenManage Server-Aktualisierungsdienstprogramm-Benutzerhandbuch* bietet Informationen zum Erhalten und Verwenden des Server-Aktualisierungsdienstprogramms (SUU), um Ihren Dell PowerEdge-Server zu aktualisieren oder die Aktualisierungen einzusehen, die für alle im Repository aufgelisteten Server vorhanden sind.

Die CD *Dell PowerEdge Installations- und Server Management* enthält eine Infodatei für den Server Administrator und weitere Infodateien für die meisten Anwendungen auf der CD.

ANMERKUNG: Informationen über die Überwachung und Einstellung von Warnungen bei Server Administrator-Verfahren finden Sie im White Paper mit dem Titel *Überwachung der OpenManage Server Administrator-Dienste* unter **www.dell.com/openmanage**.

Wie Sie technische Unterstützung erhalten

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

Außerdem ist Dell Enterprise-Ausbildung und -Zertifizierung verfügbar; weitere Informationen finden Sie unter **www.dell.com/training**. Dieser Dienst wird unter Umständen nicht an allen Standorten angeboten.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Server Administrator-Protokolle

Dell™ OpenManage™ Server Administrator: Benutzerhandbuch Version 5.2

Überblick

Der Server Administrator ermöglicht die Ansicht und Verwaltung von Hardware-, Warnungs- und Befehlsprotokollen. Alle Benutzer können entweder von der Homepage des Server Administrators oder von seiner Befehlszeilenschnittstelle auf Protokolle zugreifen und Berichte drucken. Benutzer müssen mit Administrator-Berechtigungen angemeldet sein, um Protokolle löschen zu können, oder sie müssen mit Administrator- oder Hauptbenutzer-Berechtigungen angemeldet sein, um E-Mail-Protokolle an ihre designierten Dienstkontakte senden zu können.

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

Beim Anzeigen der Server Administrator-Protokolle können Sie auf der allgemeinen Navigationsleiste auf **Hilfe** klicken, um detaillierte Informationen über das Fenster zu erhalten, das gerade zu sehen ist. Server Administrator-Protokollhilfe ist in allen Fenstern verfügbar, die dem Benutzer zugänglich sind, basierend auf den entsprechenden Zugriffsrechten und den spezifischen Hardware- und Softwaregruppen, die der 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 jedes Datenfeldes durch ein benutzerdefiniertes Begrenzungszeichen getrennt sind) in einem von Ihnen bestimmten Ort zu speichern.
- Klicken Sie auf **E-Mail**, um eine E-Mail-Nachricht zu erstellen, die den Inhalt des Protokolls als Anhang mitsendet.
- 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" erhalten Sie weitere Informationen über die Task-Schaltflächen.

Server Administrator-Protokolle

Der Server Administrator enthält die folgenden Protokolle:

- Hardware-Protokoll
- Warnungsprotokoll
- Befehlsprotokoll

Hardware-Protokoll

Verwenden Sie das Hardware-Protokoll zur Suche nach potenziellen Problemen bei den Hardwarekomponenten des Systems. Auf Dell™ PowerEdge™ *x8xx* und *x9xx* Systeme ändert sich die Hardwareprotokoll-Statusanzeige zu kritischem Status ( ) wenn die Protokolldatei 100-Prozent-Kapazität erreicht. Abhängig vom jeweiligen System sind zwei Protokolle auf dem System verfügbar: das Protokoll für die integrierte Serververwaltung (ESM) und das Systemereignisprotokoll (SEL). Das ESM- und das SEL-Protokoll bestehen jeweils aus einem Satz von integrierten Anweisungen, die Hardwarestatusmeldungen an die Systemverwaltungssoftware senden können. Jede in den Protokollen verzeichnete Komponente hat ein Statusanzeige-Symbol 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 Ausfall- (kritische) Bedingung für eine Komponente an, die einen sofortigen Eingriff erfordert. Eine Leerstelle ( ) bedeutet, dass der Zustand der Komponente unbekannt ist.

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

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

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

Aufrechterhalten des Hardwareprotokolls

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

Warnungsprotokoll

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

Mit dem Warnungsprotokoll können verschiedene Systemereignisse überwacht werden. Der 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
- Datum und Uhrzeit, zu der das Ereignis erfasst wurde
- Die Kategorie des Ereignisses
- Eine Beschreibung des Ereignisses

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

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

Befehlsprotokoll

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

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

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

Im Befehlsprotokoll enthaltene Informationen umfassen:

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

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

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Mit dem Baseboard-Verwaltungs-Controller (BMC) arbeiten

Dell™ OpenManage™ Server Administrator: Benutzerhandbuch Version 5.2

Überblick

Der Dell™ PowerEdge™-Systems Baseboard-Verwaltungs-Controller (BMC) 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 unterstützt die Industriestandards bei Intelligent Platform Management Interfaces (IPMI), so dass Sie Systeme im Remote-Zugriff konfigurieren, überwachen oder wiederherstellen können.

Der Server Administrator ermöglicht den bandinternen Remote-Zugriff auf Ereignisprotokoll-, Stromsteuerungs- und Sensorstatusdaten, und er ermöglicht das Konfigurieren des BMC. Sie können den BMC über die graphische Benutzeroberfläche von Server Administrator verwalten, und zwar durch Klicken auf das Objekt **Remote-Zugriff**, welches eine Unterkomponente der Gruppe **Hauptsystemgehäuse** ist. Es können folgende Aufgaben ausgeführt werden, die mit dem BMC in Beziehung stehen:

- BMC-Basisinformationen ansehen
- BMC-Benutzer konfigurieren
- BMC-Plattformereignisfilter-Warnungen einstellen
- BMC in einer Seriell über LAN-Verbindung konfigurieren
- BMC in einer Seriellen Schnittstellenverbindung konfigurieren
- BMC in einer virtuellen LAN-Verbindung konfigurieren

In Dell PowerEdge *x8xx*- und *x9xx*-Systemen, sind BMC und RAC zu einem einzelnen Objekt kombiniert, welches als Remote-Zugriff bekannt ist (**System→ Hauptsystemgehäuse→ Remote-Zugriff**). Sie können BMC- oder RAC-Informationen basierend auf der Hardware ansehen, die die Remote-Zugriffsfähigkeiten für das System enthält.

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

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

ANMERKUNG: Sie können BMC-Daten nur auf Dell PowerEdge *x8xx*- und *x9xx*-Systemen ansehen. Auf anderen Systemen können Sie BMC nur installieren und deinstallieren. Eingeschränkte Sensordaten sind mit BMC oder ESM Dell PowerEdge *x6xx*- und *x7xx*-Systemen verfügbar.

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

BMC-Basisinformationen ansehen

Sie können die Basisinformationen des BMC ansehen und auch die BMC-Einstellungen auf deren Standardeinstellungen zurück setzen.

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

1. Klicken Sie auf das Objekt **System**.
2. Klicken Sie auf das Objekt **Hauptsystemgehäuse**.
3. Klicken Sie auf das Objekt **Remote-Zugriff**.

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

   - **BMC-Name**
   - **IPMI-Version**
   - **System-GUID**
   - **Anzahl von möglichen aktiven Sitzungen**
   - **Anzahl von aktuellen aktiven Sitzungen**
   - **IPMI-über-LAN aktiviert**

- **SOL aktiviert**
- **IP-Adressen-Quelle**
- **IP-Adresse**
- **IP-Subnetz**
- **IP-Gateway**
- **MAC-Adresse**

BMC-Benutzer konfigurieren

BMC-Benutzer können über die Seite **Remote-Zugriff** konfiguriert werden; auf diese Seite kann über den folgenden Pfad zugegriffen werden.

1. Klicken Sie auf das Objekt **System**.
2. Klicken Sie auf das Objekt **Hauptsystemgehäuse**.
3. Klicken Sie auf das Objekt **Remote-Zugriff**.
4. Klicken Sie auf das Register **Benutzer**.

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

   Im Fenster **Benutzerkonfiguration für Remote-Zugriff** können Sie einen bestimmten BMC-Benutzer konfigurieren.
6. 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.
7. Legen Sie folgende Benutzerberechtigungen fest:
   - Wählen Sie die maximalen Beschränkungen für LAN-Benutzerberechtigungsebenen.
   - Wählen Sie Maximale serielle Schnittstellen-Benutzerberechtigung gewährt.
   - Auf Dell PowerEdge *x9xx*-Systemen wählen Sie Seriell über LAN aktivieren aus, um Seriell über LAN zu aktivieren.
8. Klicken Sie auf **Änderungen anwenden** um Änderungen zu speichern.
9. Klicken Sie auf **Zurück zum Fenster Remote-Zugriffsbenutzer** um zum Fenster **Remote-Zugriffsbenutzer** zurückzukehren.

ANMERKUNG: Sechs zusätzliche Benutzereinträge sind konfigurierbar wenn RAC installiert ist. Dies läuft auf insgesamt 16 Benutzer hinaus. Dieselben Benutzername- und Kennwortregeln sind für BMC- und RAC-Benutzer anwendbar. Wenn DRAC 5 installiert ist, werden alle 16 Benutzereinträge RAC zugeteilt.

BMC-Plattformereignisfilter-Warnungen einstellen

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

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

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

ANMERKUNG: Sie müssen mit Administrator-Berechtigungen angemeldet werden, um die BMC Plattform-Ereignis-Filterwarnungen zu konfigurieren.

Sie können folgende Plattformereignisse konfigurieren.

- Lüftersonden-Fehler
- Spannungssonden-Fehler
- Diskreter Spannungssonden-Fehler
- Temperatursonden-Warnung
- Temperatursonden-Fehler
- Gehäuseeingriff festgestellt
- Redundanz herabgesetzt
- Redundanz verloren
- Prozessor nicht vorhanden
- Prozessorwarnung
- Prozessor-Fehler
- PS/VRM/DCtoDC-Warnung
- PS/VRM/Gleichspannungsumsetzer-Fehler
- Hardwareprotokollfehler
- Automatische Systemwiederherstellung
- Batteriesondenwarnung
- Batteriesondenfehler
- Netzteil nicht vorhanden

ANMERKUNG: Mit den Einstellungen unter Plattformereignisfilter-Warnungen aktivieren kann die Generierung von Plattformereignisfilter-Warnungen deaktiviert oder aktiviert werden. Diese Einstellungen ist unabhängig von den einzelnen Plattformereignis-Warnungseinstellungen.

ANMERKUNG: Auf Dell PowerEdge 1900-Systemen werden die Plattformereignisfilter **PS/VRM/D2D-Warnung, PS/VRM/D2D-Fehler,** und **Netzteil nicht vorhanden** nicht unterstützt, obwohl Server Administrator Ihnen erlaubt, diese Ereignisfilter zu konfigurieren.

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

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

5. Wählen Sie eine der folgenden Maßnahmen:

   - **Keine**
     Es wird keine Maßnahme eingeleitet, wenn das Betriebssystem hängt oder abgestürzt ist.
   - **System neu starten**
     Fährt das Betriebssystem herunter und initiiert einen Systemneustart, dabei wird das BIOS geprüft und das Betriebssystem neu geladen.
   - **System aus- und einschalten**
     schaltet die Stromversorgung des Systems ab, macht eine Pause, schaltet die Stromversorgung ein und startet das System neu. Das Aus- und Einschalten ist dann nützlich, wenn Systemkomponenten wie Festplatten neu initialisiert werden sollen.
   - **System ausschalten**
     schaltet die Stromversorgung des Systems ab.

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

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

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

7. Klicken Sie auf **Änderungen anwenden**.

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

Plattformereigniswarnungsziele einstellen

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

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

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

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

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

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

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

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

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

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

BMC für die Verwendung einer Seriell über LAN-Schnittstellenverbindung konfigurieren

Sie können den BMC für Datenübertragung einer Seriell über LAN (SOL)-Verbindung konfigurieren.

1. Klicken Sie auf das Objekt **System**.

2. Klicken Sie auf das Objekt **Hauptsystemgehäuse**.

3. Klicken Sie auf das Objekt **Remote-Zugriff**.

4. Klicken Sie auf das Register **Konfiguration**.

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

   Das Fenster **Seriell über LAN - Konfiguration** erscheint.

6. Konfigurieren Sie folgende Details:
   - **Seriell über LAN aktivieren**
   - **Baudrate**
   - **Erforderliche Mindestberechtigung**

7. Klicken Sie auf **Änderungen anwenden** .

8. Klicken Sie auf **Erweiterte Einstellungen**, um den BMC weiter zu konfigurieren.

9. Im Fenster **Seriell über LAN - Konfiguration - erweiterte Einstellungen** konfigurieren Sie die folgenden Informationen:
   - **Intervall der Zeichenakkumulation**
   - **Schwellenwert der gesendeten Zeichen**

10. Klicken Sie auf **Änderungen anwenden.**

11. Klicken Sie auf **Zurück zu Seriell über LAN - Konfiguration** um zum Fenster **Seriell über LAN - Konfiguration** zurückzukehren.

BMC für die Verwendung einer Seriellen Schnittstellenverbindung konfigurieren

Sie können den BMC für die Kommunikation über eine serielle Schnittstellenverbindung konfigurieren.

1. Klicken Sie auf das Objekt **System**.

2. Klicken Sie auf das Objekt **Hauptsystemgehäuse**.

3. Klicken Sie auf das Objekt **Remote-Zugriff**.

4. Klicken Sie auf das Register **Konfiguration**.
5. Klicken Sie auf **Serielle Schnittstelle**.

   Das Fenster **Konfiguration der seriellen Schnittstelle** erscheint.
6. Konfigurieren Sie folgende Details:
   - Verbindungsmoduseinstellung
   - Baudrate
   - Ablaufsteuerung
   - Beschränkung der Channel-Berechtigungsebene
7. Klicken Sie auf **Änderungen anwenden.**
8. Klicken Sie auf **Terminalmoduseinstellungen**.

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

   Der Terminalmodus wird für Intelligente Plattform Schnittstellenmanagement (IPMI)-Meldungen über die serielle Schnittstelle unter Verwendung von druckbaren ASCII-Zeichen benutzt. Der Terminalmodus unterstützt auch eine begrenzte Zahl an Textbefehlen für die Unterstützung von alten textbasierten Umgebungen. Diese Umgebung ist so gestaltet, dass ein einfaches Terminal oder ein Terminalemulator verwendet werden kann.
9. 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
10. Klicken Sie auf **Änderungen anwenden**.
11. Klicken Sie auf **Zurück zum Fenster Konfiguration der seriellen Schnittstelle** um zum Fenster **Konfiguration der seriellen Schnittstelle** zu wechseln.

BMC für die Verwendung einer LAN-Verbindung konfigurieren

Sie können den BMC für Datenübertragung über eine LAN-Verbindung konfigurieren

1. Klicken Sie auf das Objekt **System**.
2. Klicken Sie auf das Objekt **Hauptsystemgehäuse**.
3. Klicken Sie auf das Objekt **Remote-Zugriff**.
4. Klicken Sie auf das Register **Konfiguration**.
5. Klicken Sie auf **LAN**.

   Die Seite **LAN-Konfiguration** wird angezeigt.

   ANMERKUNG: BMC-Verwaltungsverkehr funktioniert nicht richtig, wenn der LAN auf der Hauptplatine (LOM) mit Netzwerkadapter-Add-In-Karten geteamt wird.
6. Konfigurieren Sie folgende NIC-Konfigurationsdaten:
   - 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 teamen.)
   - NIC-Auswahl
   - MAC-Adresse
   - IPMI-Über-LAN aktivieren
   - IP-Adressen-Quelle
   - IP-Adresse

- Subnetzmaske
- Gateway-Adresse
- Beschränkung der Channel-Berechtigungsebene
- Verschlüsselungsschlüssel (Diese Option ist auf Dell PowerEdge *x9xx* -Systemen verfügbar.)

7. Konfigurieren Sie die folgenden optionalen VLAN-Konfigurationsdetails:
   - VLAN-ID - aktiviert
   - VLAN-ID
   - Priorität
8. Klicken Sie auf **Änderungen anwenden.**

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Remote Access Controller:

Dell™ OpenManage™ Server Administrator: Benutzerhandbuch Version 5.2

Überblick

Der Server Administrator-Remote Access Controller stellt eine vollständige Remote System Management-Lösung für SNMP- und CIM-Systeme dar, die mit Dell™ Remote-Zugriffskarten (DRAC), DRAC III, DRAC III/XT, Integriertem Remote-Zugriff-Contoller (ERA), oder einer ERA-Option-Karte (ERA/O) ausgestattet sind. Diese Hardware- und Softwarelösungen werden allgemein DRACs (Dell Remote Access Controller) genannt. Mit DRAC 4 und DRAC 5 kann ein grundlegender Verwaltungs-Task, von Dell OpenManage Server Administrator ausgeführt werden: Sie können mit DRAC 4 oder DRAC 5 von der graphischen Benutzeroberfläche von Server Administrator abhängig von der installierten Karte von DRAC verbinden.

DRAC 4 und DRAC 5 sind Systems Management-Hardware und -Software-Lösungen, die gestaltet wurden, um Remote-Verwaltungsfähigkeiten, Wiederherstellung abgestürzter Systeme und Stromregelungsfunktionen für Dell PowerEdge™-Systeme anzubieten.

Durch Kommunikation mit dem Baseboard-Verwaltungs-Controller (BMC) des Systems können DRAC 4 und DRAC 5 für das Senden von E-Mail-Warnungen mit Warn- oder Fehlermeldungen über Spannung, Temperatur und Lüftergeschwindigkeit konfiguriert werden. DRAC 4 und DRAC 5 protokollieren außerdem Ereignisdaten und den letzten Bildschirm vor dem Absturz (nur auf Systemen erhältlich, die das Betriebssystem Microsoft® Windows® ausführen), um Ihnen bei der Diagnose der möglichen Ursachen eines Systemfehlers zu helfen.

Abhängig von Ihrem System, ist die DRAC 4-Hardware entweder eine Systemkarte (DRAC 4/I) oder eine kurze PCI-Karte (DRAC 4/P). DRAC 4/I und DRAC 4/P sind identisch bis auf die Hardware-Unterschiede.

Die DRAC 5-Hardware ist eine integrierte Systemkarte.

DRAC 4 und DRAC 5 haben eigene Mikroprozessoren und Speicher und werden über das System angetrieben, in dem sie installiert sind. DRAC 4 und DRAC 5 können auf dem System vorinstalliert werden oder sind separat als Bausatz erhältlich.

ANMERKUNG: Die Informationen in diesem Abschnitt gehören zu einer vorherigen DRAC-Generation. Weitere Informationen über die Verwendung von DRAC 4 erhalten Sie im *Dell Remote Access Controller 4: Benutzerhandbuch* und weitere Informationen über die Verwendung von DRAC 5 erhalten Sie im *Dell Remote Access Controller 5: Benutzerhandbuch*.

