Dell™ Remote Console Switch
Benutzerhandbuch

Wichtige Hinweise, Hinweise und Vorsichtsmaßnahmen

HINWEIS: Ein HINWEIS weist auf Informationen hin, die Ihnen helfen, Ihren Rechner effizienter einzusetzen.

WICHTIGER HINWEIS: Ein WICHTIGER HINWEIS weist auf eine mögliche Beschädigung der Hardware oder auf Datenverlust hin und zeigt Ihnen, wie das Problem vermieden werden kann.

VORSICHT: VORSICHT weist auf mögliche Sachschäden, Personenschäden oder tödliche Verletzungen hin.

Zusätzliche Software: Sie erkennen an, dass das SOFTWAREPRODUKT urheberrechtlich geschützte Software von Dell Zulieferfirmen enthalten oder einschließen kann, die in der beiliegenden Dokumentation bzw. in anderen gedruckten oder elektronischen Materialien beschrieben („Zusätzliche Software“) und mit einer entsprechenden Lizenz von diesen Zulieferfirmen zur Verfügung gestellt wird. Ihre Verwendung solcher zusätzlicher Software unterliegt den geltenden Einschränkungen und anderen Bestimmungen und Bedingungen, die in der entsprechenden Dokumentation oder den Materialien in einer ReadMe-Datei zu „Zusätzlichen Softwarelizenzen“ bzw. einer vergleichbaren Datei im Installationsverzeichnis für das SOFTWAREPRODUKT dargelegt sind, und Sie stimmen der Einhaltung dieser Einschränkungen und Bedingungen zu.

Die Bereitstellung jeglicher Open Source-Software erfolgt in der Erwartung, dass sich diese als nützlich erweist, aber ohne Mängelgewähr und ohne ausdrückliche oder stillschweigende Garantie einschließlich, aber nicht beschränkt auf die Gewährleistung der Marktgängigkeit oder Eignung für einen bestimmten Zweck. Dell, die Inhaber der Urheberrechte und die jeweiligen Mitarbeiter schließen jegliche Haftung aus Verträgen oder unbeschränkte Schadenshaftung (einschließlich Fahrlässigkeit u. a.) aus. Diese Haftungsbeschränkung gilt für direkte, indirekte, zufällige, außerordentliche, exemplarische Schäden oder Folgeschäden (einschließlich, aber nicht beschränkt auf die Beschaffung von Ersatzwaren oder Dienstleistungen, Verlust von Daten, entgangenem Gewinn oder Geschäftsunterbrechung), die durch die Verwendung dieser Software verursacht werden oder daraus entstanden sind, ungeachtet jeglicher Haftungstheorie, selbst wenn auf die Möglichkeit solcher Schäden hingewiesen wurde.

In diesem Text verwendete Marken: *Avocent* ist eine eingetragene Marke der Avocent Corporation. *OSCAR* ist eine eingetragene Marke der Avocent Corporation oder ihrer Tochterunternehmen. *Dell*, *OpenManage* und das DELL Logo sind Marken von Dell Inc.; *Active Directory*, *DirectDraw*, *Internet Explorer*, *Microsoft*, *Win32*, *Windows*, *Windows NT*, *Windows Server* und *Windows Vista* sind entweder Marken oder eingetragene Marken der Microsoft Corporation in den USA und/oder in anderen Ländern; *Intel* und *Pentium* sind eingetragene Marken der Intel Corporation; *Red Hat* und *Red Hat Enterprise Linux* sind eingetragene Marken von Red Hat, Inc.; *SUSE* ist eine eingetragene Marke von Novell Inc. in den USA und in weiteren Ländern; *UNIX* ist eine eingetragene Marke der Open Group in den USA und in weiteren Ländern; *Sun*, *Sun Microsystems* und das Logo von Sun sind Marken bzw. eingetragene Marken von Sun Microsystems, Inc. oder den angeschlossenen Tochtergesellschaften in den USA und in weiteren Ländern.

Möglicherweise werden andere Marken und Markennamen in diesem Dokument verwendet, um auf Eigentümer dieser Marken und Namen oder deren Produkte zu verweisen. Dell Inc. weist jegliche Eigentumsinteressen an Marken und Markennamen anderer von sich.

590-1049- 503A

Oktober 2010

Modell 2161DS-2/4161DS/2321DS Remote Console Switch

Sicherheits- und EMV-Zulassungen und Kennzeichnungen

- UL / cUL
- CE – EU
- N (Nemko)
- GOST
- C-Tick
- NOM / NYCE
- MIC (BCC)
- SASO
- GS
- IRAM
- FCC, ICES,
- VCCI
- SONCAP
- SABS
- Bellis
- FIS / Kvalitet
- Koncar
- KUCAS
- INSM
- Ukrtest
- STZ Z

Die Sicherheits- und EMV-Zulassungen für dieses Produkt werden unter einer oder mehreren der folgenden Bezeichnungen angegeben: Zertifizierungs-Modellnummer (CMN), Hersteller-Teilnummer (MPN) oder Bezeichnung des Vertriebsstufenmodells (Sales Level Model). Die Bezeichnung, wie sie in den EMV- und/oder Sicherheitsberichten aufgeführt wird, befindet sich auf dem Geräteaufkleber.