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

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

Informationen zum Ausführen des RAS-Dienstes von der Befehlszeile aus finden Sie im *Dell OpenManage Server Administrator-Befehlszeilenschnittstelle: Benutzerhandbuch* und im *Dell Remote Access Controller Racadm: Benutzerhandbuch*.

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

HINWEIS: Fragen Sie eine DRAC 5-Karte mit Server Administrator nicht ab oder konfigurieren Sie sie nicht im Remote-Zugriff oder lokal, wenn die Karte zurückgesetzt wird oder Firmware-Aktualisierung ausführt. Während des Reset wird die DRAC 5-Karte für kurze Zeit offline gesetzt. Wenn während dem Reset auf DRAC 5 zugegriffen wird, kann dies eventuell Probleme mit den auf der graphischen Benutzeroberfläche oder der Befehlszeilenschnittstelle (CLI) angezeigten Daten verursachen.

ANMERKUNG: Der Remote Access Controller ist auf modularen Systemen nicht verfügbar. Sie müssen direkt mit dem DRAC auf einem modularen System verbinden. Weitere Informationen finden Sie im *Benutzerhandbuch zum Dell integrierten Remote-Zugriff/MC-Controller*.

ANMERKUNG: Das *Dell Remote Access Controller: Installations- und Setup-Handbuch* enthält vollständige Informationen über Installation und Konfiguration eines DRAC III-, DRAC III/XT-, ERA- oder ERA/O-Controllers und Verwendung eines DRAC für Remote-Zugriff auf nicht betriebsfähige Systeme. Das *Handbuch zum Dell integrierten Remote-Zugriff/MC-Controller* enthält vollständige Informationen zur Konfiguration und Verwendung des ERA/MC-Controllers zur Remote-Verwaltung und Überwachung des modularen Systems und seiner freigegebenen Ressourcen über ein Netzwerk.

Hardware-Voraussetzungen

Das verwaltete System muss über einen installierten DRAC verfügen, um den Remote Access Controller verwenden zu können.

Eine Liste der besonderen Hardwareanforderungen für Ihren DRAC finden Sie in der Infodatei für Ihren Remote Access Controller auf der *CD Systems Management Consoles* und im *Installations- und Setup-Handbuch zum Dell Remote Access Controller* oder dem *Dell-Benutzerhandbuch für den Integrierten Remote-Zugriff/MC Controller* auf der Dokumentations-CD Datei für den Remote Access Controller.

ANMERKUNG: Die DRAC-Software wird als Teil der Installationsoptionen von **Typisches Setup** und **Benutzerdefiniertes Setup** installiert, wenn Managed System Software von der CD *Dell PowerEdge Installation and Server Management* installiert wird, unter der Bedingung, dass das verwaltete System alle Voraussetzungen zur DRAC-Installation erfüllt. Vollständige Software- und Hardwareanforderungen finden Sie in der entsprechenden DRAC-

Dokumentation.

Softwarevoraussetzungen

Auf dem verwalteten System muss die DRAC-Software installiert sein. Eine vollständige Liste mit Software-Installationsvoraussetzungen finden Sie im *Dell Remote Access Controller: Installations- und Setup-Handbuch* oder im *Benutzerhandbuch zum Dell integrierten Remote Access/MC-Controller*.

ANMERKUNG: Die DRAC-Software wird als Teil der Installationsoptionen von **Typisches Setup** und **Benutzerdefiniertes Setup** installiert, wenn Managed System Software von der CD *Dell PowerEdge Installation and Server Management* installiert wird, unter der Bedingung, dass das verwaltete System alle Voraussetzungen zur DRAC-Installation erfüllt. Vollständige Software- und Hardwareanforderungen finden Sie in der entsprechenden DRAC-Dokumentation.

DRAC-Benutzer hinzufügen und konfigurieren

ANMERKUNG: Sie müssen Administrator-Zugriffsrechte im Server Administrator haben, um den Remote Access Controller verwenden zu können.

Die DRAC kann Informationen für bis zu 16 Benutzer speichern. Der Remote Access Controller gewährt Sicherheit durch Abfrage von Benutzernamen und Kennwort, bevor eine Remote-Verbindung erstellt wird. Der Remote Access Controller kann auch Funkrufdienste zur Benachrichtigung von Benutzern im Falle eines Systemabsturzes, Stromausfalls oder des Auftretens eines in einer Liste spezifizierten Ereignisses bieten. Funkrufdienste stehen nur für DRAC III-Karten zur Verfügung.

ANMERKUNG: Manche Konfigurationsmöglichkeiten stehen nur für Systeme mit DRAC III, DRAC III/XT, ERA und ERA/O zur Verfügung und nicht für Systeme mit DRAC 4 oder DRAC 5. Um DRAC 4 oder DRAC 5 zu konfigurieren verwenden Sie die Option Starten Sie Remote-Verbindungsbenutzeroberfläche im Fenster RAC-Eigenschaften. Weitere Informationen über die Verwendung von DRAC 4 erhalten Sie im *Dell Remote Access Controller 4: Benutzerhandbuch* und weitere Informationen über die Verwendung von DRAC 5 erhalten Sie im *Dell Remote Access Controller 5: Benutzerhandbuch*.

Um einen DRAC-Benutzer zu erstellen, führen Sie folgende Schritte durch:

1. Klicken Sie auf der Startseite des Server Administrators auf das Objekt **Hauptsystemgehäuse** und dann auf das Objekt **Remote-Zugriff**.
2. Klicken Sie auf das Register **Benutzer**.

   Das Fenster **Remote-Zugriffsbenutzer** wird eingeblendet.
3. Klicken Sie auf **Hinzufügen**.

   Das Fenster **Remote-Zugriffsbenutzer hinzufügen** wird eingeblendet.
4. Geben Sie einen Benutzernamen in das Feld **Benutzername** ein.
5. Geben Sie ein neues Kennwort in das Feld **Neues Kennwort** ein.
6. Geben Sie das gleiche Kennwort in das Bestätigungsfeld **Kennwort bestätigen** ein.
7. Numerischen Funkruf konfigurieren (nur für DRAC III-Benutzer):
   a. Klicken Sie auf das Kontrollkästchen neben **Numerischen Funkruf aktivieren** und geben Sie eine Pager-Rufnummer in das Feld **Pager-Rufnummer** ein.
   b. Geben Sie die numerische Meldung in das Feld **Numerische Meldung** ein, das die DRAC senden soll, wenn sie bestimmte Ereignisse empfängt.
8. E-Mail-Funkruf konfigurieren:
   a. Klicken Sie auf auf das Kontrollkästchen neben **E-Mail-Funkruf aktivieren** und geben Sie eine E-Mail-Adresse in das Feld **E-Mail-Adresse** ein.
   b. Geben Sie die Meldung in das Feld **Meldung** ein, das die DRAC senden soll, wenn sie bestimmte Ereignisse empfängt.
9. Alphanumerischen Funkruf konfigurieren (nur für DRAC III-Benutzer):
   a. Klicken Sie auf das Kästchen neben **Alphanumerischen Funkruf aktivieren** und geben Sie eine Pager-Rufnummer in das Feld **Pager-Rufnummer** ein.
   b. Wählen Sie das von dem Pager-Dienstanbieter verwendete Protokoll **7E0** oder **8N1**.
   c. Wählen Sie die Baudrate für den Pager **300** oder **1200**.
   d. Geben Sie die Meldung in das Feld **Benutzerdefinierte Meldung** ein, das die DRAC senden soll, wenn sie bestimmte Ereignisse empfängt.
   e. Geben Sie die PIN des Pagers in das Feld **Pager-ID** und nötigenfalls ein Pager-Kennwort in das Feld **Pager-Kennwort** ein.
   f. Klicken Sie auf **Änderungen anwenden** im unteren Teil des Fensters.
10. Legen Sie unter **Schweregrad-Konfiguration** den Trap und den Schweregrad fest, den dieser besitzen muss, um eine Funkruf-Maßnahme von der DRAC auszulösen.

    Traps ermöglichen die Konfiguration der DRAC zur Reaktion auf Warnungsbedingungen von der integrierten Serververwaltung des Systems oder auf andere Bedingungen, wie z. B. Systemabstürze oder Stromausfälle.

Die erste (linke) Spalte mit Kontrollkästchen entspricht dem Schweregrad **Information**, die zweite Spalte entspricht dem Schweregrad **Warnung** und die dritte Spalte entspricht dem Schweregrad **Kritisch**. Die letzten sieben Ereignisse können nur den Schweregrad von **Information** berichten.

11. Klicken Sie auf **Änderungen anwenden** und dann auf **OK** zum Speichern von Warnung, Funkruf und Benutzerkonfiguration im Server Administrator Datenspeicher.

    Server Administrator kehrt zum Register **Benutzer** zurück. Der gerade erstellte und konfigurierte Benutzer wird in der Liste **Benutzername** angezeigt.

Vorhandenen DRAC-Benutzer konfigurieren

ANMERKUNG: Sie müssen Administrator-Zugriffsrechte im Server Administrator haben, um den Remote Access Controller verwenden zu können.

Um einen DRAC-Benutzer zu konfigurieren, führen Sie folgende Schritte durch:

1. Klicken Sie auf der Startseite des Server Administrators auf das Objekt **Hauptsystemgehäuse** und dann auf das Objekt **Remote Access Controller**.
2. Klicken Sie auf das Register **Benutzer**.

   Das Fenster **Remote-Zugriffsbenutzer** wird eingeblendet.
3. Klicken Sie auf den Benutzernamen für den zu konfigurierenden Benutzer.
4. Kennwort ändern:
   a. Wählen Sie das Kontrollkästchen neben **Kennwort ändern** und geben Sie ein neues Kennwort im Feld **Kennwort** ein.
   b. Geben Sie das gleiche Kennwort in das Bestätigungsfeld **Kennwort bestätigen** ein.
5. Numerischen Funkruf konfigurieren (nur für DRAC III-Benutzer):
   a. Wählen Sie das Kontrollkästchen neben **Numerischen Funkruf aktivieren** und geben Sie eine Pager-Rufnummer in das Feld **Pager-Rufnummer** ein.
   b. Geben Sie die numerische Meldung in das Feld **Numerische Meldung** ein, das die DRAC senden soll, wenn sie bestimmte Ereignisse empfängt.
6. E-Mail-Funkruf konfigurieren:
   a. Wählen Sie das Kontrollkästchen neben **E-Mail-Funkruf aktivieren** und geben Sie eine E-Mail-Adresse in das Feld **E-Mail-Adresse** ein.
   b. Geben Sie die Meldung in das Feld **Meldung** ein, das die DRAC senden soll, wenn sie bestimmte Ereignisse empfängt.
7. Alphanumerischen Funkruf konfigurieren (nur für DRAC III-Benutzer):
   a. Wählen Sie das Kästchen neben **Alphanumerischen Funkruf aktivieren** und geben Sie eine Pager-Rufnummer in das Feld **Pager-Rufnummer** ein.
   b. Wählen Sie das von dem Pager-Dienstanbieter verwendete Protokoll **7E0** oder **8N1**.
   c. Wählen Sie die Baudrate für den Pager **300** oder **1200**.
   d. Geben Sie die Meldung in das Feld **Benutzerdefinierte Meldung** ein, das die DRAC senden soll, wenn sie bestimmte Ereignisse empfängt.
   e. Geben Sie die PIN des Pagers in das Feld **Pager-ID** und nötigenfalls ein Pager-Kennwort in das Feld **Pager-Kennwort** ein.
   f. Klicken Sie auf **Änderungen anwenden** im unteren Teil des Fensters.
8. Legen Sie unter **Schweregrad-Konfiguration** den Trap und den Schweregrad fest, den dieser besitzen muss, um eine Funkruf-Maßnahme von der DRAC auszulösen.

   Traps ermöglichen die Konfiguration der DRAC zur Reaktion auf Warnungsbedingungen von der integrierten Serververwaltung des Systems oder auf andere Bedingungen, wie z. B. Systemabstürze oder Stromausfälle.

   Die erste (linke) Spalte mit Kontrollkästchen entspricht dem Schweregrad **Information**, die zweite Spalte entspricht dem Schweregrad **Warnung** und die dritte Spalte entspricht dem Schweregrad **Kritisch**. Die letzten sieben Ereignisse können nur den Schweregrad von **Information** berichten.
9. Klicken Sie auf **Änderungen anwenden** und dann auf **OK** zum Speichern von Warnung, Funkruf und Benutzerkonfiguration im Server Administrator Datenspeicher.

   Server Administrator kehrt zum Register **Benutzer** zurück.

DRAC-Netzwerkeigenschaften konfigurieren

ANMERKUNG: Sie müssen Administrator-Zugriffsrechte im Server Administrator haben, um den Remote Access Controller verwenden zu können.

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 zurückgesetzt werden, selbst wenn der IP-Adressenkonflikt durch Änderung der IP-Adresse des anderen NIC gelöst 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.

Zur Konfiguration der Netzwerkeigenschaften für die DRAC führen Sie folgende Schritte durch:

1. Klicken Sie auf der Startseite des Server Administrators auf das Objekt **Hauptsystemgehäuse** und dann auf das Objekt **Remote-Zugriff**.
2. Klicken Sie auf das Register **Konfiguration**.

   Das Fenster **Netzwerkeigenschaften konfigurieren** wird angezeigt.
3. Wählen Sie das Kontrollkästchen neben **NIC aktivieren** (diese Option ist standardmäßig ausgewählt).
4. Wenn das DHCP-System für die Zuweisung der NIC-Informationen aktiviert ist, wählen Sie das Kontrollkästchen neben **DHCP verwenden (Für NIC-IP-Adresse)**. Wenn Sie dies nicht wünschen, heben Sie die Auswahl dieses Kontrollkästchen auf und geben Sie die NIC-Informationen des DRAC in den Feldern **Statische IP-Adresse**, **Statische Subnetzmaske** und **Statische Gateway-Adresse** ein.
5. Einwähl-Netzwerkbetrieb aktivieren (nur für DRAC III-Benutzer):
   a. Wählen Sie das Kästchen neben **Einwählen aktivieren** (diese Option ist standardmäßig ausgewählt).
   b. Wenn das DHCP-System für die Zuweisung der Einwähl-Informationen aktiviert ist, wählen Sie das Kästchen neben **DHCP verwenden (Für Einwähl-IP-Adresse)**. Wenn Sie dies nicht tun, heben Sie die Markierung für dieses Kästchens auf und geben Sie die Basis-IP-Adresse des DRAC III-Modems in das Feld **Basis-IP-Adresse** ein.
   c. Legen Sie die Einstellungen von **Einwähl-Authentisierung** fest, die die Einwähl-Verbindungen erfordern:
      - **Beliebig** - Ermöglicht der Verbindung einen beliebigen Verschlüsselungstyp zu verwenden, einschließlich keine Verschlüsselung.
      - **Verschlüsselt** - Erfordert einen Verschlüsselungstyp für die Verbindung.
      - **CHAP** - Erfordert, dass die Verbindung CHAP verwendet.
6. Um die SMTP-Server-Adresssteuerung zu aktivieren, klicken Sie auf das Kontrollkästchen neben **SMTP aktivieren** und geben Sie die SMTP-Serveradresse in das Feld **SMTP (E-Mail)-Serveradresse** ein.
7. Klicken Sie auf **Änderungen anwenden** und dann auf **OK**, um die Änderungen zu speichern.

DRAC-Warnungseigenschaften konfigurieren

DRACs können zur Reaktion auf Warnungsbedingungen von der integrierten Serververwaltung des Systems oder auf andere Bedingungen wie z. B. Betriebssystemabstürze oder Stromausfälle konfiguriert werden.

DRACs bieten die folgenden Typen von Warnungsmaßnahmen:

- Alphanumerische Funkrufe (nur DRAC III) (Informationen zur Konfiguration dieses Warnungsmaßnahmentyps finden Sie unter "DRAC-Benutzer hinzufügen und konfigurieren".)
- Numerische Funkrufe (nur DRAC III) (Informationen zur Konfiguration dieses Warnungsmaßnahmentyps finden Sie unter "DRAC-Benutzer hinzufügen und konfigurieren".)
- E-Mail (Informationen über die Konfiguration dieses Warnungsmaßnahmentyps finden Sie unter "DRAC-Benutzer hinzufügen und konfigurieren".)
- SNMP-Traps (Informationen zur Konfiguration dieses Warnungsmaßnahmentyps finden Sie im folgenden Unterabschnitt).

SNMP-Warnungseigenschaften konfigurieren

ANMERKUNG: Sie müssen Administrator-Zugriffsrechte im Server Administrator haben, um den Remote Access Controller verwenden zu können.

Zur Konfiguration der Warnungseigenschaften des Remote Access Controller führen Sie folgende Schritte durch:

1. Klicken Sie auf der Startseite des Server Administrators auf das Objekt **Hauptsystemgehäuse** und dann auf das Objekt **Remote-Zugriff**.
2. Klicken Sie auf das Register **Konfiguration**.
3. Klicken Sie auf **SNMP**.
4. Klicken Sie auf **Hinzufügen** oder auf **Ziel-IP-Adresse**, um vorhandene SNMP-Warnungseigenschaften zu bearbeiten.

5. Wählen Sie das Kontrollkästchen neben **SNMP-Trap aktivieren**, falls es nicht bereits ausgewählt ist.

6. Geben Sie den SNMP-Community-Namen, zu der die Ziel-Verwaltungsstation gehört, in das Feld **Community** ein.

7. Geben Sie die Ziel-IP-Adresse der Verwaltungsstation ein, an die der DRAC seine SNMP-Traps senden soll, wenn ein Ereignis im Feld **IP-Adresse** erscheint.

8. Verwenden Sie die Kontrollkästchen unter **Schweregrad-Konfiguration** zur Festlegung der Ereignisse und des Schweregrads, die diese Ereignisse aufweisen müssen, um eine Warnungsmaßnahme vom DRAC auszulösen.

   Die erste (linke) Spalte mit Kontrollkästchen entspricht dem Schweregrad **Information**, die zweite Spalte entspricht dem Schweregrad **Warnung** und die dritte Spalte entspricht dem Schweregrad **Kritisch**. Die letzten sieben Ereignisse können nur den Schweregrad von **Information** berichten.

9. Klicken Sie auf **Änderungen anwenden** und dann auf **OK**, um die Änderungen zu speichern.

DRAC III Einwähl (PPP)-Benutzer- und Modemeinstellungen konfigurieren

Einwähl (PPP)-Benutzer- und Modemfunktionen sind derzeit nur für die DRAC III verfügbar.

DRAC III-Benutzer für Einwählen (PPP) hinzufügen und konfigurieren

ANMERKUNG: Sie müssen Administrator-Zugriffsrechte im Server Administrator haben, um den Remote Access Controller verwenden zu können.

In diesem Unterabschnitt wird beschrieben, wie ein Einwähl (PPP)-Benutzer hinzufügt und konfiguriert wird. Nachdem die Einwählbenutzer authentisiert sind, müssen Sie die DRAC-Benutzerauthentisierung im Anmeldebildschirm des Remote Access Controllers eingeben, um auf die DRAC III zugreifen zu können.