Ausführlichere Angaben bezüglich EMV und EA entnehmen Sie bitte dem *Dell Regulatory Technical Bulletin*, das Ihrem Remote Console Switch beiliegt.

Inhaltsverzeichnis

Sicherheitsvorkehrungen

Die folgenden Sicherheitsrichtlinien helfen Ihnen, Ihre eigene Sicherheit zu gewährleisten und Ihr System und Arbeitsumfeld vor potentiellen Störungen zu bewahren.

⚠ **VORSICHT: Die Stromversorgung Ihres Systems kann möglicherweise hohe Spannungen und Energiegefahrenquellen erzeugen, die Verletzungen verursachen können. Das Entfernen von Abdeckungen und der Zugriff auf Komponenten innerhalb des Systems darf nur von autorisierten Wartungstechnikern durchgeführt werden. Dieser Warnhinweis gilt für Dell™ PowerEdge™ Server und Dell PowerVault™ Speichersysteme.**

Dieses Dokument bezieht sich nur auf den Dell 2161DS-2/4161DS/2321DS Console Switch. Sie sollten außerdem die ergänzenden Sicherheitsanweisungen lesen und befolgen.

- Die Ihrer Racklösung beigelegte *Remote Console Switch-Installationsanleitung*, die die Installation des Systems im Rack beschreibt.
- Das *Benutzerhandbuch*, das Informationen zu Einrichtung und Betrieb Ihres rackmontierten Serversystems liefert.
- Bei Bedarf die entsprechende Avocent Installationsanleitung und das Benutzerhandbuch für Ihr Produkt. Weitere Informationen finden Sie unter www.avocent.com/manuals.

Allgemeine Sicherheitsvorkehrungen

- Beachten und befolgen Sie die Wartungsbeschriftungen.
- Warten Sie alle Produkte nur gemäß den Anweisungen in der entsprechenden Systemdokumentation.
- Das Öffnen und Entfernen von Abdeckungen, die mit einem dreieckigen Symbol mit Blitzzeichen gekennzeichnet sind, kann Sie möglicherweise einem elektrischen Stromschlag aussetzen.
- Die Komponenten in diesen Einheiten sollten nur von qualifizierten Wartungstechnikern gewartet werden.
  - Dieses Produkt enthält keine Komponenten, die gewartet werden können. Nicht öffnen.

- Wenn einer der folgenden Fälle eintritt, unterbrechen Sie die Verbindung des Produkts zur elektrischen Stromversorgung und ersetzen Sie das Teil, oder nehmen Sie Kontakt mit einem qualifizierten Kundendienstmitarbeiter auf:
  - Netzkabel, Verlängerungskabel oder Stecker sind beschädigt.
  - Ein Gegenstand ist in das Produkt gefallen.
  - Das Produkt wurde Wasser ausgesetzt.
  - Das Produkt ist heruntergefallen und/oder wurde beschädigt.
  - Das Produkt arbeitet nicht ordnungsgemäß bei Befolgen der Bedienungsanleitung.
- Stellen Sie das System nicht in der Nähe von Heizkörpern und Wärmequellen auf. Achten Sie darauf, dass die Lüfteröffnungen nicht blockiert sind.
- Stellen Sie sicher, dass keine Lebensmittel oder Flüssigkeiten auf die Systemkomponenten geraten, und betreiben Sie das Produkt niemals in einer feuchten Umgebung. Wird das System Feuchtigkeit ausgesetzt, sehen Sie im entsprechenden Abschnitt der Anleitung zur Störungsbeseitigung nach, oder nehmen Sie Kontakt mit einem qualifizierten Kundendienstmitarbeiter auf.
- Verwenden Sie das Produkt nur mit zugelassenen Geräten.
- Lassen Sie das Gerät abkühlen, bevor Sie Abdeckungen entfernen oder interne Komponenten berühren.
- Betreiben Sie das Produkt nur mit einer externen Stromversorgung, die den auf dem Produktaufkleber angegebenen elektrischen Nennwerten entspricht. Wenn Unklarheiten darüber bestehen, welche Art von Stromversorgung benötigt wird, nehmen Sie Kontakt mit Ihrem Fachhändler oder der örtlichen Elektrizitätsgesellschaft auf.

WICHTIGER HINWEIS: Um Beschädigungen an Ihrem System zu vermeiden, stellen Sie sicher, dass der Spannungswahlschalter (falls vorhanden) an der Stromversorgung auf die Spannung eingestellt ist, die dem am Standort verfügbaren Wechselstrom am ehesten entspricht. Stellen Sie außerdem sicher, dass Ihr Monitor und die angeschlossenen Geräte mit der geeigneten Stromversorgung betrieben werden.

- Stellen Sie sicher, dass Ihr Monitor und die angeschlossenen Geräte mit der am Standort verfügbaren Stromversorgung entsprechend ihrer Nennwerte betrieben werden können.
- Verwenden Sie nur die mit dem Produkt gelieferten Netzkabel.

- Zur Vermeidung von Elektroschocks müssen die Stromkabel des Systems und der Peripheriegeräte in ordnungsgemäß geerdete Steckdosen gesteckt werden. Diese Kabel sind mit dreipoligen Steckern versehen, um eine ordnungsgemäße Erdung sicherzustellen. Verwenden Sie keine Adapterstecker, und entfernen Sie den Erdungsanschluss eines Kabels nicht.
- Beachten Sie die Nennleistung von Verlängerungskabeln und Mehrfachsteckdosen. Stellen Sie sicher, dass die Gesamt-Amperestromstärke aller Geräte, die an eine Mehrfachsteckdose angeschlossen sind, 80 % der maximalen Amperestromstärkeleistung der Mehrfachsteckdose nicht überschreitet.
- Schützen Sie Ihr System vor plötzlichen kurzzeitigen Stromversorgungsschwankungen durch die Verwendung eines Überspannungsbegrenzers, Line Conditioner oder einer unterbrechungsfreien Stromversorgung (USV).
- Verlegen Sie alle System- und Stromkabel mit größter Sorgfalt. Verlegen Sie die Kabel so, dass man nicht darauf tritt oder darüber stolpert. Stellen Sie sicher, dass keine Gegenstände auf den Kabeln liegen.
- Nehmen Sie keine Veränderungen an Stromkabeln und Steckern vor. Nehmen Sie bzgl. baulicher Veränderungen Kontakt mit einem qualifizierten Elektriker oder Ihrer Elektrizitätsgesellschaft auf. Befolgen Sie stets die maßgeblichen Verkabelungsvorschriften.

Rackbefestigung von Systemen

- Beachten Sie die dem Rack beigelegte Installationsdokumentation bzgl. spezifischer Vorsichtshinweise und -maßnahmen.
- Rack-Kits für Systeme müssen von einem qualifizierten Wartungstechniker im Rack befestigt werden. Wird ein Rack von einem anderen Hersteller als Dell verwendet, stellen Sie sicher, dass das Rack den Spezifikationen eines Dell-Racks entspricht.
- Erhöhte Umgebungstemperatur: Beim Einbau in geschlossenen Rack-Gruppen kann es vorkommen, dass die Betriebstemperatur in der Rack-Umgebung höher als die Raumtemperatur ist. Achten Sie darauf, dass die auf der Einheit angegebene maximale Umgebungstemperatur nicht überschritten wird.

- Unzureichende Belüftung: Der Einbau von Geräten im Rack muss so vorgenommen werden, dass die für den sicheren Betrieb der Geräte benötigte Luftzufuhr sichergestellt ist.
- Mechanische Belastung: Der Einbau von Geräten im Rack muss unter Berücksichtigung einer gleichmäßigen mechanischen Belastung erfolgen, damit Gefahrensituationen aufgrund von ungleichmäßiger Belastung vermieden werden.
- Stromkreisüberlastung: Es muss darauf geachtet werden, welche Auswirkungen der Anschluss der Geräte an den Versorgungsstromkreis und eine Überlastung des Stromkreises auf den Überlastungsschutz und die Verkabelung haben können. Die maximalen Spannungswerte sind auf den Typenschildern der Geräte angegeben.
- Zuverlässige Geräteerdung: Achten Sie darauf, dass der Erdungsanschluss für rackmontierte Geräte dauerhaft zuverlässig ist. Achten Sie vor allem auf Stromanschlüsse, die nicht direkt an den Versorgungsstromkreis angeschlossen sind (z. B. bei Verwendung von Mehrfachsteckdosen).

LAN-Optionen

- Nicht während eines Gewitters anschließen oder verwenden. Es besteht die Gefahr eines Elektroschocks durch Blitzschlag.
- Niemals in feuchter Umgebung anschließen oder verwenden.