ANMERKUNG: Der Verwaltungssystem-PPP-Client des Server Administrator verwendet das 192.168.234.235-Netzwerk zur Kommunikation mit der installierten DRAC III. Es ist möglich, dass diese Netzwerk-IP-Adresse bereits auf anderen Systemen oder Anwendungen verwendet wird. In einem solchen Fall wird die PPP-Verbindung nicht funktionieren. Wenn diese Adresse bereits verwendet wird, muss der Benutzer die IP-Adresse des verwalteten System-PPP-Clients in eine andere Nummer ändern. Zur Änderung der IP-Adresse des verwalteten System-PPP-Servers zur Verwendung eines anderen Netzwerks, um Konflikte zu vermeiden, muss das Dienstprogramm racadm verwendet werden. Informationen zur Verwendung des racadm-Dienstprogramms erhalten Sie im *Dell Remote Access Controller Racadm-Benutzerhandbuch*.

Um Einwähl-Benutzer hinzuzufügen und zu konfigurieren, führen Sie folgende Schritte durch:

1. Auf der Startseite des Server Administrators, klicken Sie auf das Objekt **Hauptsystemgehäuse** und dann auf das Objekt **Remote-Zugriff**.

2. Klicken Sie auf das Register **Konfiguration**.

3. Klicken Sie auf **Einwähl-Benutzer.**

4. Klicken Sie auf **Hinzufügen**.

5. Geben Sie einen Benutzernamen in das Feld **Benutzername ein.**

6. Geben Sie ein neues Kennwort in das Feld **Kennwort** ein.

7. Geben Sie eine Rückrufnummer in das Feld **Rückrufnummer** ein.

   Diese Nummer wird dann vom Remote Access Controller angerufen, wenn **Rückruftyp** auf **Voreingestellt** eingestellt wird.

8. Wählen Sie eine Einstellung aus dem Drop-Down-Menü **Rückruftyp**.

   - **Keine** - Bei Anruf trennt der Remote Access Controller die Verbindung nicht und ruft nicht zurück; die Verbindung bleibt aktiv.
   - **Voreingestellt** - Wenn ein Anruf eingeht, dann unterbricht der Remote Access Controller den Anruf und ruft die im Feld **Rückrufnummer** angegebene Nummer an; diese Einstellung aktiviert die Rückrufnummernsteuerung.
   - **Benutzerdefiniert -** Bei einem Anruf fragt der Remote Access Controller den Benutzer nach der Rückrufnummer. Der Remote Access Controller trennt dann die Verbindung und ruft die vom Benutzer angegebene Nummer zurück.

9. Klicken Sie auf **Änderungen anwenden** und dann auf **OK**, um die Änderungen zu speichern.

DRAC III-Einträge für Wählen nach Bedarf hinzufügen und konfigurieren

ANMERKUNG: Sie müssen Administrator-Zugriffsrechte im Server Administrator haben, um den Remote Access Controller verwenden zu können.

Wenn Sie die Einwähl (PPP)-Einstellung auf **Voreingestellt** stellen, bewirkt der Eintrag für Wählen nach Bedarf, dass der Remote Access Controller die Verbindung trennt und die Verwaltungsstation unter einer voreingestellten Nummer zurückruft. Bei dem Rückruf müssen Sie die DRAC-Benutzerauthentisierung

zum Zugriff auf den RAS-Dienst verwenden.

ANMERKUNG: Die Software des verwalteten DRAC III-Systems verwendet eine PPP-Verbindung zur Kommunikation mit dem installierten DRAC. Die IP-Adresse für diese PPP-Verbindung ist 192.168.234.235. Es ist möglich, dass diese Netzwerk-IP-Adresse bereits auf anderen Systemen oder Anwendungen verwendet wird. In einem solchen Fall wird die PPP-Verbindung nicht funktionieren. Wenn diese Adresse bereits verwendet wird, muss der Benutzer die IP-Adresse des verwalteten System-PPP-Clients in eine andere Nummer ändern. Zur Änderung der IP-Adresse des verwalteten System-PPP-Servers zur Verwendung eines anderen Netzwerks, um Konflikte zu vermeiden, muss das Dienstprogramm racadm verwendet werden. Informationen zur Verwendung des racadm-Dienstprogramms erhalten Sie im *Dell Remote Access Controller Racadm-Benutzerhandbuch*.

Um einen Eintrag für Wählen nach Bedarf hinzuzufügen, führen Sie folgende Schritte durch:

1. Auf der Startseite des Server Administrators, klicken Sie auf das Objekt **Hauptsystemgehäuse** und dann auf das Objekt **Remote-Zugriff**.
2. Klicken Sie auf das Register **Konfiguration**.
3. Wählen Sie **Wählen nach Bedarf**
4. Klicken Sie auf **Hinzufügen**.
5. Geben Sie die die IP-Adresse der Verwaltungsstation ein, die der Remote Access Controller zurückruft, wenn er vom Benutzer angerufen wird.
6. Geben Sie die Telefonnummer in das Feld **Telefonnummer** ein, die das Modem des Systems verwendet.
7. Geben Sie den Benutzernamen für den 'Wählen nach Bedarf'-Benutzer im Feld **Benutzername** ein.
8. Geben Sie das Kennwort für den 'Wählen nach Bedarf'-Benutzer im Feld **Kennwort** ein.
9. Wählen Sie eine Einstellung aus dem Drop-Down-Menü **Authentisierung**.
   - **Beliebig** - Ermöglicht eine Verbindung mit einem beliebigen Verschlüsselungstyp, einschließlich keine Verschlüsselung.
   - **Verschlüsselt** - Erfordert einen Verschlüsselungstyp für die Verbindung.
   - **CHAP** - Erfordert, dass die Verbindung CHAP verwendet.
10. Klicken Sie auf **Änderungen anwenden** und dann auf **OK**, um die Änderungen zu speichern.

DRAC III Modemeinstellungen konfigurieren

ANMERKUNG: Sie müssen Administrator-Zugriffsrechte im Server Administrator haben, um den Remote Access Controller verwenden zu können.

Wenn der DRAC III-Einbausatz das optionale PCMCIA-Modem enthält, muss das Modem vor der Verwendung konfiguriert werden.

Zur Konfiguration eines DRAC III-Modems führen Sie folgende Schritte durch:

1. Auf der Startseite des Server Administrators, klicken Sie auf das Objekt **Hauptsystemgehäuse** und dann auf das Objekt **Remote-Zugriff**.
2. Klicken Sie auf das Register **Konfiguration**.
3. Klicken Sie auf **Modem**.
4. Wählen Sie für **Wählmodus** entweder **Impuls** oder **Ton**.
5. Wählen Sie das Land aus dem Drop-Down-Menü **Landesvorwahl** aus, in dem sich die DRAC III befindet.
6. Geben Sie für **Initialisierungs-Zeichenkette** die für die DRAC III erforderliche Initialisierungs-Zeichenkette ein.
7. Wählen Sie eine **Baudraten**-Einstellung aus dem Drop-Down-Menü (die Standardeinstellung ist **38400**).
8. Klicken Sie auf **Änderungen anwenden** und dann auf **OK**, um die Änderungen zu speichern.

DRAC-Remote-Funktionseigenschaften konfigurieren

ANMERKUNG: Sie müssen Administrator-Zugriffsrechte im Server Administrator haben, um den Remote Access Controller verwenden zu können.

Wenn das lokale Start-Image des verwalteten Systems beschädigt wurde, kann ein DRAC den Host-Server mit einem Diskettenstart-Image starten, das der RAC zuvor von einem einfache Dateiübertragungsprotokoll-Server (TFTP) herunterlädt. Diese Funktion wird Remote-Diskettenstart genannt. Ein DRAC kann auch die eigene Firmware mit einem Firmware-Image aktualisieren, das auf einem TFTP-Server gespeichert ist. Diese Funktion wird Remote-Firmware-Aktualisierung genannt. Das Verfahren ähnelt dem Aktualisieren eines System-BIOS.

Um die Funktionen Remote-Diskettenstart und Remote-Firmware-Aktualisierung Ihres DRAC zu konfigurieren, führen Sie folgende Schritte durch:

1. Klicken Sie auf der Startseite des Server Administrators auf das Objekt **Hauptsystemgehäuse** und dann auf das Objekt **Remote-Zugriff**.
2. Klicken Sie auf das Register **Konfiguration**.

   Das Fenster **Netzwerkeigenschaften konfigurieren** wird angezeigt.
3. Klicken Sie auf **Remote-Funktionen**.

   Das Fenster **Remote-Eigenschaften** wird eingeblendet.
4. Wählen Sie das Kontrollkästchen neben **Remote-Diskettenstart aktivieren**, um die Remote-Startparameter zu konfigurieren.
5. Remote-Startparameter der DRAC konfigurieren:
   a. Wählen Sie das Kontrollkästchen neben **Remote-Diskettenstart aktivieren**.
   b. Geben Sie die IP-Adresse des TFTP-Servers in das Feld **Remote-Diskette-TFTP-Adresse** ein.
   c. Geben Sie den Dateinamen des Start-Images in das Feld **Remote-Diskette-TFTP-Pfad** ein. Der Pfad muss relativ zum Stammverzeichnis des TFTP-Servers angegeben werden.
6. DRAC-Firmware-Aktualisierungsparameter konfigurieren:
   a. Wählen Sie das Kästchen neben **Remote-Firmware-Aktualisierung aktivieren**.
   b. Geben Sie die IP-Adresse des TFTP-Servers in das Feld **Remote-Firmware-TFTP-Adresse** ein.
   c. Geben Sie den Firmware-Image-Dateinamen in das Feld **Remote-Firmware-Aktualisierungspfad** ein. Der Pfad muss relativ zum Stammverzeichnis des TFTP-Servers angegeben werden.
7. Klicken Sie auf **Änderungen anwenden** und dann auf **OK**, um die Änderungen zu speichern.

DRAC-Sicherheit konfigurieren

ANMERKUNG: Sie müssen Administrator-Zugriffsrechte im Server Administrator haben, um den Remote Access Controller verwenden zu können.

ANMERKUNG: Im *Installations- und Setup-Handbuch für den Dell Remote Access Controller* finden Sie weitere Informationen über DRAC-Sicherheitsoptionen.

Um die DRAC-Sicherheit von der Server Administrator-Startseite zu konfigurieren, klicken Sie auf **System**→ **Hauptsystemgehäuse**→ **Remote-Zugriff** und klicken Sie auf das Register **Sicherheit**. Auf der Registerkarte **Sicherheit** können Sie die CSR-Zertifikatsverwaltung durchführen und die Authentisierungsoptionen für die RAC-Benutzeranmeldung festlegen.

ANMERKUNG: Einige der DRAC-Zertifikatsverwaltungsoperationen verwenden FTP-Protokolle für die Kommunikation mit der DRAC-Firmware. Wenn eine Firewall-Software auf Ihrem System installiert ist, können diese Operationen fehlschlagen.

Zertifikatsverwaltung

Verwenden Sie das Fenster **Zertifikatsverwaltung**, um eine Zertifikatsignierungsanforderung (CSR) zu erstellen, ein Server-Zertifikat oder eine Zertifizierungsstelle (CA) in die DRAC-Firmware zu laden oder um ein vorhandenes Server-Zertifikat oder CA-Zertifikat anzuzeigen. Im Fenster **Zertifikatsverwaltung** stehen folgende Optionen zur Verfügung:

- CSR erstellen
- Zertifikat hochladen
- Zertifikat anzeigen

Eine CSR ist eine digitale Bewerbung an eine CA um ein sicheres Server-Zertifikat. Sichere Server-Zertifikate sind erforderlich zur Sicherstellung der Identität eines entfernten Systems und zur Vergewisserung, dass mit dem entfernten System ausgetauschte Informationen von anderen weder gesehen noch geändert. Um die Sicherheit für den DRAC zu gewährleisten wird dringend empfohlen, eine CSR zu erstellen, die CSR an eine CA zu senden und das von der CA erhaltene Zertifikat hochzuladen.

Bei einer Zertifikatsvollmacht handelt es sich um ein Geschäftsunternehmen, das in der IT-Industrie auf Grund seiner hohen Standards bezüglich der zuverlässigen Sicherheitsüberprüfung, Identifizierung und weiterer Sicherheitskriterien bekannt ist. Beispiele für CAs sind Thwate und VeriSign. Sobald die CA die CSR empfangen hat, werden die in der CSR enthaltenen Informationen eingesehen und überprüft. Wenn der Bewerber den Sicherheitsstandards der CA genügt, wird für den Bewerber ein Zertifikat ausgestellt, das den Bewerber bei Übertragungen über Netzwerke oder über das Internet eindeutig identifiziert.

Nachdem die CA die CSR überprüft und ein Zertifikat gesendet hat, muss das Zertifikat zur DRAC-Firmware hochgeladen werden. Die in der DRAC-Firmware gespeicherten CSR-Informationen müssen mit den Informationen des Zertifikats übereinstimmen.

CSR erstellen

HINWEIS: Jede neue CSR überschreibt die vorherige CSR der Firmware. Es ist sehr wichtig, dass die CSR in der Firmware mit dem Zertifikat der CA übereinstimmt.

1. Wählen Sie im Fenster **Zertifikatsverwaltung** die Option **Neue CSR erstellen** und klicken Sie auf **Weiter**.

   Das Fenster **Zertifikatsignierungsanforderung erstellen** wird eingeblendet.

2. Geben Sie für jedes aufgelistete Attribut einen Wert ein oder wählen Sie einen Wert aus dem Drop-Down-Menü aus und klicken Sie auf **Erstellen**.

   Eine Meldung wird eingeblendet, dass die CSR erfolgreich erstellt wurde. Der Pfad, an dem die CSR gespeichert wurde, wird ebenfalls eingeblendet.

3. Jetzt kann die CSR an eine CA gesendet werden.

Zertifikat hochladen

Um Ihr Server-Zertifikat oder CA-Zertifikat zur DRAC-Firmware hochzuladen, muss das Zertifikat auf dem Host-Server des DRAC anwesend sein. Sie müssen den CSR-Typ, den genauen Dateinamen und den vollständigen Dateipfad zum Zertifikat auf dem Server bestimmen. Dann klicken Sie auf **Hochladen**.

ANMERKUNG: Es wird keine Warnmeldung angezeigt, wenn nicht der richtige Pfad für den Standort des Zertifikats auf dem Host-Server eingegeben wird.

1. Wählen Sie im Fenster **Zertifikatsverwaltung** die Option **Zertifikat hochladen** und klicken Sie auf **Weiter**.

   Das Fenster **Zertifikat hochladen** wird eingeblendet.

2. Wählen Sie einen Zertifikatstyp aus dem Drop-Down-Menü.

   Die Auswahloptionen sind **Server-Zertifikat** und **CA-Zertifikat**.

3. Geben Sie den genauen Pfad und den Dateinamen des Zertifikats an, das hochgeladen werden soll.

   ANMERKUNG: Wenn ein voll qualifizierter Pfad oder Dateiname angegeben wird, der Leerzeichen enthält, muss die Zeichenkette in Anführungszeichen angegeben werden. Wenn sich die Datei z. B. unter **c:\Sicherheit Dateien\Zertifikate\sslcert.cer** befindet, muss der voll qualifizierte Pfadname und Dateiname in Anführungszeichen angegeben werden, da sich zwischen "Sicherheit" und "Dateien" ein Leerzeichen befindet. Beispiel: `"c:\Sicherheit Dateien\Zertifikate\sslcert.cer"`

4. Klicken Sie auf **Hochladen**.

   Eine Meldung wird eingeblendet, dass das Zertifikat erfolgreich zur DRAC-Firmware hochgeladen wurde.

5. Starten Sie den DRAC neu, um das neue Zertifikat zu aktivieren.

ANMERKUNG: Nachdem das Zertifikat hochgeladen wurde, muss der DRAC zurückgesetzt werden, um sicherzustellen, dass das neue Zertifikat benutzt wird.

Zertifikat anzeigen

Die folgenden Informationen sind sowohl im Fenster **Server-Zertifikat anzeigen** als auch im Fenster **CA-Zertifikat anzeigen** enthalten. Siehe Tabelle 7-1.

Tabelle 7-1. Zertifikatsinformationen

Attribut	Wert
Typ	Zertifikatstyp, entweder ein Server-Zertifikat oder ein CA-Zertifikat
Seriennummer	Seriennummer des Zertifikats
Schlüsselgröße	Schlüsselgröße der Verschlüsselung
Gültig von	Ausstellungsdatum des Zertifikats
Gültig bis	Ablaufdatum des Zertifikats
Bewerber	Vom Bewerber eingegebene Zertifikatsattribute
Aussteller	Vom Aussteller zurückgegebene Zertifikatsattribute

Authentisierungsoptionen der Remote-Verbindung konfigurieren

Verwenden Sie das Fenster **Authentisierungsoptionen für Remote-Verbindung**, um Anmelde-Authentisierungsoptionen für DRAC-Benutzer einzustellen. Der DRAC kann so konfiguriert werden, dass die Anmeldung nur durch Benutzer erfolgen kann, die mit dem Remote Access Controller erstellt wurden (RAC-Benutzer), oder dass die DRAC-Anmeldung nur durch Benutzer erfolgen kann, die vom Remote Access Controller und über das lokale Betriebssystem erstellt

wurden.

1. Klicken Sie auf **System**→ **Hauptsystemgehäuse**→ **Remote-Zugriff** und dann auf das Register **Sicherheit**.

   Das Fenster **Zertifikatsverwaltung** wird eingeblendet.

2. **Klicken Sie auf** Authentisierungsoptionen.

   Das Fenster **Authentisierungsoptionen für Remote-Verbindung** wird eingeblendet. Es sind zwei Konfigurationsoptionen verfügbar, von denen jede durch ein Kontrollkästchen markiert werden kann.

   Das Kontrollkästchen **RAC-**Authentisierung ist standardmäßig ausgewählt und kann nicht deselektiert werden. Diese Einstellung ermöglicht die Anmeldung an den DRAC durch Benutzer, die über den erstellt wurden (DRAC-Benutzer).

   Wählen Sie das Kontrollkästchen **Lokale Betriebssystem-**Authentisierung, um die Anmeldung an den DRAC auch durch Benutzer zu ermöglichen, die über das lokale Betriebssystem erstellt wurden.

   ANMERKUNG: Das Kontrollkästchen für **Authentisierung des lokalen Betriebssystems** ist standardmäßig ausgegraut und kann für DRAC-Firmware-Version 3.20 oder später weder markiert noch abmarkiert werden. Verwenden Sie Active Directory-Authentisierung für DRAC-Firmware-Version 3.20 oder später. Informationen zum Verwenden von Microsoft Active Directory mit dem Dell Remote Access Controller (DRAC III, DRAC III/XT, ERA und ERA/O) erhalten Sie im *Dell Remote Access Controller: Installations- und Setup-Handbuch*.