1

Produktüberblick

Der Dell™ 2161DS-2/4161DS/2321DS Remote Console Switch für mehrere Benutzer kombiniert die bewährte digitale Dell KVM-Switching-Technologie (Keyboard, Video, Mouse) mit ausgereiftem Kabelmanagement, flexiblem Zugriff für bis zu vier Benutzer gleichzeitig sowie einer patentierten Benutzeroberfläche der nächsten Generation. Der Remote Console Switch beinhaltet USB- und PS/2-Ports auf der Benutzerseite, die alle gängigen Geräteplattformen unterstützen.

Unter Verwendung der leistungsstarken On-Screen-Verwaltung über die Avocent™ OSCAR™-Benutzeroberfläche ermöglichen die Remote Console Switch Software oder die integrierte Weboberfläche eine einfache Systemkonfiguration und Geräteauswahl.

Merkmale und Vorteile des Remote Console Switches

Intelligentes SIP-Modul

Der Remote Console Switch bietet darüber hinaus die Funktionalität des intelligenten SIP-Moduls. Das SIP-Modul mit CAT 5-Design reduziert das Kabelaufkommen entscheidend und bietet gleichzeitig optimale Bildschirmauflösungen und Monitoreinstellungen. Der integrierte Speicher des SIP-Moduls vereinfacht die Konfiguration durch Zuweisen und Speichern eindeutiger Gerätenamen oder elektronischer Kennnummern (EID) für jedes angeschlossene Gerät. Das SIP-Modul wird direkt über das Gerät mit Strom versorgt und verfügt selbst bei ausgeschaltetem Remote Console Switch über eine „Keep Alive"-Funktion.

Es sind PS/2- und USB-SIP-Module erhältlich, die eine direkte KVM-Konnektivität zu Geräten ermöglichen. Außerdem ist ein USB2-Virtual-Media-SIP erhältlich. Jeder Remote Console Switch verfügt über bis zu 32 ARI-Ports (Analog Rack Interface) für den Anschluss von SIP-Modulen.

Mithilfe eines SIP-Moduls können Sie das Remote Console Switch-System um zusätzliche Switches erweitern. Mit dieser Flexibilität kann die Leistungsfähigkeit Ihres Systems an zunehmende Datenmengen angepasst werden.

Multi-Plattform-Support

Die für die Verwendung mit dem Remote Console Switch erhältlichen Dell SIP-Module unterstützen PS/2-, USB- und USB2-Geräteumgebungen. Wenn diese Module in Verbindung mit der OSCAR® Benutzeroberfläche eingesetzt werden, ist ein einfaches Umschalten zwischen Plattformen möglich.

Kompatibilität mit den intelligenten Kabeln von Avocent® IQ-Modulen

Das intelligente Kabel des IQ-Moduls von Avocent kann ebenfalls zum Anschluss von Geräten an den Remote Console Switch eingesetzt werden. Erhältlich sind PS/2-, USB-, Sun®- und serielle Kabeloptionen. Weitere Informationen entnehmen Sie bitte der entsprechenden Avocent Installationsanleitung und dem Benutzerhandbuch für Ihr Produkt. Weitere Informationen finden Sie unter www.avocent.com/manuals.

OSCAR-Benutzeroberfläche

Sie können den Remote Console Switch mithilfe der Avocent OSCAR-Benutzeroberfläche verwalten. Die OSCAR-Benutzeroberfläche bietet intuitive Menüs, mit denen Sie Ihr Switch-System konfigurieren und Rechner auswählen können. Geräte können über Namen, EIDs oder Portnummern identifiziert werden, wodurch eine eindeutige Zuweisung von Gerätenamen ermöglicht wird.

Integrierte Weboberfläche

Die integrierte Weboberfläche bietet ähnliche Verwaltungsfunktionen wie die Remote Console Switch Software, erfordert aber keinen Software-Server und keine Installation. Die integrierte Weboberfläche wird direkt vom Switch aus gestartet und alle Server, die an den Remote Console Switch angeschlossen sind, werden automatisch erkannt. Sie können die integrierte Weboberfläche verwenden, um Remote Console Switches über einen Webbrowser zu konfigurieren. Starten Sie den Viewer über die integrierte Weboberfläche, um KVM- und Virtual Media-Sitzungen zu Zielgeräten aufzubauen. Die integrierte Weboberfläche unterstützt zudem LDAP-Authentifizierung, wodurch die Zugriffsberechtigungen für mehrere Remote Console Switches über eine zentrale Oberfläche verwaltet werden können.

DSView® 3 Managementsoftware-Plug-in

Die Avocent DSView 3 Managementsoftware ist eine sichere, Webbrowser-basierte zentrale Verwaltungslösung für Unternehmen, mit deren Hilfe Benutzer über verwaltete Einheiten auf die Zielgeräte zugreifen und diese verwalten, überwachen und steuern können. Von einem zentralen Zugriffspunkt aus kann gezielt eine Sitzung zu einem Zielgerät gestartet werden.

Mit der DSView 3 Software können Sie Server und Geräte verschiedener Hersteller verwalten und entsprechende Verbindungen herstellen. Über das DSView 3 Software-Plug-in lässt sich der Dell Remote Console Switch in die heterogene Netzwerkumgebung der DSView 3 Software integrieren. Sobald ein Remote Console Switch hinzugefügt wurde, können Sie die DSView 3 Software für Fehlerbehandlung, Sitzungsmanagement sowie Firmware-Aktualisierungen und vieles mehr nutzen.

Virtual Media

Virtual Media ermöglicht die Anzeige von Daten, die sich auf virtuellen Speichergeräten befinden, auf einem beliebigen, an den Remote Console Switch angeschlossenen Server. Außerdem können Sie die Daten zwischen den Speichergeräten und Servern verschieben und kopieren. Remote-Systeme lassen sich effizienter verwalten, indem die Installation und Wiederherstellung von Betriebssystemen, die Wiederherstellung oder Duplizierung von Festplatten sowie BIOS-Aktualisierungen und Server-Backups über Remote-Zugriff ermöglicht werden.

Virtual Media-Geräte können direkt an die USB-Ports am Switch oder am Server, über den die Browsersitzung der integrierten Weboberfläche läuft, angeschlossen werden. Sie können eine Virtual Media-Sitzung zu einem Server über den Viewer öffnen. Der Viewer kann sowohl über die integrierte Weboberfläche als auch über die Remote Console Switch Software geöffnet werden.

HINWEIS: Um eine Virtual Media-Sitzung mit einem Server zu öffnen, muss der Server zunächst über ein Virtual Media-fähiges USB2-SIP-Modul an einen Remote Console Switch angeschlossen werden.

Sicherheit

Mit der OSCAR-Benutzeroberfläche können Sie Ihr System durch ein Bildschirmschoner-Kennwort schützen. Der Bildschirmschoner-Modus wird aktiviert und es ist kein Zugriff möglich, bis das entsprechende Kennwort zur Reaktivierung des Systems eingegeben wird. Wenn Sie im Dialogfeld für das Kennwort Hilfe eingeben, werden Sie an den technischen Kundendienst von Dell weitergeleitet.

Es wird empfohlen, den Remote Console Switch in einer durch eine Firewall geschützten Datencenter-Infrastruktur zu verwenden.

Verschlüsselung

Der Remote Console Switch unterstützt 128-Bit-SSL- sowie AES-, DES- und 3DES-Verschlüsselung von Tastatur-/Maus-, Video- und Virtual Media-Sitzungen.

Betriebsmodi

Die OSCAR-Benutzeroberfläche bietet praktische Betriebsmodi zur einfachen Systemverwaltung des Remote Console Switches. Mit diesen Modi (Senden, Scannen, Switching und Teilen) können Sie Ihre Switching-Aktivitäten verwalten. In Kapitel 3, „Steuern des Systems über die Analogports“ auf Seite 35, werden diese Modi genauer erläutert.

Video

Der Remote Console Switch bietet eine optimale Bildschirmauflösung für analoges VGA, SVGA und XGA. Je nach Kabelabstand zwischen Switch und Servern können Auflösungen von bis zu 1024 x 768 erzielt werden.

Tabelle 1-1. Maximale Auflösung bei Bildwiederholfrequenz nach Videotyp

720 x 400 bei 70 Hz VGA
640 x 480 bei 60 Hz VGA
640 x 480 bei 72 Hz VESA
640 x 480 bei 75 Hz VESA
800 x 500 bei 60 Hz VESA
800 x 600 bei 56 Hz VESA
800 x 600 bei 60 Hz VESA
800 x 600 bei 70 Hz VESA
800 x 600 bei 75 Hz VESA
1024 x 640 bei 60 Hz VESA
1024 x 768 bei 60 Hz VESA
1024 x 768 bei 70 Hz VESA
1024 x 768 bei 75 Hz VESA
1280 x 800 bei 60 Hz VESA

FLASH-Aktualisierung

Sie können Ihren Remote Console Switch und die SIP-Module jederzeit aktualisieren und damit gewährleisten, dass Ihr System immer mit der neuesten Firmware-Version ausgeführt wird. FLASH-Aktualisierungen können über die OSCAR-Benutzeroberfläche, die integrierte Weboberfläche oder die serielle Konsole eingeleitet werden. Der Remote Console Switch kann so konfiguriert werden, dass automatische Firmware-Aktualisierungen der SIP-Module durchgeführt werden. Weitere Informationen finden Sie unter „Anhang D: FLASH-Aktualisierungen“ auf Seite 225.