3. Klicken Sie auf **Änderungen anwenden** und dann auf **OK**, um die Änderungen zu speichern.

Dell Remote Access Controller aktivieren und verwenden

Um das DRAC-**Anmeldefenster** des Remote Access Controller mit der Server Administrator-Homepage einzublenden, klicken Sie auf das Objekt **Hauptsystemgehäuse**, dann auf das Objekt **Remote Access Controller**, auf das Register **Remote-Verbindung** und dann auf **Remote-Verbindung**. Das DRAC-**Anmeldefenster** wird eingeblendet.

Nachdem Sie sich an den RAC angemeldet haben, können Sie Ihr System überwachen und verwalten, einschließlich des Zugriffs auf System- und Sitzungsinformationen, der Verwaltung der DRAC-Konfigurationen und Durchführung von Remote-Zugrifffunktionen auf dem verwalteten System. Anleitungen zur Verwendung eines DRAC finden Sie im *Dell Remote Access Controller: Installations- und Setup-Handbuch*.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Setup und Administration

Dell™ OpenManage™ Server Administrator: Benutzerhandbuch Version 5.2

Sicherheitsverwaltung

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

Rollenbasierte Zugriffsregelung

RBAC verwaltet Sicherheit, indem es die Vorgänge bestimmt, die von Personen in bestimmten Rollen ausgeführt werden können. Jedem Benutzer werden eine oder mehrere Rollen und jeder Rolle ein oder mehrere Benutzerberechtigungen zugewiesen, die Benutzern in der jeweiligen Rolle zustehen. Mit RBAC gleicht die Sicherheits-Administration sehr der Struktur einer Firma.

Benutzerberechtigungen

Der Server Administrator gewährt unterschiedliche Zugriffsrechte, basierend auf den dem Benutzer zugewiesenen Gruppenzugriffsrechten. Die drei Benutzerebenen sind: Benutzer, Hauptbenutzer und Administrator.

Benutzer können die meisten Informationen anzeigen.

Hauptbenutzer können Warnungsgrenzwerte einstellen und konfigurieren, welche Warnungsmaßnahmen ausgeführt werden sollen, wenn ein Warnungs- oder Fehlerereignis eintritt.

Administratoren können Maßnahmen zum Herunterfahren konfigurieren und durchführen, automatische Wiederherstellungsmaßnahmen konfigurieren, falls ein Betriebssystem auf einem System nicht mehr reagiert, und Hardware-, Ereignis- und Befehlsprotokolle löschen. *Administratoren* können das System auch konfigurieren, um E-Mails zu senden.

Der Server Administrator erteilt Nur-Lese-Zugriff an Benutzer, die mit *Benutzer*berechtigungen angemeldet sind, Lese- und Schreibzugriff an Benutzer mit *Hauptbenutzer*berechtigungen und Lese-, Schreib- und Administrator-Zugriffsrechte an Benutzer, die mit *Administrator*rechten angemeldet sind. Siehe Tabelle 3-1.

Tabelle 3-1. Benutzerberechtigungen

Benutzerberechtigungen	Zugriffstyp		
	Administrator	Schreiben	Lesen
Benutzer			X
Hauptbenutzer		X	X
Administrator	X	X	X

Lesen lässt die Ansicht von vom Server Administrator berichteten Daten zu. Lesezugriff lässt keine Änderung oder Einstellung von Werten auf dem verwalteten System zu.

Schreiben erlaubt Änderungen oder Einstellungen auf dem verwalteten System.

Administrator-Zugriff lässt außerdem das Herunterfahren des verwalteten Systems zu.

Berechtigungsebenen für den Zugriff auf Server Administrator-Dienste

In Tabelle 3-2 wird zusammengefasst, welche Benutzerebenen die Berechtigungen für den Zugriff auf die Server Administrator-Dienste sowie die Verwaltung dieser Dienste besitzen.

Tabelle 3-2. Server Administrator-Benutzerberechtigungsebenen

Dienst	Erforderliche Benutzerberechtigungsebene	

	Ansicht	Verwaltung
Instrumentation	B, H, A	H, A
Remote-Zugriff	B, H, A	A
Speicherverwaltung	B, H, A	A

In Tabelle 3-3 werden die Abkürzungen der in Tabelle 3-2 verwendeten Benutzerberechtigungsebenen definiert.

Tabelle 3-3. Legende der Server Administrator-Benutzerberechtigungsebenen

B	Benutzer
H	Hauptbenutzer
A	Administrator

Authentisierung

Das Server Administrator-Authentisierungsschema stellt sicher, dass die richtigen Zugriffstypen den korrekten Benutzerberechtigungen zugewiesen werden. Darüber hinaus validiert das Server Administrator-Authentisierungsschema den Kontext innerhalb dessen des gegenwärtige Verfahrens läuft, wenn die Befehlszeilenschnittstelle aufgerufen wird. Dieses Authentisierungsschema stellt sicher, dass alle Server Administrator-Funktionen, ob auf sie über die Homepage des Server Administrators oder über die CLI zugegriffen wird, korrekt authentisiert werden.

Microsoft Windows Authentisierung

Für unterstützte Microsoft® Windows®-Betriebssysteme verwendet Server Administrator-Authentifizierung integrierte Windows Authentication (früher NTLM genannt) zur Authentisierung. Dieses Authentifizierungssystem ermöglicht die Einschließung 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 basiert die Server Administrator-Authentifizierung auf der Pluggable Authentication Modules-Bibliothek (PAM). Benutzer können sich entweder lokal oder im Remote-Zugriff bei Server Administrator anmelden, indem verschieden Verwaltungsprotokolle, wie z. B. LDAP, NIS, Kerberos und Winbind verwendet werden.

ANMERKUNG: Server Administrator-Authentifizierung, die Winbind und Kerberos auf dem SUSE Linux Enterprise Server (Version 9 Service Pack 3) verwendet, wird nicht unterstützt, weil die kompatiblen 32-Bit-Bibliotheken für Winbind und Kerberos im Betriebssystem nicht vorhanden sind.

Verschlüsselung

Zugriff auf den Server Administrator erfolgt über eine sichere HTTPS-Verbindung mittels Secure Socket Layer-Technologie (SSL) zur Sicherung und zum Schutz der Identität des verwalteten Systems. Java Secure Socket Extension (JSSE) wird von unterstützten Microsoft Windows-, Red Hat Enterprise Linux- und SUSE® LINUX Enterprise-Betriebssystemen zum Schutz der Benutzeranmeldeinformationen und anderer Daten, die über die Socket-Verbindung übertragen werden, verwendet, wenn ein Benutzer auf die Startseite des Server Administrators zugreift.

Benutzerberechtigungen zuweisen

Allen Benutzern des Server Administrators müssen Benutzerberechtigungen zugewiesen werden, bevor der Server Administrator installiert wird, um die Sicherheit kritischer Systemkomponenten zu gewährleisten.

Die folgenden Verfahren enthalten schrittweise Anleitungen für die Einrichtung von Server Administrator-Benutzern und die Zuweisung von Benutzerrechten für jedes unterstützte Betriebssystem:

- "Server Administrator-Benutzer für unterstützte Microsoft Windows-Betriebssysteme erstellen"
- "Server Administrator-Benutzer für unterstützte Red Hat Enterprise Linux und SUSE LINUX Enterprise Server-Betriebssysteme erstellen"

HINWEIS: Jedem Benutzerkonto mit Zugriff auf den Server Administrator muss ein Kennwort zugeteilt werden, um den Zugriff auf die kritischen Systemkomponenten zu sichern. Zudem können sich Benutzer auf Grund von Einschränkungen des Betriebssystems ohne zugewiesenes Kennwort nicht am Server Administrator eines Systems anmelden, auf dem Windows Server® 2003 ausgeführt wird.

HINWEIS: Sie sollten Gästekonten für unterstützte Microsoft Windows-Betriebssysteme deaktivieren, um den Zugriff auf die kritischen Systemkomponenten zu kontrollieren. Weitere Informationen erhalten Sie unter Gastkonten und anonyme Konten in unterstützten Windows-Betriebssystemen deaktivieren

Server Administrator-Benutzer für unterstützte Microsoft Windows-Betriebssysteme erstellen

ANMERKUNG: Für diese Verfahren müssen Sie mit Administrator-Zugriffsrechten angemeldet sein.

Benutzer erstellen und Benutzerberechtigungen zuweisen in unterstützten Windows Server 2003-Betriebssystemen

ANMERKUNG: Bei Fragen über das Erstellen von Benutzern und Zuweisen von Benutzergruppenzugriffsrechten oder für detailliertere Anleitungen, lesen Sie die Dokumentation für das jeweilige Betriebssystem.

1. Klicken Sie auf die Schaltfläche **Start**, klicken Sie mit der rechten Maustaste auf **Arbeitsplatz** und klicken Sie auf **Verwalten**.
2. Erweitern Sie in der Konsolenstruktur **Lokale Benutzer und Gruppen** und klicken Sie auf **Benutzer**.
3. Klicken Sie auf **Maßnahme** und dann auf **Neuer Benutzer**.
4. Geben Sie die entsprechenden Informationen in das Dialogfeld ein, wählen Sie die entsprechenden Kontrollkästchen aus oder entfernen Sie die Häkchen wieder und klicken Sie auf **Erstellen**.

Jedem Benutzerkonto mit Zugriff auf den Server Administrator muss ein Kennwort zugeteilt werden, um den Zugriff auf die kritischen Systemkomponenten zu sichern. Zudem können sich Benutzer auf Grund von Einschränkungen des Betriebssystems ohne zugewiesenes Kennwort nicht am Server Administrator eines Systems anmelden, auf dem Windows Server 2003 ausgeführt wird.

5. Klicken Sie in der Konsolenstruktur unter **Lokale Benutzer und Gruppen** auf **Gruppen**.
6. Klicken Sie auf die Gruppe, der der neue Benutzer hinzugefügt werden soll: **Benutzer**, **Hauptbenutzer** oder **Administrator**.
7. Klicken Sie auf **Maßnahme** und dann auf **Eigenschaften**.
8. Klicken Sie auf **Hinzufügen**.
9. Klicken Sie auf **Namen prüfen**, um den Benutzernamen, den Sie hinzufügen, zu bestätigen.
10. Klicken Sie auf **OK**.

    Neue Benutzer können sich bei Server Administrator mit den Benutzerberechtigungen für ihre zugewiesene Gruppe anmelden.

Benutzer erstellen und Benutzerberechtigungen zuweisen in unterstützten Windows 2000-Betriebssystemen

ANMERKUNG: Bei Fragen über das Erstellen von Benutzern und Zuweisen von Benutzergruppenzugriffsrechten oder für detailliertere Anleitungen, lesen Sie die Dokumentation für das jeweilige Betriebssystem.

1. Klicken Sie mit der rechten Maustaste auf **Arbeitsplatz** und klicken Sie auf **Verwalten**.
2. Erweitern Sie in der Konsolenstruktur **Lokale Benutzer und Gruppen** und klicken Sie auf **Benutzer**.
3. Klicken Sie auf **Maßnahme** und dann auf **Neuer Benutzer**.
4. Geben Sie die entsprechenden Informationen in das Dialogfeld ein, wählen Sie die entsprechenden Kontrollkästchen aus oder entfernen Sie die Häkchen wieder und klicken Sie auf **Erstellen**.

Jedem Benutzerkonto mit Zugriff auf den Server Administrator muss ein Kennwort zugeteilt werden, um den Zugriff auf die kritischen Systemkomponenten zu sichern. Zudem können sich Benutzer auf Grund von Einschränkungen des Betriebssystems ohne zugewiesenes Kennwort nicht am Server Administrator eines Systems anmelden, auf dem Windows Server 2003 ausgeführt wird.

5. Klicken Sie in der Konsolenstruktur unter **Lokale Benutzer und Gruppen** auf **Gruppen**.
6. Klicken Sie auf die Gruppe, der der neue Benutzer hinzugefügt werden soll: **Benutzer**, **Hauptbenutzer** oder **Administrator**.
7. Klicken Sie auf **Maßnahme** und dann auf **Eigenschaften**.
8. Klicken Sie auf **Hinzufügen**.
9. Klicken Sie auf den Namen des hinzuzufügenden Benutzers und klicken Sie auf **Hinzufügen**.
10. Klicken Sie auf **Namen prüfen**, um den Benutzernamen, den Sie hinzufügen, zu bestätigen.
11. Klicken Sie auf **OK**.

    Neue Benutzer können sich bei Server Administrator mit den Benutzerberechtigungen für ihre zugewiesene Gruppe anmelden.

Benutzer zu einer Domäne hinzufügen

ANMERKUNG: Um Informationen über das Erstellen von Benutzern und Zuweisen von Benutzer-Gruppenzugriffsberechtigungen zu erhalten oder um weitere detaillierte Anleitungen zu erhalten, lesen Sie die Dokumentation für das jeweilige Betriebssystem.

ANMERKUNG: Für die Durchführung der folgenden Verfahren muss Microsoft Active Directory® auf dem System installiert sein.

1. Klicken Sie auf die Schaltfläche **Start** und gehen Sie dann auf **Systemsteuerung Verwaltung Active Directory Benutzer und Computer**.
2. In der Konsolenstruktur klicken Sie mit der rechten Maustaste auf **Benutzer**, oder Sie klicken mit der rechten Maustaste auf den Container, dem Sie den neuen Benutzer hinzufügen möchten, dann gehen Sie auf **Neuer Benutzer**.
3. Geben Sie die entsprechenden Benutzernameninformationen in das Dialogfeld ein und klicken Sie auf **Weiter**.

Jedem Benutzerkonto mit Zugriff auf den Server Administrator muss ein Kennwort zugeteilt werden, um den Zugriff auf die kritischen Systemkomponenten zu sichern. Zudem können sich Benutzer auf Grund von Einschränkungen des Betriebssystems ohne zugewiesenes Kennwort nicht am Server Administrator eines Systems anmelden, auf dem Windows Server 2003 ausgeführt wird.

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 am Server Administrator mit den Benutzerberechtigungen für ihre zugewiesene Gruppe und Domäne anmelden.

HINWEIS: Mit Active Directory müssen Sie, wenn Sie universelle Gruppen von getrennten Domänen hinzufügen, ein Zuordnungsobjekt mit universeller Reichweite erstellen. Die vom Dienstprogramm Dell™ Schema Extender erstellten Standardeinstellungszuordnungsobjekte sind lokale Domänenguppen und funktionieren nicht mit universellen Gruppen von anderen Domänen.

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

Administrator-Zugriffsrechte werden dem als root angemeldeten Benutzer zugewiesen. Zum Erstellen von Benutzern mit Benutzer- und Hauptbenutzerberechtigungen führen Sie folgende Schritte durch.

ANMERKUNG: Zur Durchführung dieser Verfahren müssen Sie als root angemeldet sein.

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 Zuweisen von Benutzer-Gruppenzugriffsberechtigungen zu erhalten oder um weitere detaillierte Anleitungen zu erhalten, lesen Sie die Dokumentation für das jeweilige Betriebssystem.

Benutzer mit Benutzerberechtigungen erstellen

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

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

   wobei <*Gruppe*> *nicht* Stamm 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.

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

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

Benutzer mit Hauptbenutzerberechtigungen erstellen

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

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

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

2. Geben Sie `passwd <Benutzername>` ein und drücken Sie <Eingabe>.

3. Wenn Sie dazu aufgefordert werden, geben Sie ein Kennwort für den neuen Benutzer ein.

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

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

Gastkonten und anonyme Konten in unterstützten Windows-Betriebssystemen deaktivieren

ANMERKUNG: Für dieses Verfahren müssen Sie mit Administrator-Zugriffsrechten angemeldet sein.

1. Wenn auf dem System Windows Server 2003 ausgeführt wird, klicken Sie auf die Schaltfläche **Start**, klicken Sie mit der rechten Maustaste auf **Arbeitsplatz** und klicken Sie auf **Verwalten**. Wenn auf dem System Windows 2000 ausgeführt wird, klicken Sie mit der rechten Maustaste auf **Arbeitsplatz** und klicken Sie auf **Verwalten**.

2. Erweitern Sie in der Konsolenstruktur **Lokale Benutzer und Gruppen** und klicken Sie auf **Benutzer**.

3. Klicken Sie auf das Systemnamenbenutzerkonto **Gast** oder **IUSR_**.

4. Klicken Sie auf **Maßnahme** und zeigen Sie auf **Eigenschaften**.

5. Wählen Sie **Konto ist deaktiviert** und klicken Sie auf **OK**.

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

SNMP-Agenten konfigurieren

Der Server Administrator unterstützt die Systemverwaltungsnorm einfaches Netzwerkverwaltungsprotokoll (SNMP) auf allen unterstützten Betriebssystemen. Der SNMP-Support ist abhängig von Ihrem Betriebssystem und wie das Betriebssystem installiert wurde installiert/nicht. 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. Weitere Informationen finden Sie unter "Installationsvoraussetzungen".

Sie können den SNMP-Agenten zur Änderung des Community-Namens, Aktivierung von Set-Vorgängen und Senden von Traps an eine Verwaltungsstation konfigurieren. Zur Konfiguration des SNMP-Agenten für die korrekte Interaktion mit Verwaltungsanwendungen, wie z. B. dem Dell OpenManage™ IT Assistant, führen Sie die im Folgenden beschriebenen Verfahren aus.

ANMERKUNG: Die Standardkonfiguration des SNMP-Agenten enthält normalerweise einen SNMP-Community-Namen wie z. b. **public**. Aus Sicherheitsgründen sollten Sie die SNMP Community-Namen von ihren Standardwerten ändern. Informationen zur Änderung von SNMP-Community-Namen erhalten Sie im entsprechenden untenstehenden Abschnitt. Zusätzliche Richtlinien erhalten Sie im Artikel **Securing an SNMP Environment (Eine SNMP-Umgebung sichern)** datiert Mai 2003 in der Zeitschrift Dell Power Solutions. Diese Zeitschrift ist auch unter **www.dell.com/powersolutions** erhältlich.

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

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

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

- SNMP-Agenten für Systeme konfigurieren, auf denen unterstützte Windows-Betriebssysteme ausgeführt werden
- SNMP-Agenten auf Systemen konfigurieren, auf denen unterstützte Red Hat Enterprise Linux-Betriebssysteme ausgeführt werden
- SNMP-Agenten auf Systemen konfigurieren, auf denen unterstützte Red Hat Enterprise SUSE LINUX-Server-Betriebssysteme ausgeführt werden

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, Aktivierung von Set-Vorgängen und Senden von Traps an eine Verwaltungsstation konfigurieren. Zur Konfiguration des SNMP-Agenten für die korrekte Interaktion mit Verwaltungsanwendungen wie dem IT Assistant führen Sie die im folgenden beschriebenen Verfahren aus.