Kaskadierte (gestufte) Erweiterung

Die Remote Console Switch-Funktionen ermöglichen eine Kaskadierung mit zusätzlichen Dell Console Switches über jeden ARI-Port (Analog Rack Interface) am Switch. Die kaskadierten Switches werden genau wie andere Geräte angeschlossen. Mithilfe dieser zusätzlichen gestuften Einheiten können Sie bis zu 512 Server in einem System verbinden. Siehe „Hinzufügen eines kaskadierten Switches“ auf Seite 27.

Merkmale und Vorteile der Remote Console Switch Software

HINWEIS: Anweisungen zur Verwendung der Remote Console Switch-Software finden Sie in der Bedienungsanleitung der Dell Remote Console Switch-Software oder in der in die Software integrierten Hilfe.

Die Dell™ Remote Console Switch Software ist eine plattformübergreifende Verwaltungsanwendung, mit der Dell Remote Console Switches und alle angeschlossenen Server überwacht und gesteuert werden können. Das plattformübergreifende Design stellt Kompatibilität mit den meisten gängigen Betriebssystemen und Hardware-Plattformen sicher. Die Remote Console Switch Software bietet sichere switchbasierte Authentifizierung, Datenübertragung und Speicherung von Benutzername/Kennwort. Authentifizierung und Zugangskontrolle werden individuell von jedem Switch durchgeführt, um so die Systemsteuerung zu dezentralisieren.

Die Remote Console Switch Software verwendet eine Explorer-ähnliche Navigationsoberfläche mit einer intuitiven Bildschirmunterteilung und ermöglicht damit den gezielten und umfassenden Zugriff auf Ihr gesamtes System. Sie können alle vorhandenen Switches verwalten, neue Switches einrichten oder eine Videositzung mit einem Systemserver starten. Durch vordefinierte Gruppierungen wie Server, Standorte und Verzeichnisse wird die Auswahl der anzuzeigenden Einheiten leicht gemacht. Dank leistungsfähiger Such- und Sortierfunktionen können Sie beliebige Einheiten mühelos auffinden.

Einfache Installation und Konfiguration

Die Remote Console Switch Software ist einfach zu installieren und zu bedienen. Die automatische Erkennung der verwalteten Switches ermöglicht das Installieren neuer Einheiten in Minutenschnelle. Die Installation mithilfe eines Assistenten und die Online-Hilfe erleichtern die anfängliche Konfiguration des Systems. Über die intuitive grafische Benutzeroberfläche können die Switches einfach und direkt verwaltet und aktualisiert werden.

Umfassende Anpassungsfähigkeit

Die Remote Console Switch Software lässt sich an Ihre spezifischen Systemanforderungen anpassen. Nutzen Sie vordefinierte Gruppen oder erstellen Sie Ihre eigenen. Erstellen Sie benutzerorientierte Einheiten- und Feldbezeichnungen und Symbole für ein Höchstmaß an Flexibilität und Benutzerfreundlichkeit. Die Verwendung aussagekräftiger Namen erleichtert das Auffinden von Systemeinheiten.

Umfassende Verwaltung der Remote Console Switches

Mithilfe der Remote Console Switch Software können Sie mehrere Switches in einem System hinzufügen und verwalten. Sobald ein neuer Switch installiert wurde, können Sie Switch-Parameter konfigurieren, Benutzer-Videositzungen steuern und trennen sowie zahlreiche Steuerungsfunktionen ausführen, z. B. Neustarten und Aktualisieren von Switches. Die Remote Console Switch Software ist kompatibel mit dem Dell OpenManage™ IT Assistant Event Viewer und erlaubt somit Systemadministratoren, Systemereignisberichte zusammenzufassen.

IPv4- und IPv6-Funktionen

Der Remote Console Switch ist mit Systemen kompatibel, die IPv4 oder IPv6, die beiden derzeit verwendeten Internetprotokollversionen, verwenden. Sie können die Netzwerkeinstellungen ändern und über den seriellen Port, die OSCAR-Benutzeroberfläche oder die integrierte Weboberfläche den IPv4- oder den IPv6-Modus auswählen.

LDAP

Die Dell Remote Console Switch Software ermöglicht, dass die Zugriffsberechtigungen für mehrere Remote Console Switches über eine einzige Schnittstelle verwaltet werden können, anstatt jeden Remote Console Switch einzeln verwalten zu müssen. Die LDAP-Funktionalität sorgt für erhöhte Sicherheit und Effizienz, da die Notwendigkeit entfällt, Zugriffsberechtigungen für individuelle Remote Console Switches zu aktualisieren, indem Berechtigungen über eine einzige netzwerkweite Authentifizierungsquelle vergeben werden.