ANMERKUNG: Konsultieren Sie die Dokumentation des Betriebssystems für zusätzliche Details über die SNMP-Konfiguration.

SNMP-Zugriff durch Remote Hosts aktivieren

Standardmäßig nimmt der Windows Server 2003 keine SNMP-Pakete von Remote Hosts an. Für Systeme mit Windows Server 2003 muss der SNMP-Dienst so konfiguriert werden, dass er SNMP-Pakete von Remote Hosts annimmt, wenn geplant ist, das System von Remote Hosts aus über SNMP-Verwaltungsanwendungen zu verwalten.

Damit ein System mit einem Windows Server 2003-Betriebssystem SNMP-Pakete von Remote Hosts empfangen kann, führen Sie folgende Schritte aus:

1. Klicken Sie auf die Schaltfläche **Start, klicken Sie mit der rechten Maustaste auf Arbeitsplatz und klicken Sie auf Verwalten**.

   Das Fenster **Computerverwaltung** wird angezeigt.

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

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

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

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

5. Klicken Sie auf das Register **Sicherheit**.

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

Die Konfiguration der SNMP-Community-Namens bestimmt, welche Systeme das System über SNMP verwalten kann. Der von Verwaltungsanwendungen verwendete SNMP-Community-Name muss mit einem SNMP-Community-Namen übereinstimmen, der auf dem Server Administrator-System konfiguriert wurde, so dass die Verwaltungsanwendungen Verwaltungsinformationen vom Server Administrator abrufen können.

1. Wenn auf dem System Windows Server 2003 ausgeführt wird, klicken Sie auf die Schaltfläche **Start**, klicken Sie mit der rechten Maustaste auf **Arbeitsplatz** und klicken Sie auf **Verwalten**. Wenn auf dem System Windows 2000 ausgeführt wird, klicken Sie mit der rechten Maustaste auf **Arbeitsplatz** und klicken Sie auf **Verwalten**.

   Das Fenster **Computerverwaltung** wird angezeigt.

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

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

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

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

5. Klicken Sie auf das Register **Sicherheit**, um einen Community-Namen hinzuzufügen oder zu ändern.

   a. Um einen Community-Namen hinzuzufügen, klicken Sie auf **Hinzufügen** unter der Liste **Akzeptierte Community-Namen**.

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

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

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

   c. Zum Ändern eines Community-Namens wählen Sie einen Community-Namen aus der Liste **Akzeptierte Community-Namen** aus und klicken Sie auf **Bearbeiten**.

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

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

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

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

SNMP-Set-Vorgänge aktivieren

SNMP-Set-Vorgänge müssen auf dem Server Administrator-System aktiviert sein, damit Server Administrator-Attribute mittels IT Assistant geändert werden können.

1. Wenn auf dem System Windows Server 2003 ausgeführt wird, klicken Sie auf die Schaltfläche **Start**, klicken Sie mit der rechten Maustaste auf **Arbeitsplatz** und klicken Sie auf **Verwalten**. Wenn auf dem System Windows 2000 ausgeführt wird, klicken Sie mit der rechten Maustaste auf **Arbeitsplatz** und klicken Sie auf **Verwalten**.

   Das Fenster **Computerverwaltung** wird angezeigt.

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

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

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

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

5. Klicken Sie auf das Register **Sicherheit,** um die Zugriffsrechte für eine Community zu ändern.

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

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

7. Legen Sie für die **Community-Rechte LESEN SCHREIBEN** oder **LESEN ERSTELLEN** fest und klicken Sie auf **OK**.

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

8. Klicken Sie auf **OK** zum Speichern der Änderung.

Das System auf das Senden von SNMP-Traps an eine Verwaltungsstation konfigurieren

Der Server Administrator erzeugt SNMP-Traps als Reaktion auf Änderungen im Status von Sensoren und anderen überwachten Parametern. Sie müssen ein oder mehrere Trap-Ziele auf dem Server Administrator-System konfigurieren, damit SNMP-Traps an eine Verwaltungsstation gesendet werden können.

1. Wenn auf dem System Windows Server 2003 ausgeführt wird, klicken Sie auf die Schaltfläche **Start**, klicken Sie mit der rechten Maustaste auf **Arbeitsplatz** und klicken Sie auf **Verwalten**. Wenn auf dem System Windows 2000 ausgeführt wird, klicken Sie mit der rechten Maustaste auf **Arbeitsplatz** und klicken Sie auf **Verwalten**.

   Das Fenster **Computerverwaltung** wird angezeigt.

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

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

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

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

5. Klicken Sie auf das Register **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 **Add to list (Zur Liste hinzufügen)** gleich neben dem Feld **Community-Name** .

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

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

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

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

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

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

Der Server Administrator verwendet die SNMP-Dienste, die vom ucd-snmp- oder net-snmp-SNMP-Agenten bereitgestellt werden. Sie können den SNMP-Agenten zur Änderung des Community-Namens, Aktivierung von Set-Vorgängen und Senden von Traps an eine Verwaltungsstation konfigurieren. Zur Konfiguration des SNMP-Agenten für die korrekte Interaktion mit Verwaltungsanwendungen wie dem IT Assistant führen Sie die im folgenden beschriebenen Verfahren aus.

ANMERKUNG: Konsultieren Sie die Dokumentation des Betriebssystems für zusätzliche Details über die SNMP-Konfiguration.

SNMP-Agent Access Control Konfiguration

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

Bei Red Hat Enterprise Linux-Betriebssystemen erlaubt die standardmäßige SNMP-Agent-Konfiguration lediglich einen Lesezugriff für die "öffentliche" Community, nur für den "System"-Zweig MIB-II (gekennzeichnet mit dem OID 1.3.6.1.2.1.1) der MIB-Struktur. Diese Konfiguration erlaubt es nicht, dass Verwaltungsanwendungen Informationen vom Server Administrator oder andere Systems Management-Informationen außerhalb des "System"-Zweigs MIB-II abrufen oder ändern.

Server Administrator SNMP Agent - Installationsmaßnahmen

Wenn der Server Administrator diese Standard-SNMP-Konfiguration während der Installation entdeckt, versucht er die SNMP-Agent-Konfiguration so zu ändern, dass die "öffentliche" Community einen Lesezugriff für die gesamte MIB- Struktur bekommt. Dazu ändert der Server Administrator die SNMP-Agent-Konfigurationsdatei **/etc/snmp/snmpd.conf** an zwei Stellen.

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

```
view all included .1
```

Mit der zweiten Änderung wird die Zeile für den Standard-"Zugriff" abgeändert, so dass die "öffentliche Community Lesezugriff auf die gesamte MIB-Struktur erhält. Der Server Administrator sucht folgende Zeile:

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

Wenn der Server Administrator die obenstehende Zeile findet, dann ändert er sie folgendermaßen ab:

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

Diese Änderungen an der standardmäßigen SNMP-Agent-Konfiguration erlauben der "öffentlichen" Community den Lesezugriff auf die gesamte MIB-Struktur.

ANMERKUNG: Damit sicher gestellt ist, dass der Server Administrator die SNMP-Agent-Konfiguration ändern kann, um einen korrekten Zugriff auf die Systems Management-Daten zu geben, wird empfohlen, etwaige andere SNMP-Agent-Konfigurationsänderungen erst nach Installation von Server Administrator vorzunehmen.

Server Administrator SNMP kommuniziert mithilfe des SNMP Multiplexing (SMUX)-Protokolls mit dem SNMP-Agenten. Wenn Server Administrator SNMP eine Verbindung mit dem SNMP-Agenten herstellt, sendet es einen Objekt-Bezeichner an den SNMP Agenten, um sich als ein SMUX-Peer zu identifizieren. Weil dieser Objekt-Bezeichner mit dem SNMP Agenten konfiguriert werden muss, fügt Server Administrator die folgende Zeile zur SNMP Agent-Konfigurationsdatei **/etc/snmp/snmpd.conf** während der Installation hinzu, falls diese noch nicht vorhanden ist:

```
smuxpeer .1.3.6.1.4.1.674.10892.1
```

SNMP-Community-Namen ändern

Die Konfiguration der SNMP-Community-Namens bestimmt, welche Systeme das System über SNMP verwalten kann. Der von Verwaltungsanwendungen verwendete SNMP-Community-Name muss mit einem SNMP-Community-Namen übereinstimmen, der auf dem Server Administrator-System konfiguriert wurde, so dass die Verwaltungsanwendungen Verwaltungsinformationen vom Server Administrator abrufen können.

Zum Ändern des SNMP-Community-Namens, der zum Abrufen von Verwaltungsinformationen von einem Server Administrator ausführenden System verwendet wird, bearbeiten Sie die SNMP-Agentenkonfigurationsdatei **/etc/snmp/snmpd.conf** und führen Sie folgende Schritte durch:

1. Suchen Sie die folgende Zeile:

   ```
   com2sec publicsec default public
   ```

   oder

   ```
   com2sec notConfigUser default public
   ```

2. Bearbeiten Sie diese Zeile und ersetzen Sie `public` durch den neuen SNMP-Community-Namen. Nach der Bearbeitung muss die Zeile wie folgt aussehen:

   ```
   com2sec publicsec default Community-Name
   ```

oder

```
com2sec notConfigUser default Community-Name
```

3. Zur Aktivierung von Änderungen an der SNMP-Konfiguration starten Sie den SNMP-Agenten neu durch Eingabe von:

```
service snmpd restart
```

SNMP-Set-Vorgänge aktivieren

SNMP-Set-Vorgänge müssen auf dem System aktiviert sein, auf dem Server Administrator ausgeführt wird, damit Server Administrator-Attribute mittels IT Assistant geändert werden können.

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

1. Suchen Sie die folgende Zeile:

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

oder

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

2. Bearbeiten Sie diese Zeile und ersetzen Sie das erste none durch all. Nach der Bearbeitung muss die Zeile wie folgt aussehen:

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

oder

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

3. Zur Aktivierung von Änderungen an der SNMP-Konfiguration starten Sie den SNMP-Agenten neu durch Eingabe von:

```
service snmpd restart
```

Das System auf das Senden von Traps an eine Verwaltungsstation konfigurieren

Der Server Administrator erzeugt 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 Verwaltungsstation gesendet werden können.

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

1. Fügen Sie der Datei die folgende Zeile hinzu:

```
trapsink IP_Adresse Community-Name
```

wobei *IP_address* die IP-Adresse der Verwaltungsstation ist und *community_name* der SNMP-Community-Name

2. Zur Aktivierung von Änderungen an der SNMP-Konfiguration starten Sie den SNMP-Agenten neu durch Eingabe von:

```
service snmpd restart
```

SNMP-Agenten auf Systemen konfigurieren, auf denen unterstützte Red Hat Enterprise SUSE LINUX-Server-Betriebssysteme ausgeführt werden

Der Server Administrator verwendet die SNMP-Dienste, die vom ucd-snmp- oder net-snmp-Agenten bereitgestellt werden. Sie können den SNMP Agenten konfigurieren, um SNMP-Zugriff von Remote-Hosts zu aktivieren, den Community-Namen zu ändern, Set-Vorgänge zu aktivieren und Traps an eine Verwaltungsstation zu senden. Zur Konfiguration des SNMP-Agenten für die korrekte Interaktion mit Verwaltungsanwendungen wie dem IT Assistant führen Sie die im folgenden beschriebenen Verfahren aus.

ANMERKUNG: Beim SUSE Linux Enterprise Server (Version 9) befindet sich die SNMP-Agenten-Konfigurationsdatei unter **/etc/snmpd.conf**. Beim SUSE Linux Enterprise Server (Version 10) befindet sich die SNMP-Agenten-Konfigurationsdatei unter **/etc/snmp.conf**.

ANMERKUNG: Konsultieren Sie die Dokumentation des Betriebssystems für zusätzliche Details über die SNMP-Konfiguration.

Server Administrator SNMP - Installationsmaßnahmen

Server Administrator SNMP kommuniziert mithilfe des SNMP Multiplexing (SMUX)-Protokolls mit dem SNMP-Agenten. Wenn Server Administrator SNMP eine Verbindung mit dem SNMP-Agenten herstellt, sendet es einen Objekt-Bezeichner an den SNMP Agenten, um sich als ein SMUX-Peer zu identifizieren. Dieser

Objekt-Bezeichner muss mit dem SNMP Agenten konfiguriert werden, deshalb fügt Server Administrator während der Installation die folgende Zeile zur SNMP-Agenten-Konfigurationsdatei (**/etc/snmpd.conf** oder **/etc/snmp/snmpd.conf**) hinzu, falls diese noch nicht vorhanden ist:

```
smuxpeer .1.3.6.1.4.1.674.10892.1
```

SNMP-Zugriff von Remote Hosts aktivieren

Die Standard-SNMP Agent-Konfiguration auf SUSE LINUX Enterprise Server-Betriebssystemen gibt nur schreibgeschützten Zugriff auf die komplette MIB-Struktur an die "public" Community vom lokalen Host. Mit dieser Konfiguration können SNMP Verwaltungsanwendungen wie IT Assistant, die auf anderen Hosts ausgeführt werden, Server Administrator-Systeme nicht richtig ermitteln und verwalten. Wenn Server Administrator diese Konfiguration während der Installation feststellt, protokolliert es eine Nachricht an die Betriebssystem-Protokolldatei **/var/log/messages**, um anzuzeigen, dass der SNMP-Zugriff zum lokalen Host eingeschränkt wird. Sie müssen den SNMP Agenten konfigurieren, um SNMP-Zugriff von Remote Hosts zu aktivieren, wenn Sie planen, das System mithilfe von SNMP-Verwaltungsanwendungen von Remote-Hosts zu verwalten.

ANMERKUNG: Aus Sicherheitsgründen ist es ratsam, den SNMP-Zugriff auf bestimmte Remote-Hosts soweit wie möglich einzuschränken.

Um den SNMP- Zugang von einem bestimmten Remote-Host zu einem System zu aktivieren, das Server Administrator ausführt, bearbeiten Sie die SNMP-Agenten-Konfigurationsdatei **/etc/snmpd.conf** oder **/etc/snmp/snmpd.conf** und führen folgende Schritte durch:

1. Suchen Sie die folgende Zeile:

   ```
   rocommunity public 127.0.0.1
   ```

2. Bearbeiten oder kopieren Sie diese Zeile, indem Sie 127.0.0.1 mit der Remote-Host-IP-Adresse ersetzen. Nach der Bearbeitung muss die Zeile wie folgt aussehen:

   ```
   rocommunity public IP_Adresse
   ```

   ANMERKUNG: Sie können SNMP-Zugriff von mehrfachen spezifischen Remote-Hosts aktivieren, indem Sie eine `rocommunity`-Direktive für jeden Remote-Host hinzufügen.

3. Zur Aktivierung von Änderungen an der SNMP-Konfiguration starten Sie den SNMP-Agenten neu durch Eingabe von:

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

Um den SNMP- Zugang von allen Remote-Hosts zu einem System zu aktivieren, das Server Administrator ausführt, bearbeiten Sie die SNMP-Agenten-Konfigurationsdatei **/etc/snmpd.conf** oder **/etc/snmp/snmpd.conf** und führen folgende Schritte durch:

1. Suchen Sie die folgende Zeile:

   ```
   rocommunity public 127.0.0.1
   ```

2. Bearbeiten Sie diese Zeile indem Sie 127.0.0.1 löschen. Nach der Bearbeitung muss die Zeile wie folgt aussehen:

   ```
   rocommunity public
   ```

3. Zur Aktivierung von Änderungen an 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, so dass die Verwaltungsanwendungen Verwaltungsinformationen vom Server Administrator abrufen können.

Zum Ändern des Standard-SNMP-Community-Namens, der zum Abrufen von Verwaltungsinformationen von einem Server Administrator ausführenden System verwendet wird, bearbeiten Sie die SNMP-Agentenkonfigurationsdatei **/etc/ /snmpd.conf** oder **/etc/snmp/snmpd.conf**und führen Sie folgende Schritte aus:

1. Suchen Sie die folgende Zeile:

   ```
   rocommunity public 127.0.0.1
   ```

2. Bearbeiten Sie diese Zeile indem Sie `public` durch den neuen SNMP-Community-Namen ersetzen. Nach der Bearbeitung muss die Zeile wie folgt aussehen:

   ```
   rocommunity community_name 127.0.0.1
   ```

3. Zur Aktivierung von Änderungen an der SNMP-Konfiguration starten Sie den SNMP-Agenten neu durch Eingabe von:

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

SNMP-Set-Vorgänge aktivieren

SNMP-Set-Vorgänge müssen auf dem System aktiviert sein, auf dem Server Administrator ausgeführt wird, damit Server Administrator-Attribute mittels IT Assistant geändert werden können. Um Remote-Herunterfahren eines Systems von IT Assistant zu aktivieren, müssen SNMP Set-Vorgänge aktiviert sein.

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

Um SNMP Set-Vorgänge in einem System zu aktivieren, das Server Administrator ausführt, bearbeiten Sie die SNMP-Agenten-Konfigurationsdatei **/etc/snmpd.conf** oder **/etc/snmp/snmpd.conf** und führen folgende Schritte durch:

1. Suchen Sie die folgende Zeile:

   ```
   rocommunity public 127.0.0.1
   ```

2. Bearbeiten Sie diese Zeile indem Sie `rocommunity` mit `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
   ```

Das System auf das Senden von Traps an eine Verwaltungsstation konfigurieren

Der Server Administrator erzeugt 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 Verwaltungsstation gesendet werden können.

Um Ihr System, das Server Administrator ausführt, so zu konfigurieren, dass Traps an eine Management Station gesendet werden, bearbeiten Sie die SNMP-Agenten-Konfigurationsdatei **/etc/snmpd.conf** oder **/etc/snmp/snmpd.conf** und führen folgende Schritte durch:

1. Fügen Sie der Datei die folgende Zeile hinzu:

   ```
   trapsink IP_Adresse Community-Name
   ```

   wobei `IP_address` die IP-Adresse der Verwaltungsstation ist und `community_name` der SNMP-Community-Name

2. Zur Aktivierung von Änderungen an der SNMP-Konfiguration starten Sie den SNMP-Agenten neu durch Eingabe von:

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

Firewall auf Systemen konfigurieren, auf denen unterstützte Red Hat Enterprise Linux-Betriebssysteme ausgeführt werden.

Wenn beim Installieren von Red Hat Enterprise Linux die Firewall-Sicherheit aktiviert wird, dann wird die SNMP-Schnittstelle an allen externen Netzwerk-Schnittstellen standardmäßig geschlossen. Damit SNMP-Verwaltungsanwendungen, wie z. B. IT Assistant, Informationen vom Server Administrator ermitteln und empfangen können, muss der SNMP-Anschluss auf mindestens einer externen Netzwerkschnittstelle geöffnet sein. Wenn der Server Administrator ermittelt, dass kein SNMP-Anschluss der Firewall aller externen Netzwerkschnittstellen geöffnet ist, zeigt der Server Administrator eine Warnmeldung an und trägt eine Meldung im System-Protokoll ein.

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

Um den SNMP-Anschluss mittels einer der zuvor beschriebenen Methoden zu öffnen, führen Sie folgende Schritte durch:

1. Geben Sie an der von Befehlsaufforderung von Red Hat Enterprise Linux den Befehl setup ein und drücken Sie <Eingabe>, um das Textmodus-Setup-Dienstprogramm zu starten.

ANMERKUNG: Dieser Befehl steht nur dann zur Verfügung, wenn das Betriebssystem mit Standardeinstellungen installiert worden ist.

   Das Menü **Hilfsprogramm auswählen** wird eingeblendet.

2. Wählen Sie **Firewall-Konfiguration** mit dem Nach-Unten-Pfeil aus und drücken Sie <Eingabe>.

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

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-Anschlussnummer ist **161**. Wenn Sie die graphische Benutzeroberfläche von X Window System verwenden, dann kann es sein, dass bei neueren Versionen von Red Hat Enterprise Linux durch Drücken von <F1> nicht die Informationen über die Firewall-Sicherheitsstufen angezeigt werden.

a. Zur Deaktivierung der Firewall wählen Sie **No firewall** (keine Firewall) oder **Deaktiviert** aus und gehen dann zu Schritt 7 weiter.

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

4. Drücken Sie <Tab>, um zu **An die eigenen Bedürfnisse anpassen** zu wechseln und drücken Sie auf <Eingabe>.

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

5. Wählen Sie aus, ob eine gesamte Netzwerkschnittstelle oder nur ein SNMP-Anschluss jeder Netzwerkschnittstelle geöffnet werden soll.

   a. Um eine gesamte Netzwerkschnittstelle zu öffnen, wechseln Sie mit der Tabulatortaste zu einem der vertrauenswürdigen Komponenten und drücken Sie die Leertaste. Ein Sternchen im Feld links neben dem Komponentennamen zeigt an, dass die gesamte Schnittstelle geöffnet wird.

   b. Um einen SNMP-Anschluss jeder Netzwerkschnittstelle zu öffnen, wechseln Sie mit der Tabulatortaste zu **Weitere Schnittstellen** und geben Sie `snmp:udp` ein.

6. Drücken Sie auf <Tab>, um **OK** auszuwählen und drücken Sie auf <Eingabe>.

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

7. Drücken Sie auf <Tab>, um **OK** auszuwählen und drücken Sie auf <Eingabe>.

   Das Menü **Hilfsprogramm auswählen** wird eingeblendet.

8. Drücken Sie auf <Tab>, um **Beenden** auszuwählen und drücken Sie auf <Eingabe>.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Storage Management Service

Dell™ OpenManage™ Server Administrator: Benutzerhandbuch Version 5.2

Überblick

Der Storage Management Service enthält RAID und nicht-RAID Speicherverwaltung, welche in Server Administrator integriert wird. Auf Microsoft® Windows®, Red Hat® Enterprise Linux® und SUSE ® LINUX Enterprise Server wird Storage Management Service mit typischem Setup oder benutzerdefiniertem Setup installiert. Der Storage Management Service enthält Speicherverwaltungsinformationen in einer integrierten Graphikansicht.

Der Storage Management Service:

- Erlaubt Ihnen das Ausführen von Controller- und Gehäusefunktionen bei allen unterstützten RAID- and Nicht-RAID-Controllern und -Gehäusen von einer einheitlichen graphischen oder Befehlszeilenoberfläche aus und ohne den Einsatz von BIOS-Dienstprogrammen.
- Erlaubt die Anzeige des Status der lokalen und entfernten Speichermedien, die an das überwachte System angeschlossen sind.
- Unterstützt SCSI, SATA, ATA und SAS; Fibre Channel wird jedoch nicht unterstützt.
- Schützt Daten durch das Konfigurieren von Datenredundanz, das Vergeben von Ersatzgeräten oder das Neu erstellen fehlerhafter Laufwerke.
- Bietet eine graphische Benutzeroberfläche in der Form eines Assistenten mit Funktionen für neue und für fortgeschrittene Anwender sowie eine detaillierte Online-Hilfe.
- Bietet eine voll funktionsfähige und mit Skripten einsetzbare Befehlszeilenoberfläche.
- Bietet eine detaillierte Online-Hilfe

Informationen über die Ausführung des Storage Management von der Befehlszeile aus finden Sie im *Benutzerhandbuch für die Server Administrator-Befehlszeilenoberfläche*.

HINWEIS: Der Storage Management Service (Storage Management) ermöglicht Ihnen Speicher-Tasks auszuführen, die Daten zerstören können. Storage Management sollte von erfahrenen Speichermedienadministratoren genutzt werden, die sich mit ihrer Speichermedienumgebung auskennen.

ANMERKUNG: Die vollständige Dokumentation über Storage Management erhalten Sie in der Storage Management-Onlinehilfe und dem *Dell™ OpenManage™ Server Administrator Storage Management: Benutzerhandbuch*.

ANMERKUNG: Das Storage Management Service ist nur auf Systemen mit den Betriebssystemen Microsoft Windows, Red Hat Enterprise Linux und SUSE LINUX Enterprise Server verfügbar.

ANMERKUNG: Es wird empfohlen, dass Sie Red Hat Enterprise Linux Version 3 (Update 6) oder Red Hat Enterprise Linux Version 4 für Storage Management Service verwenden.

Bei der Verwendung des Storage Management können Sie auf der allgemeinen Navigationsleiste auf **Hilfe** klicken, um detaillierte Informationen über das Fenster zu erhalten, das gerade zu sehen ist. 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.

Softwarevoraussetzungen

Vollständige Hardware- und Softwareanforderungen erhalten Sie in der Storage Management -Infodatei (**readme_sm.txt**) und Server Administrator-Infodatei (**readme_sa.txt**). Diese Dateien sind auf der CD *Systems Management Consoles* verfügbar.

Hardware-Voraussetzungen

Grundlegenden oder Storage Management auf einem System installieren, das keinen unterstützten Controller besitzt oder ein Controller, der nicht an einen Speicher angeschlossen ist, ist eine nicht unterstützte Konfiguration. Eine Liste von unterstützten Controllern und andere Informationen über die Storage Management Service-Hardwareanforderungen erhalten Sie in den Infodateien Server Administrator (**readme_sa.txt**) und Storage Management (**readme_sm.txt**) auf der *Systems Management Consoles*.

Storage Management Service

Installation von Storage Management ersetzt jede vorherige Installation des verwalteten Systems des Array Manager (Server-Software) und Konsole (Client-Software), die sich auf dem System befindet. Wenn nur die Array Manager-Konsole auf dem System installiert ist, dann ersetzt die Installation von Storage Management die Konsole von Array Manager nicht.

Der Storage Management Service enthält erweiterte Funktionen für die Konfiguration der lokal in einem System befindlichen RAID- und Nicht-RAID-Festplattenspeicher. Storage Management ermöglicht Ihnen das Ausführen von Controller- und Gehäusefunktionen bei allen unterstützten RAID- und Nicht-RAID-Controllern und -Gehäusen sowie bei PowerVault™ 2xxS- und PowerVault MD1000-Gehäusen von der graphischen Oberfläche des Server Administrators aus und ohne den Einsatz von BIOS-Dienstprogrammen.

Durch den Einsatz des Storage Management Service können Sie die Daten schützen, indem Sie Daten-Redundanz konfigurieren, Hotspares zuweisen oder fehlerhafte Laufwerke neu erstellen. Sie können außerdem datenverändernde Tasks ausführen, wie zum Beispiel das Löschen von virtuellen Festplatten oder das Zurücksetzen der Controller-Konfiguration. Alle Anwender des Storage Management Service sollten sich mit ihrer Speichermedienumgebung und dem Storage Management auskennen.

Ergänzend zu den Schnittstellenfunktionen von Server Administrator bietet der Storage Management Service Assistentenfunktionen für neue und fortgeschrittene Benutzer und eine detaillierte Onlinehilfe.

Die Befehlszeilenoberfläche (CLI) des Storage Management bietet erweiterte Optionen für die Server Administrator-Befehle **omreport** und **omconfig**. Diese Optionen bieten eine voll funktionsfähige und mit Skripten einsetzbare Befehlszeilenoberfläche.

Der Storage Management Service unterstützt SCSI, SATA, ATA und SAS; dagegen wird Fibre Channel nicht unterstützt.

Diese Version von Storage Management unterstützt keine Windows-Datenträger und Festplattenverwaltung. Weitere Informationen finden Sie unter "Storage Management Service".

Storage Management Service und Array Manager

Der Dell OpenManage Storage Management ist ein Ersatz für Array Manager. Der Storage Management Service enthält die gleichen Funktionen zur Speichermedienverwaltung und zur Konfiguration wie der Array Manager. Es gibt Unterschiede in der Betriebssystemunterstützung und anderen Funktionen. Lesen Sie die Details unter "Array Manager zu Storage Management migrieren" und weitere Details erhalten Sie im *Storage Management-Benutzerhandbuch*.

Strukturobjekte des Storage Management

Wenn installiert, ist das Storage Management verfügbar nach Auswahl des Strukturobjekts **Speichermedien** in der graphischen Benutzeroberfläche von Server Administrator. Das Objekt **Speichermedien** erweitert sich, um Strukturobjekte für die unterstützten Controller anzuzeigen, die an das System angeschlossen sind. Das Controller-Objekt wird erweitert, um den an den Controller angeschlossenen Speicher zu zeigen.

Abhängig von den an das System angeschlossenen Controllern und Speichermediengeräten zeigt das erweiterte Objekt **Speichermedien** die folgenden Objekte niedriger Ebene:

- Controller
- Batterie
- Konnektor
- Gehäuse oder Rückwandplatine
- Physische Festplatten
- EMMs (Gehäuseverwaltungs-Module)
- Lüfter
- Netzteile
- Temperaturen
- Firmware-/Treiberversion
- Virtuelle Festplatten

Register Funktionszustand

Das Register **Funktionszustand** zu jedem Strukturobjekt zeigt Statusinformationen für das ausgewählte Objekt.

Register Informationen/Konfiguration

Das Register **Informationen/Konfiguration** zu jedem Strukturobjekt zeigt Eigenschaftsinformationen für das ausgewählte Objekt. Wenn Sie den Storage Management Service nutzen, hat das Register **Informationen/Konfiguration** außerdem Drop-Down-Menüs und Schaltflächen für das Ausführen von Speicher-Tasks und das Starten von Assistenten.

Storage Management-Tasks

Der Storage Management Service besitzt Drop-Down-Menüs und Assistenten für das Ausführen von Tasks für das Storage Management und die Konfiguration. Der Abschnitt diskutiert eine der allgemeinen Speicher-Tasks und -assistenten, die der Storage Management Service anbietet.

ANMERKUNG: Eine vollständige Dokumentation der Speicher-Tasks des Storage Management und anderer Funktionen finden Sie in der Onlinehilfe des Storage Management.

Assistent zum Erstellung einer virtuellen Festplatte

Der Storage Management Service bietet den Schnell-Assistenten und den erweiterten Assistenten zur Erstellung von virtuellen Festplatten. Der Schnell-Assistent berechnet eine angemessene Konfiguration der virtuellen Festplatte, basierend auf Überlegungen zum verfügbaren Speicherplatz und dem Controller. Beim Benutzen des Schnell-Assistenten wählen Sie die RAID-Stufe und die Größe der virtuellen Festplatte. Der Schnell-Assistent wählt eine erforderliche Festplattenkonfiguration, die der ausgewählten RAID-Stufe und Größe entspricht. Der Schnell-Assistent erfordert minimale Benutzereingaben und ist für neue Benutzer empfehlenswert.

Der erweiterte Assistent zur Erstellung von virtuellen Festplatten ermöglicht die Angabe der Lese-, Schreib- und Cache-Regeln für die virtuelle Festplatte. Sie können außerdem die physischen Festplatten und den Controller-Konnektor wählen, der verwendet werden soll. Sie benötigen umfangreiches Wissen über RAID-Stufen und die Hardware, um den erweiterten Assistent zu nutzen. Dieser Assistent ist empfehlenswert für fortgeschrittene Benutzer.

So starten Sie den Schnell-Assistent und den erweiterten Assistenten zur Erstellung einer virtuellen Festplatte:

1. Erweitern Sie das Objekt **Speichermedien**, um die Controller-Objekte anzuzeigen.
2. Erweitern Sie ein Controller-Objekt.
3. Wählen Sie das Objekt **Virtuelle Festplatten**.
4. Klicken Sie auf **Zur Seite Assistent zum Erstellen von virtuellen Festplatten wechseln.**
5. Weitere Informationen finden Sie in der Onlinehilfe zum Storage Management.

Assistent zum Neu konfigurieren einer virtuellen Festplatte

Der Assistent zum Neu konfigurieren einer virtuellen Festplatte ermöglicht das Ändern der Konfiguration einer virtuellen Festplatte. Mit diesem Task können Sie die RAID-Stufe ändern oder die Größe der virtuellen Festplatte erhöhen, indem Sie physische Festplatten hinzufügen.

So starten Sie den Assistenten zum Neu konfigurieren einer virtuellen Festplatte:

1. Erweitern Sie das Objekt **Speichermedien**, um die Controller-Objekte anzuzeigen.
2. Erweitern Sie ein Controller-Objekt.
3. Wählen Sie das Objekt **Virtuelle Festplatten**.
4. Wählen Sie **Neu konfigurieren** aus dem Drop-Down-Menü **Verfügbare Tasks**.
5. Klicken Sie auf **Ausführen.**
6. Weitere Informationen finden Sie in der Onlinehilfe zum Storage Management.

Integrität der redundanten virtuellen Festplatten erhalten

Wenn Sie eine redundante virtuelle Festplatte erstellt haben, überprüft der Task Übereinstimmungsüberprüfung die Fehlerfreiheit der redundanten (Paritäts)-Informationen. Dieser Task gilt nur für redundante virtuelle Festplatten. Wenn notwendig, erstellt der Task Übereinstimmungsüberprüfung die redundanten Daten neu.

So starten Sie den Task Übereinstimmungsüberprüfung:

1. Erweitern Sie das Objekt **Speichermedien**, um die Controller-Objekte anzuzeigen.
2. Erweitern Sie ein Controller-Objekt.
3. Wählen Sie das Objekt **Virtuelle Festplatten**.
4. Wählen Sie **Übereinstimmungsprüfung** aus dem Drop-Down-Menü **Verfügbare Tasks**.
5. Klicken Sie auf **Ausführen.**
6. Weitere Informationen finden Sie in der Onlinehilfe zum Storage Management.

Globalen Hotspare zuweisen und die Zuweisung rückgängig machen.

Ein globaler Hotspare ist eine nicht verwendete Backup-Festplatte, die ein Teil der Array-Gruppe ist. Hotspares bleiben im Standby-Modus. Wenn eine physische Festplatte, die von einer virtuellen Festplatte genutzt wird, einen Fehler hat, wird der zugewiesene Hotspare aktiviert, um die fehlerhafte physische Festplatte zu ersetzen, ohne das System zu unterbrechen oder ohne einen Benutzereingriff erforderlich zu machen. Wenn ein Hotspare aktiviert wird, erstellt er die Daten für alle redundanten virtuellen Festplatten neu, die die fehlerhafte physische Festplatte verwendeten.

Sie können die Hotspare-Zuweisung ändern, indem Sie eine Festplattenzuweisung rückgängig machen und eine andere Festplatte je nach Bedarf wählen. Sie

können auch mehr als eine physische Festplatte als einen globalen Hotspare zuweisen.

Globale Hotspares müssen manuell zugewiesen und die Zuweisung muss manuell rückgängig gemacht werden. Sie werden nicht spezifischen virtuellen Festplatten zugewiesen. Wenn Sie einen Hotspare einer virtuellen Festplatte zuweisen wollen (es ersetzt jede fehlerhafte physische Festplatte auf der virtuellen Festplatte), gehen Sie nach Anleitung vor, um dedizierte Hotspares zuzuweisen oder deren Zuweisung rückgängig zu machen.

So weisen Sie einen dedizierten Hotspare zu

1. Wählen Sie die Festplatte in der Tabelle **Konnektor** (Kanal oder Schnittstelle) aus, die Sie als dedizierten Hotspare verwenden wollen . Auf einigen Controller kann mehr als eine Festplatte ausgewählt werden. Die Festplatten, die Sie als dedizierte Hotspares ausgewählt haben, werden in Tabelle **Zurzeit als dedizierte Hotspares konfigurierte Festplatten** angezeigt.
2. Klicken Sie auf **Änderungen anwenden** wenn bereit.

So machen Sie die Zuweisung eines dedizierten Hotspare rückgängig

1. Klicken Sie auf die Festplatte in Tabelle **Zurzeit als dedizierte Hotspares konfigurierte Festplatten** um die Zuweisung rückgängig zu machen. Durch Klicken auf die Festplatte wird die Festplatte von der Tabelle **Zurzeit als dedizierte Hotspares konfigurierte Festplatten** entfernt und zur Tabelle Konnektor (Kanal oder Schnittstelle) zurückgeschickt.
2. Klicken Sie auf **Änderungen anwenden** wenn bereit.

Diesen Task im Storage Management ausfindig zu machen

1. Erweitern Sie das Strukturobjekt **Speicher**, um die Controller-Objekte anzuzeigen.
2. Erweitern Sie ein Controller-Objekt.
3. Wählen Sie das Objekt **Virtuelle Festplatten**.
4. Wählen Sie **Dedizierten Hotspare zuweisen/Zuweisung rückgängig machen** aus dem Drop-Down-Menü Verfügbare Tasks.
5. Klicken Sie auf **Ausführen**.
6. Weitere Informationen finden Sie in der Onlinehilfe zum Storage Management.

Neu erstellen einer fehlerhaften physischen Festplatte

Wenn eine fehlerhafte physische Festplatte Teil einer redundanten virtuellen Festplatte ist, sollte der physische Festplattenfehler keine Datenverluste nach sich ziehen, wenn sie sofort ersetzt wird. Der Task Neu erstellen ist verfügbar, wenn das Objekt **Physische Festplatten** ausgewählt wird Weitere Informationen finden Sie in der Onlinehilfe zum Storage Management.

Globale Tasks

Die folgenden globalen Tasks sind verfügbar, wenn das Objekt Speichermedien ausgewählt ist. Weitere Informationen finden Sie in der Onlinehilfe zum Storage Management.

- **Globaler erneuter Scan:** Ein globaler erneuter Scan aktualisiert Konfigurationsänderungen (zum Beispiel neue oder ausgebaute Geräte) für alle Controller und deren angeschlossenen Komponenten.
- **Smart-temperaturbedingtes Herunterfahren aktivieren/deaktivieren.** In der Standardeinstellung fahren das Betriebssystem und der Server herunter, wenn die Gehäuse PV220S und PV221S die kritische Temperatur von 0 oder 50 Grad Celsius erreichen. Mit dem Task Smart-temperaturbedingtes Herunterfahren können Sie angeben, das nur das Gehäuse und nicht das Betriebssystem und der Server heruntergefahren werden, wenn das Gehäuse die kritische Temperatur erreicht. Um das System auf die Standardeinstellung zurückzusetzen, benutzen Sie den Task Smart-temperaturbedingtes Herunterfahren deaktivieren.

Controller-Tasks

Die folgenden Controller-Tasks sind verfügbar, wenn das Objekt **Controller** ausgewählt ist. Weitere Informationen finden Sie in der Onlinehilfe zum Storage Management.

- **Erneuter Scan eines Controllers:** Ein Controller-Scan aktualisiert Konfigurationsänderungen (zum Beispiel neue oder ausgebaute Geräte) für alle Controller und die angeschlossenen Komponenten.
- **Erstellung einer virtuellen Festplatte:** Weitere Informationen finden Sie unter Assistent zur Erstellung einer virtuellen Festplatte
- **Alarm aktivieren, deaktivieren, abstellen und testen:** Diese Tasks ermöglichen das Verwalten des Controller-Alarms. Ein Beispiel: Sie können den Alarm für das Ereignis eines Gerätefehlers aktivieren oder ihn abstellen, wenn er ertönt.

- **Neuerstellungsrate einstellen:** Die Neuerstellungsrate bezieht sich darauf, wie viele der Systemressourcen für das Neuerstellen einer fehlerhaften physischen Festplatte reserviert werden. Dieser Task ermöglicht das Justieren der Einstellung.
- **Konfigurations-Reset:** Dieser Task löscht alle Informationen im Controller, so dass Sie eine neue Konfiguration ausführen können. Dieser Vorgang zerstört alle virtuellen Festplatten des Controllers.
- **Protokolldatei exportieren:** Dieser Task exportiert das Controller-Protokoll in eine Textdatei.
- **Fremdkonfiguration importieren:** Dieser Task importiert virtuelle Festplatten, die sich auf physischen Festplatten befinden, welche von einem anderen Controller verschoben worden sind.
- **Fremdkonfiguration löschen:** Verwenden Sie den Task Fremdkonfiguration löschen um die Informationen zur virtuellen Festplatte von den kürzlich verbundenen physischen Festplatten zu leeren oder zu löschen.
- **Hintergrundinitialisierungsrate einstellen:** Dieser Task ändert den Anteil von Systemressourcen, die dem Task Hintergrundinitialisierung gewidmet sind.
- **Übereinstimmungsüberprüfungsrate einstellen:** Dieser Task ändert den Anteil von Systemressourcen, die dem Task Übereinstimmungsüberprüfung gewidmet sind.
- **Rekonstruktionsrate einstellen:** Dieser Task ändert den Anteil von Systemressourcen, die dem Task Rekonstruktion gewidmet sind.
- **Patrol Read-Modus einstellen:** Diese Funktion identifiziert Festplattenfehler, um Festplattenfehler und Datenverlust oder -korruption zu vermeiden.
- **Patrol Read starten und stoppen:** Mit diesen Tasks können Sie das Task Patrol Read starten oder einen ausführenden Task stoppen, wenn der Patrol Read-Modus auf manuell eingestellt ist.
- **Fremdkonfiguration importieren / wiederherstellen:** Dieser Task importiert virtuelle Festplatten und stellt sie wieder her, die sich auf physischen Festplatten befinden, welche von einem anderen Controller verschoben worden sind.

Batterie-Tasks

Die folgenden Batterie-Tasks sind verfügbar, wenn das Objekt **Batterie** ausgewählt ist. Dieser Task ist nur verfügbar bei Controllern, die eine Batterie haben, die überholt werden muss. Weitere Informationen finden Sie in der Onlinehilfe zum Storage Management.

- **Batterie überholen:** Dieser Task entlädt und lädt die Controller-Batterie vollständig.
- **Lernzyklus starten:** Verwenden Sie den Task Lernzyklus starten um den Lernzyklus der Batterie zu beginnen.
- **Verzögerung Batterielernyzklus:** Verwenden Sie diesen Task, um die Startzeit des Lernzyklus bis zu sieben Tage zu verzögern.

Konnektor-Tasks

Die folgenden Konnektor-Tasks sind verfügbar, wenn das Objekt **Konnektor** ausgewählt ist. Weitere Informationen finden Sie in der Onlinehilfe zum Storage Management.

- **Konnektor neu scannen:** Dieser Task scannt die Controller-Konnektoren neu, um die aktuell angeschlossenen Geräte zu überprüfen oder um neue Geräte zu erkennen, die den Konnektoren hinzugefügt wurden. Das Ausführen eines Konnektor-Neuscans entspricht dem Ausführen eines Controller-Neuscans.

Gehäuse-Tasks

Die folgenden Gehäuse-Tasks sind verfügbar, wenn das Objekt **Gehäuse** ausgewählt ist. Weitere Informationen finden Sie in der Onlinehilfe zum Storage Management.

- **Alarm deaktivieren und aktivieren:** Benutzen Sie diesen Task, um den Gehäusealarm zu verwalten. Wenn aktiviert, ertönt der Alarm, wenn am Gehäuse eine Fehlerbedingung eintritt.
- **Bestandsdaten einstellen:** Benutzen Sie diesen Task, um die Systemkennnummer und den Bestandsnamen des Gehäuses einzustellen.
- **Temperatursondenwerte einstellen:**Die Temperatursonden überwachen die Temperatur des Gehäuses. Jede Temperatursonde besitzt einen Warnungs- und einen Fehlerschwellenwert. Der Warnungsschwellenwert zeigt an, dass das Gehäuse eine inakzeptabel hohe oder niedrige Temperatur erreicht hat. Benutzen Sie diesen Task, um den Warnungsschwellenwert zu ändern.
- **Blinken:** Verwenden Sie den Task Blinken, um die Leuchtdioden (LEDs) auf dem Gehäuse zu blinken. Sie können diesen Task verwenden um ein Gehäuse ausfindig zu machen. Die LEDs auf dem Gehäuse können verschiedene Farben und Blinkmuster angezeigt werden.

Temperatur-Tasks

Die folgenden Temperatur-Tasks sind verfügbar, wenn das Objekt **Temperatur** ausgewählt ist. Weitere Informationen finden Sie in der Onlinehilfe zum Storage Management.

- **Temperatursondenwerte einstellen:** Die Temperatursonden überwachen die Temperatur des Gehäuses. Jede Temperatursonde besitzt einen Warnungs- und einen Fehlerschwellenwert. Der Warnungsschwellenwert zeigt an, dass das Gehäuse eine inakzeptabel hohe oder niedrige Temperatur erreicht hat. Benutzen Sie diesen Task, um den Warnungsschwellenwert zu ändern.

Tasks der physischen Festplatte