Die Dell Remote Console Switches können die Authentifizierung unter Verwendung des Active Directory-Standardschemas oder des erweiterten Dell Schemas durchführen, um maximale Kompatibilität mit Dell Hardwarekomponenten zu bieten.

Kompatibilität mit Avocent-Produkten

Die Remote Console Switch Software kann auch zur Verwaltung bestimmter Avocent Switches eingesetzt werden, wodurch eine erhöhte Flexibilität bei der Verwaltung von Systemen erreicht wird.

Außerdem bietet die Remote Console Switch Software Unterstützung für Avocent IQ-Module und erweitert somit die Auswahl an Servertypen, die verwaltet werden können. Durch die zusätzliche Unterstützung von Avocent IQ-Modulen werden nun auch die folgenden Verbindungen unterstützt:

- PS/2-Module (Module von Dell und Avocent erhältlich)
- USB-Module (Module von Dell und Avocent erhältlich)
- Serielle Module (Avocent-Module erhältlich)
- Sun-Module (Avocent-Module erhältlich)
- PS2M-Module (Avocent-Module erhältlich)

HINWEIS: Dell SIPs werden an direkt verbundenen Avocent Switches nicht unterstützt.

2

Installation

Das Remote Console Switch-System umfasst den Remote Console Switch, die Remote Console Switch Software und die integrierte Weboberfläche. Sie können entweder die Remote Console Switch Software oder die integrierte Weboberfläche für die Verwaltung Ihres Systems nutzen. Mit der integrierten Weboberfläche kann ein einzelner Remote Console Switch und dessen Verbindungen verwaltet werden, während die Remote Console Switch Software die Verwaltung von mehreren Switches und ihren Verbindungen ermöglicht.

Wenn Sie sich für die Verwendung der integrierten Weboberfläche entscheiden, ist es nicht notwendig, die Remote Console Switch Software zu installieren. Wenn Sie die Remote Console Switch Software bereits verwendet haben, können Sie die Datenbank auf die integrierte Weboberfläche migrieren. Siehe „Migration von Remote Console Switches zur integrierten Weboberfläche“ auf Seite 142.

HINWEIS: Stellen Sie sicher, dass alle Remote Console Switches auf die entsprechende aktuelle Firmware-Version aktualisiert wurden. Informationen zum Aktualisieren eines Remote Console Switches über die integrierte Weboberfläche finden Sie unter „Aktualisieren der Firmware“ auf Seite 125.

Schnell-Setup-Checkliste für den Remote Console Switch

So richten Sie den Remote Console Switch ein (siehe „Remote Console Switch Installation und Setup“ auf Seite 10):

1. Stellen Sie die Mausbeschleunigung auf jedem Server auf **Langsam** oder **Keine** ein.
2. Installieren Sie die Remote Console Switch-Hardware, und schließen Sie ein SIP (Server Interface Pod) oder Avocent IQ-Modul an jeden Server oder gestuften Switch an. Schließen Sie alle SIPs oder Avocent IQ-Module über CAT 5-Kabel an den Remote Console Switch an, und schließen Sie die Tastatur-, Monitor- und Mausstecker an den Analogport des Remote Console Switches an.

3 Schließen Sie ein Terminal an den seriellen Konfigurationsport auf der Rückseite des Remote Console Switch an und richten Sie die Netzwerkkonfiguration ein (Netzwerkgeschwindigkeit und Adresstyp). Die IP-Adresse kann hier oder über die Remote Console Switch Software eingestellt werden. Zur einfacheren Konfiguration empfiehlt Dell die Verwendung einer statischen IP-Adresse.

4 Geben Sie unter Verwendung der lokalen Portkonfiguration alle Servernamen über die OSCAR-Benutzeroberfläche ein.

Anweisungen zur Verwendung der Remote Console Switch-Software finden Sie in der Bedienungsanleitung der Dell Remote Console Switch-Software oder in der in die Software integrierten Hilfe.

Remote Console Switch Installation und Setup

Das Remote Console Switch-System verwendet die Infrastruktur des Ethernet-Netzwerks und das TCP/IP-Protokoll, um Informationen über Tastatur, Monitor und Maus zwischen Benutzer und angeschlossenen Rechnern zu übertragen. Obwohl 10BaseT Ethernet oder Gigabit verwendet werden kann, empfiehlt Dell ein dediziertes geswitchtes 100BaseT-Netzwerk.

Erste Schritte

Überprüfen Sie vor der Installation des Remote Console Switches anhand der folgenden Liste, ob alle im Lieferumfang des Remote Console Switches enthaltenen Teile sowie weitere für eine ordnungsgemäße Installation erforderlichen Teile vorhanden sind.