Die folgenden Tasks der physischen Festplatte sind verfügbar, wenn das Objekt **Physische Festplatte** ausgewählt ist. Weitere Informationen finden Sie in der Onlinehilfe zum Storage Management.

- **Blinken und Nicht-Blinken:** Der Task Blinken ermöglicht das Auffinden einer Festplatte in einem Gehäuse, in dem eine der Leuchtdioden (LED.) auf der

Festplatte zum Blinken gebracht wird. Der Task Nicht-Blinken beendet den Task Blinken.

- **Tote Segmente entfernen:** Unter bestimmten Umständen erlaubt dieser Task das Wiederherstellen von Festplattenspeicherplatz, der im Moment nicht verwendet wird.
- **Globalen Hotspare zuweisen und die Zuweisung rückgängig machen:** Globalen Hotspare zuweisen und die Zuweisung rückgängig machen.
- **Zum Entfernen vorbereiten:** Verwenden Sie diesen Task, um eine Festplatte aus einem Gehäuse zu entfernen.

HINWEIS: Um Datenverlust zu verhindern, stellen Sie sicher, dass Sie diesen Task ausführen.

- **Online und Offline:** Benutzen Sie den Offline-Task, um eine Festplatte zu deaktivieren, bevor sie entfernt wird. Benutzen Sie den Online-Task, um eine offline geschaltete Festplatte wieder zu reaktivieren.
- **Initialisieren:** Bei einigen Controllern bereitet der Task Initialisieren eine physische Festplatte für die Nutzung als Bestandteil einer virtuellen Festplatte vor.
- **Neu erstellen:** Weitere Informationen finden Sie unter Neu erstellen einer fehlerhaften physischen Festplatte
- **Neuerstellung abbrechen:** Verwenden Sie den Task Neuerstellung abbrechen, um eine Neuerstellung abzubrechen, die durchgeführt wird.
- **Physische Festplatte löschen und Löschen abbrechen:** Verwenden Sie den Task Physische Festplatte löschen, um Daten zu löschen, die sich auf einer physischen Festplatte befinden.

Tasks der virtuellen Festplatte

Die folgenden Tasks der virtuellen Festplatte sind verfügbar, wenn das Objekt **Virtuelle Festplatte** ausgewählt ist. Weitere Informationen finden Sie in der Onlinehilfe zum Storage Management.

- **Neu konfigurieren:** Weitere Informationen finden Sie unter Assistent zum Neu konfigurieren einer virtuellen Festplatte
- **Neuerstellung abbrechen:** Verwenden Sie den Task Neuerstellung abbrechen, um eine Neuerstellung abzubrechen, während sie durchgeführt wird.
- **Neukonfiguration abbrechen:** Verwenden Sie den Task Neukonfiguration abbrechen, um eine Neukonfiguration der virtuellen Festplatte abzubrechen, während sie durchgeführt wird.
- **Formatieren und Initialisieren; langsam und Schnell Initialisieren.** Benutzen Sie den Task Formatieren oder langsam und schnell initialisieren, um die Dateien zu löschen und das Dateisystem einer virtuellen Festplatte zu entfernen.
- **Hintergrund-Initialisierung abbrechen:** Bei einigen Controllern beginnt die Hintergrund-Initialisierung redundanter virtueller Festplatten automatisch, nachdem die virtuelle Festplatte erstellt wurde. Benutzen Sie diesen Task, wenn Sie die Hintergrund-Initialisierung abbrechen müssen.
- **Tote Segmente wiederherstellen:** Verwenden Sie den Task Tote Segmente wiederherstellen, um die Daten auf einer RAID-5 virtuellen Festplatte wiederherzustellen, das beschädigt wurde.
- **Löschen.** Verwenden Sie diesen Task, um alle Daten auf der virtuellen Festplatte zu löschen.
- **Dedizierten Hotspare zuweisen und die Zuweisung rückgängig machen:** Globalen Hotspare zuweisen und die Zuweisung rückgängig machen.
- **Übereinstimmungsüberprüfung, Übereinstimmungsüberprüfung abbrechen, Übereinstimmungsüberprüfung anhalten und Übereinstimmungsüberprüfung wieder aufnehmen:** Weitere Informationen finden Sie unter "Integrität der redundanten virtuellen Festplatten erhalten."
- **Blinken und Nicht-Blinken:** Die Tasks Blinken und Nicht-Blinken starten oder stoppen das Blinken der Anzeigeleuchten auf den physischen Festplatten einer virtuellen Festplatte.
- **Umbenennen:** Verwenden Sie diesen Task, um eine virtuelle Festplatte umzubenennen.
- **Änderungsregel:** Benutzen Sie diesen Task, um die Lese-, Schreib- oder Cache-Regeln einer virtuellen Festplatte zu ändern.
- **Split Mirror:** Verwenden Sie diesen Task, um gesiegelte Daten zu trennen, die ursprünglich als RAID 1-, RAID 1-Verkettetes- oder RAID 10-virtuelle Festplatte konfiguriert wurden.
- **Spiegelung beenden:** Verwenden Sie diesen Task, um gesiegelte Daten zu trennen und die Hälfte des Spiegels als freien Speicherplatz wiederherzustellen.

Weitere Funktionen des Storage Management und Dokumentation

Die vollständige Dokumentation über Storage Management Service erhalten Sie in der Storage Management-Onlinehilfe und dem *Dell OpenManage Server Administrator Storage Management: Benutzerhandbuch*. Informationen über das Starten der Online-Hilfe finden Sie unter "Anzeigen der Online-Hilfe."

Array Manager zu Storage Management migrieren

Wenn Sie eine vorhandene Installation von Array Manager mit Storage Management ersetzen, treffen die folgenden Migrationserwägungen zu:

- **Erhalt der virtuellen Festplatte:** Sie können die Namen der virtuellen Festplatte bewahren, wenn Sie von Array Manager zu Storage Management migrieren. Um dies zu tun, kann Array Manager nicht vor der Installation von Storage Management deinstalliert werden. Wenn Array Manager vor der Installation von Storage Management deinstalliert wird, dann wird Storage Management die mit Array Manager erstellten virtuellen Festplatten umbenennen. Ungeachtet dessen ob Array Manager deinstalliert ist, wird Storage Management in der Lage sein, die mit Array Manager erstellten virtuellen Festplatten zu identifizieren und zu verwalten.
- **SNMP-Traps:** Die Architektur zur Handhabung von SNMP-Traps und Verwaltungsinformationsbasis(MIB), ist in Storage Management unterschiedlich vom Array Manager. Sie müssen Anwendungen modifizieren, die an den Empfang von SNMP-Traps von Array Manager angepasst sind.
- **Ereignisnummerierung:** Das Nummerierungsschema für die Warnungen oder Ereignisse des Storage Management unterscheidet sich vom Nummerierungsschema der entsprechenden Array Manager-Ereignisse. Weitere Informationen finden Sie in der Onlinehilfe zum Storage Management.

Storage Management-Befehlszeilenoberfläche

Informationen über die Ausführung des Storage Management Service von der Befehlszeile aus finden Sie im *Benutzerhandbuch für die Server Administrator-Befehlszeilenoberfläche*. Wenn der Storage Management installiert ist, können Sie sich außerdem auf die Onlinehilfe beziehen, um Informationen über die erweiterten Befehlszeilenoptionen **omreport** und **omconfig** zu finden.

Anzeigen der Online-Hilfe

Server Administrator enthält eine kontextabhängige Onlinehilfe. Um auf diese Online-Hilfe zuzugreifen, klicken Sie auf **Hilfe** in der allgemeinen Navigationsleiste. Die Navigationsleiste 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.

Weitere Informationen finden Sie in der Onlinehilfe des Storage Management. Diese Hilfe ist verfügbar, wenn das Objekt **Speichermedien** oder ein darunter liegendes Strukturobjekt ausgewählt ist.

Die Onlinehilfe des Storage Management Service.

- Bietet konzeptionelle Informationen über Speichermedienkonzepte wie virtuelle Festplatten, RAID und so weiter
- Beschreibt die Komponenten der graphischen Benutzeroberfläche in den verschiedenen Fenstern der Anwendung.
- Gibt detaillierte schrittweise Anleitungen über die Tasks, die sie in der graphischen Benutzeroberfläche ausführen können.
- Beschreibt die verfügbaren CLI-Befehle und ihre Unterbefehle

Die Onlinehilfe des Storage Management ist in zwei Formaten verfügbar:

- **Umgebungsabhängige Hilfe:** Um auf die kontextabhängige Online-**Hilfe** zuzugreifen, klicken Sie auf Hilfe in der allgemeinen Navigationsleiste.
- **Inhaltsübersicht:** Die Hilfe-Bildschirme für die kontextabhängige Hilfe enthalten Verknüpfungen zum Inhaltsverzeichnis der Online-Hilfe. Um auf das Inhaltsverzeichnis zuzugreifen, klicken Sie zuerst auf **Hilfe** in der allgemeinen Navigationsleiste. Klicken Sie auf das Link **Zurück zur Seite Storage Management-Inhalt** um das Inhaltverzeichnis anzuzeigen. Diese Verknüpfung wird oben und unten auf jedem Hilfe-Bildschirm angezeigt. Verwenden Sie das Inhaltsverzeichnis, um auf alle Themen zuzugreifen, die die Online-Hilfe behandelt.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Server Administrator verwenden

Dell™ OpenManage™ Server Administrator: Benutzerhandbuch Version 5.2

Server Administrator-Sitzung starten

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

Um eine Server Administrator-Sitzung auf einem Remote-System zu starten, rufen Sie Ihren Web-Browser auf und geben Sie eine der folgenden Zeilen 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 zugewiesene IP-Adresse des verwalteten Systems ist und `1311` die Standardschnittstellennummer

Das **Server Administrator Anmelde**fenster erscheint.

ANMERKUNG: Geben Sie `https: //` (und nicht `http://`) in das Adressfeld ein, um eine gültige Antwort im Browser zu erhalten.

ANMERKUNG: **Die Standardeinstellungsschnittstelle für Dell OpenManage Server Administrator ist 1311.** Sie können den Anschluss ändern, falls erforderlich. Anleitungen zum Setup Ihrer Systemeinstellungen erhalten Sie unter "Dell Systems Management Server Administration-Verbindungsdienst und Sicherheitssetup".

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

An- und Abmelden

Um sich beim Server Administrator anzumelden, geben Sie Ihren/Ihr zuvor festgelegten/festgelegtes **Benutzernamen** und **Kennwort** in die entsprechenden Felder des **Anmeldungs**fensters der Systemverwaltung ein. Unter "Einfache Anmeldung" finden Sie Informationen zur Umgehung der Anmeldeseite und zum Zugriff auf die Server Administrator-Webanwendung, indem Sie auf das **Dell OpenManage Server Administrator**-Symbol auf Ihrem Desktop klicken.

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

Wenn Sie von einer definierten Domäne auf den Server Administrator zugreifen, müssen Sie ebenfalls den korrekten **Domänen**namen angeben.

ANMERKUNG: Das Drop-Down-Menü **Anwendung** wird als ein nichtauswählbares Feld für Systeme angezeigt, die nur auf eine Dell OpenManage Server Administrator--Komponente zugreifen können. Das Drop-Down-Menü funktioniert nur, wenn zwei oder mehr Dell OpenManage Server Administrator-Komponenten auf dem verwalteten System verfügbar sind.

Wählen Sie das Kontrollkästchen **für Active Directory-Anmeldung**, um sich mithilfe des Active Directory® von Microsoft® anzumelden.

Zum Beenden der Server Administrator-Sitzung klicken Sie auf der allgemeinen Navigationsleiste auf **Abmelden**. Die Schaltfläche **Abmelden** befindet sich in der rechten oberen Ecke der Homepage des Server Administrators.

Einfache Anmeldung

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

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

Für den lokalen Maschinenzugang ist es nicht erforderlich, dass Sie auf der Maschine ein Konto mit korrekten Berechtigungen haben (Benutzer, Hauptbenutzer oder Verwalter). Andere Benutzer werden gegen Microsoft Active Directory authentisiert.

Um Server Administrator mithilfe von Einzelanmeldungsauthentisierung gegen Microsoft Active Directory zu starten, muss die Hinzufügung der folgenden

Parameter bestanden werden in:

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

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

Beispiel:

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

Um Server Administrator mithilfe der einfachen Anmeldungs-Authentifizierung gegen die Benutzerkonten der lokalen Maschine zu starten, muss die Hinzufügung der folgenden Parameter bestanden werden in:

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

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

Beispiel:

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

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

Systeme, auf denen ein unterstütztes Microsoft Windows Server 2003-Betriebssystem ausgeführt wird

Die Sicherheitseinstellungen für den Browser müssen konfiguriert werden, damit Sie sich von einem Remote-Verwaltungssystem am Server Administrator anmelden können, auf dem ein unterstütztes Microsoft Windows Server® 2003-Betriebssystem ausgeführt wird.

Die Sicherheitseinstellungen für den Browser verhindern auf der Client-Seite möglicherweise die Ausführung von Skripts, die vom 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 am Server Administrator möglicherweise ein leerer Bildschirm angezeigt. In diesem Fall wird eine Fehlermeldung ausgegeben mit der Anweisung, die Browser-Einstellungen zu konfigurieren.

Internet Explorer

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

   Für Windows 2000:

   - Unter **Verschiedenes** wählen Sie die Optionsschaltfläche **Meta Refresh zulassen**.
   - Unter **Active Scripting** wählen Sie die Optionsschaltfläche **Aktivieren**.

   Für Windows 2003:

   - Unter **Verschiedenes,** wählen Sie die Optionsschaltfläche **Meta Refresh zulassen**.
   - Unter **Active Scripting,** wählen Sie die Optionsschaltfläche **Aktivieren**.
   - Unter **Active Scripting** wählen Sie die Optionsschaltfläche **Skriptzugriff auf Internet Explorer Web Browser-Steuerungen zulassen**.
7. Klicken Sie auf **OK**, um die neuen Einstellungen zu speichern.
8. Schließen Sie den Browser.
9. Melden Sie sich am Server Administrator an.

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

1. Starten Sie den Browser.

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

Mozilla

1. Starten Sie den Browser.
2. Klicken Sie auf **Bearbeiten**→ **Einstellungen**.
3. Klicken Sie auf **Erweitert Scripts und Plugins.**
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 am Server Administrator an.

Server Administrator-Homepage

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

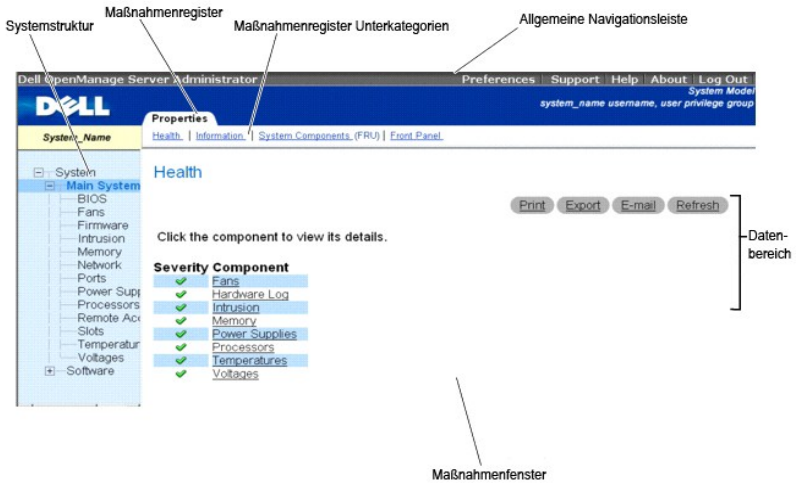
Mit nur wenigen Ausnahmen besteht die Server Administrator-Homepage aus drei Hauptbereichen:

- Die allgemeine Navigationsleiste enthält Verknüpfungen zu den allgemeinen Diensten.
- Die 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-Homepage angemeldet ist, werden darüber hinaus das Systemmodell, der zugewiesene Systemname und der Benutzername des gegenwärtigen Benutzers sowie die Benutzerberechtigungen in der rechten oberen Ecke des Fensters angezeigt.

Abbildung 5-1 zeigt ein Beispiel-Layout für die Server Administrator-Homepage für einen mit Administratorrechten angemeldeten Benutzer.

Abbildung 5-1. Beispiel-Server Administrator-Homepage



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

ANMERKUNG: Viele der Systemstrukturobjekte, Systemkomponenten, Maßnahmenregister oder Datenbereichsfunktionen sind nicht verfügbar für Benutzer, die nur mit Benutzer-Zugriffsrechten angemeldet sind. Administrator- oder Hauptbenutzer-Zugriffsrechte sind zur Ansicht vieler der konfigurierbaren Systemstrukturobjekte, Systemkomponenten, Maßnahmenregister oder Datenbereichsfunktionen erforderlich. Darüber hinaus haben nur Benutzer, die mit Administrator-Rechten angemeldet sind, Zugriff auf die Herunterfahr-Funktion im Register **Herunterfahren**.

Allgemeine Navigationsleiste

Die allgemeine Navigationsleiste und ihre Verknüpfungen stehen allen Benutzerstufen zur Verfügung, ungeachtet der jeweiligen Position im Programm.

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

Systemstruktur

Die Systemstruktur wird auf der linken Seite der Server Administrator-Homepage angezeigt und enthält die anzeigbaren Komponenten des Systems. Die Systemkomponenten werden nach Komponententyp kategorisiert. Wenn das Hauptobjekt, genannt **System**, erweitert wird, sind die Systemkomponenten-Hauptkategorien, die erscheinen können, **Hauptsystemgehäuse**, **Software** und **Speicher**

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

Maßnahmenfenster

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

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

Datenbereich

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

unterstrichene Einträge und Messanzeigen.

Statusanzeigen der Systemkomponente

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

Tabelle 5-1. Statusanzeigen der Systemkomponente

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

Task-Schaltflächen

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

- Klicken Sie auf **Drucken**, wird eine Kopie des geöffneten Fensters auf dem Standarddrucker ausgegeben.
- Durch das Klicken auf **Exportieren** wird eine Textdatei erstellt, in der die Werte jedes Datenfeldes in dem offenen Fenster aufgelistet sind. Die Exportdatei wird in dem von Ihnen bestimmten Speicherort gespeichert. Unter "Benutzer- und Systemeinstellungen vornehmen" finden Sie eine Anleitung zur benutzerspezifischen Einstellung der Begrenzungszeichen, mit denen die Feldwerte 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.

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

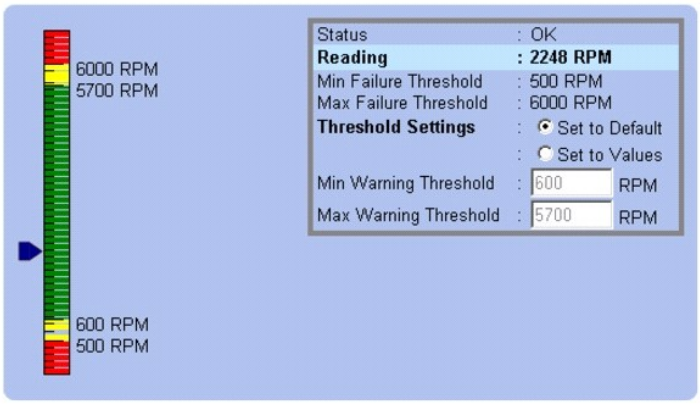
Unterstrichene Einträge

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

Messanzeigen

Temperatursonden, Lüftersonden und Spannungssonden werden durch eine Messanzeige dargestellt. Abbildung 5-2 zeigt z. B. Messwerte von der CPU-Lüftersonde eines Systems.

Abbildung 5-2. Messanzeige



Online-Hilfe verwenden

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

Voreinstellungen-Homepage verwenden

Die Voreinstellungen-Homepage zeigt standardmäßig auf die Seite **Zugriffs-Konfiguration** im Register **Voreinstellungen**.

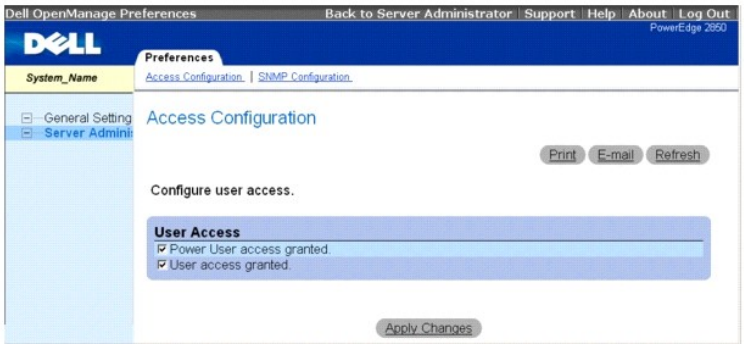
Auf der Voreinstellungen-Homepage können Sie den Zugriff auf Benutzer mit Benutzer- und Hauptbenutzer-Zugriffsrechten einschränken, das SNMP-Kennwort einrichten und Benutzer- und Secure Port-Systemeinstellungen konfigurieren.

Wie die Server Administrator-Homepage besteht die Voreinstellungen-Homepage aus drei Hauptbereichen:

- Die allgemeine Navigationsleiste enthält Verknüpfungen zu den allgemeinen Diensten.
  - Klicken auf **Zurück zu Server Administrator** kehrt zur Server Administrator-Homepage zurück.
- Auf der linken Seite der Voreinstellungen-Homepage (in der die Systemstruktur auf der Server Administrator-Homepage angezeigt wird) werden die Voreinstellungskategorien für das verwaltete System angezeigt.
- Das Maßnahmenfenster zeigt die für das verwaltete System verfügbaren Einstellungen und Voreinstellungen an.

Abbildung 5-3 zeigt ein Beispiel-Layout für eine Einstellungen-Homepage.

Abbildung 5-3. Beispiel Einstellungen-Homepage



Server Administrator-Befehlszeilenschnittstelle verwenden

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

In vielen Fällen lässt die CLI Benutzer mit wohl durchdachten Aufgabenplänen Informationen über das System schnell abrufen. Mit CLI-Befehlen können Administratoren Stapelprogramme oder Skripts schreiben, die zu bestimmten Zeiten ausgeführt werden sollen. Wenn diese Programme ausgeführt werden, können sie Berichte über wichtige Komponenten, z. B. Lüftergeschwindigkeit, sammeln. Mit zusätzlichem Skripting kann die CLI zur Sammlung von Daten während Spitzenbelastungszeiten verwendet werden, die dann mit den gleichen, zu Zeiten geringerer Systembelastung gesammelter Daten verglichen werden. Befehlsergebnisse können zur späteren Analyse in eine Datei geschrieben 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*.

Dell Systems Management Server Administration-Verbindungsdienst und Sicherheitssetup

Dieser Abschnitt behandelt die folgenden Themen:

- Benutzer- und Systemeinstellungen vornehmen
- X.509-Zertifikatsverwaltung

Benutzer- und Systemeinstellungen vornehmen

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

ANMERKUNG: Zum Festlegen oder Zurücksetzen von Benutzer- oder Systemeinstellungen müssen Sie mit Administrator-Rechten angemeldet sein.

Führen Sie folgende Schritte durch, um die Benutzereinstellungen festzulegen:

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

   Die **Voreinstellungen**-Homepage wird eingeblendet.

2. Klicken Sie auf **Allgemeine Einstellungen**.

3. Um einen vorgewählten E-Mail-Empfänger hinzuzufügen, geben Sie die E-Mail-Adresse des angegebenen Servicekontakts in das Feld **Senden an:**ein und klicken Sie auf **Änderungen anwenden**.

   ANMERKUNG: Durch Klicken auf **E**-Mail wird eine E-Mail-Nachricht, an die eine HTML-Datei des Fensters angehängt ist, an die vorgegebene E-Mail-Adresse gesendet, und zwar von jedem Fenster aus.

4. Zum Ändern der Darstellung der Homepage wählen Sie einen anderen Wert in den Feldern **Skin** oder **Schema** und klicken Sie auf **Änderungen anwenden**.

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

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

   Die **Voreinstellungen**-Homepage wird eingeblendet.

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

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

   - Mit der Funktion **Sitzungszeitüberschreitung** kann die Zeit begrenzt werden, in der eine Server Administrator-Sitzung aktiv bleiben kann. Wählen Sie die Optionsschaltfläche **Aktivieren**, um den Server Administrator die Sitzung beenden zu lassen, wenn für einen bestimmten Zeitraum keine Benutzermaßnahme stattfindet. Benutzer, deren Sitzung beendet wird, müssen sich erneut anmelden. Wählen Sie das Optionsschaltfläche **Deaktivieren**, um die Zeitüberschreitungsfunktion des Server Administrators zu deaktivieren.
   - Das Feld **HTTPS-Anschluss** bestimmt den sicheren Anschluss für den Server Administrator. Der sichere Standardanschluss für Server Administrator ist 1311.

   ANMERKUNG: Die Änderung der Anschlussnummer auf eine ungültige bzw. eine bereits belegte Anschlussnummer kann andere Anwendungen oder Browser beim Zugriff auf den Server Administrator auf dem verwalteten System behindern. 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 verwaltete System fest, mit der sich der Server Administrator zu Beginn einer Sitzung verbindet. Wählen Sie die Optionsschaltfläche **Alle** zum Binden an alle für das System in Frage kommenden IP-Adressen. Wählen Sie die Optionsschaltfläche **Spezifisch** zum Binden an eine bestimmte IP-Adresse.

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

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

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

   - Im Feld **Befehlsprotokollumfang** wird der maximale Umfang (in MB) für die Befehlsprotokolldatei festgelegt.
   - Das Feld **Support-Verknüpfung** enthält die URL für die Geschäftsabteilung, 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. Die verfügbaren Verschlüsselungsstufen enthalten **Automatische Verhandlung** und **128 Bit oder höher**.
     - **Automatische Verhandlung**: Um Verbindung vom Browser mit jeder Verschlüsselungsstärke zu erlauben. Der Browser verhandelt automatisch mit dem Server Administrator Web Server und verwendet die höchste verfügbare Verschlüsselungsstufe für die Sitzung. Legacy-Browser mit der schwächeren Verschlüsselung können an den Server Administrator anschließen.
     - **128 Bit oder höher:** Um Verbindungen von Browsern mit 128 Bit oder höherer Verschlüsselungskraft zu erlauben. Eine der folgenden ChiffreßFolgen ist basierend auf den Browser für jegliche feststehenden Sitzungen anwendbar:

     SSL_RSA_WITH_RC4_128_SHA

     SSL_RSA_WITH_RC4_128_MD5

     SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA

     TLS_DHE_RSA_WITH_AES_128_CBC_SHA

SSL_RSA_WITH_3DES_EDE_CBC_SHA

TLS_RSA_WITH_AES_128_CBC_SHA

TLS_DHE_DSS_WITH_AES_128_CBC_SHA

SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA

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

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

HINWEIS: 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 **Servervoreinstellungen** vorgenommen haben, klicken Sie auf **Änderungen anwenden**.

X.509-Zertifikatsverwaltung

Web-Zertifikate sind erforderlich zur Sicherstellung der Identität eines entfernten Systems und zur Vergewisserung, dass mit dem entfernten System ausgetauschte Informationen von anderen weder gesehen noch geändert. Zur Gewährleistung der Systemsicherheit wird empfohlen, entweder ein neues X.509-Zertifikat zu erstellen, ein bestehendes wieder zu verwenden oder eine root-Zertifikatskette von einer Certification Authority (CA) zu importieren.

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

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

Verwenden Sie das X.509-Zertifikathilfsprogramm, um entweder ein neues X.509-Zertifikat zu erstellen, ein bestehendes wieder zu verwenden oder eine root-Zertifikatskette von einer CA zu importieren. Zu CAs gehören Verisign, Entrust und Thawte.

Server Administrator steuern

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

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

Server Administrator starten

Unterstützte Microsoft Windows-Betriebssysteme

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

1. Klicken Sie auf die Schaltfläche **Start** und zeigen Sie auf **Einstellungen**→ **Systemsteuerung**→ **Verwaltung**→ **Dienste**.

   Das Fenster **Dienste** wird eingeblendet.

2. Klicken Sie mit der rechten Maustaste auf das Dell Systems Management Server Administration-Symbol (**DSM SA)-Verbindungsdienst**.

3. Klicken Sie auf **Start**.

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

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

```
dsm_om_connsvc start
```

Server Administrator anhalten

Unterstützte Microsoft Windows-Betriebssysteme

Um Server Administrator anzuhalten, führen Sie folgende Schritte durch:

1. Klicken Sie auf die Schaltfläche **Start** und zeigen Sie auf **Einstellungen**→ **Systemsteuerung**→ **Verwaltung**→ **Dienste**.

   Das Fenster **Dienste** wird eingeblendet.

2. Klicken Sie mit der rechten Maustast auf das Symbol **DSM SA-Verbindungsdienst**.

3. Klicken Sie auf **Anhalten**.

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

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

```
dsm_om_connsvc stop
```

Server Administrator neu starten

Unterstützte Microsoft Windows-Betriebssysteme

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

1. Klicken Sie auf die Schaltfläche **Start** und zeigen Sie auf **Einstellungen**→ **Systemsteuerung**→ **Verwaltung**→ **Dienste**.

   Das Fenster **Dienste** wird eingeblendet.

2. Klicken Sie mit der rechten Maustaste auf das Symbol **DSM SA-Verbindungsdienst**.

3. Klicken Sie auf **Neu starten**.

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

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

```
dsm_om_connsvc restart
```

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Was ist neu in Version 5.2

Dell™ OpenManage™ Server Administrator: Benutzerhandbuch Version 5.2

- Hinzugefügter Support für Dell™ PowerEdge™ 2970.
- Hinzugefügter Support für Microsoft ® Windows-Server ® 2003-Familie (x86) (SP2 mit Web, Standard und Enterprise Editions).
- Hinzugefügter Support für Microsoft Windows-Server 200364-Familie (x86) (SP2 mit Web, Standard und Enterprise Editions).
- Hinzugefügter Support für Microsoft Windows Server 2003 R2 Standard, Enterprise und Datacenter x64 Editions mit SP2
- Hinzugefügter Support für Red Hat® Enterprise Linux ® Server 5 (x86) und (x86_64)-Systeme.
- Hinzugefügter Support für die sichere Socket-Schicht (SSL)-Verschlüsselung auf der Servereinstellungsseite.
- Hinzugefügter Support für Mozilla Firefox 2.0 Browser.
- Hinzugefügter Support für NIS-, Kerberos, LDAP- und Winbind-Authentifizierungsprotokolle für Linux-Betriebssysteme.
- Hinzugefügter Support für Intel ® und AMD™-Branding auf der Seite Prozessorinformationen.
- Hinzugefügte neue Einstellung auf der Seite Einstellungen→ SNMP-Konfiguration, um die SNMP-Satzvorgänge zu konfigurieren.

ANMERKUNG: SNMP-Satzvorgänge sind standardmäßig in Server Administrator deaktiviert.

Zurück zum Inhaltsverzeichnis