Im Lieferumfang des Remote Console Switches enthalten:

- Remote Console Switch-Einheit
- Länderspezifisches Netzstromkabel
- 0-HE-Befestigungshalterung
- 1-HE-Befestigungshalterung
- Befestigungskit für 1-HE-Befestigungshalterung
- Serielles Kabel
- CAT 5-Kabel
- Benutzerhandbuch auf CD-ROM für das Remote Console Switch-System

- Installationsanweisungen
- Sicherheitshandbuch
- Handbuch mit Vorschriften

Zusätzlich benötigte Teile:

- Ein Dell SIP oder IQ-Modul pro angeschlossenes Gerät
- Ein CAT 5-Patchkabel pro angeschlossenes Gerät (bis zu 30 m)

Optionales Zubehör:

- Front-Zugangsplatte
- Port Expansion Module (PEM)

HINWEIS: Eine Virtual Media-Sitzung kann nicht mit einem Server aufgebaut werden, der an ein PEM angeschlossen ist.

Einrichten des Netzwerks

Das Remote Console Switch-System verwendet IP-Adressen zur eindeutigen Identifizierung der Remote Console Switch-Einheiten sowie der Rechner, auf denen die Remote Console Switch Software ausgeführt wird. Der Remote Console Switch unterstützt DHCP und statische IP-Adressen. (Wenn Sie Ihre Remote-Software mit dem vorhergehenden 2161DS Switch verbinden, müssen Sie BootP anstelle von DHCP verwenden.)

HINWEIS: Anweisungen zur Verwendung der Remote Console Switch-Software finden Sie in der Bedienungsanleitung der Dell Remote Console Switch-Software oder in der in die Software integrierten Hilfe.

Tastaturen

USB- oder PS/2-Tastaturen können an den Analogport des Remote Console Switches angeschlossen werden.

HINWEIS: Der Remote Console Switch unterstützt auch die Verwendung von mehreren Tastaturen und mehreren Mäusen am Analogport. Die Verwendung von mehr als einem Eingabegerät gleichzeitig kann jedoch zu unvorhersehbaren Ergebnissen führen.

Rackbefestigung der Remote Console Switch-Einheit

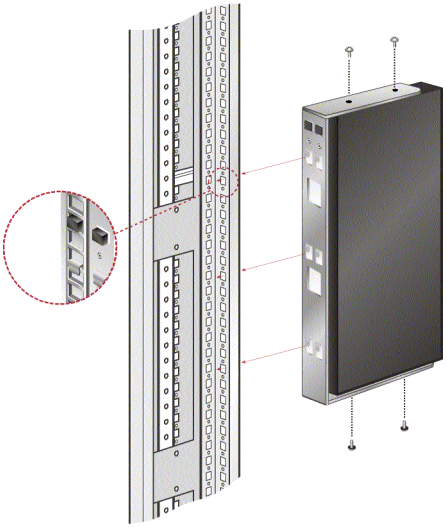
Für die Rackbefestigung der Remote Console Switch-Einheit ist ein Switch-Befestigungskit (0 HE oder 1 HE) erforderlich. Vor der Installation von Remote Console Switches und anderen Komponenten im Rack muss das Rack an seinem vorgesehenen Standort stabilisiert werden. Bestücken Sie das Rack von unten nach oben mit Komponenten. Vermeiden Sie eine ungleichmäßige Belastung und achten Sie darauf, dass das Rack nicht überladen wird.

VORSICHT: Vor der Installation von Systemen in einem Rack müssen Sie bei freistehenden Racks die Front- und Seitenstabilisatoren oder bei einem mit anderen Racks verbundenen Rack die Frontstabilisatoren installieren. Werden vor der Installation der Systeme im Rack keine Stabilisatoren angebracht, kann das Rack umkippen und möglicherweise Verletzungen verursachen. Deshalb sollten vor der Installation der Komponenten in einem Rack stets Stabilisatoren angebracht werden.

So installieren Sie die Switch-Befestigungshalterung für 0 HE (standardmäßig ab Werk):

1. Richten Sie die Bohrungen der Befestigungshalterungen mit den Schraublöchern im Switch aus.
2. Befestigen Sie die Halterung mithilfe der halbrunden Sechskantschrauben an beiden Seiten des Switches.
3. Bauen Sie die Switch-Einheit in das Rack ein, indem Sie die drei Montagehaken an einer Seite der Halterung in die quadratischen Bohrungen im vertikalen Rack einführen.
4. Drücken Sie die Einheit nach unten, bis der blaue Druckknopf herausspringt und hörbar einrastet.

Abbildung 2-1. Installation der 0-HE-Befestigungshalterung



So installieren Sie die 2161DS-2/4161DS Remote Console Switch 1-HE-Vierpunkt-Switchbefestigungshalterung:

1. Entfernen Sie die Schrauben von den Seiten des 1-HE-Vierpunkt-Switches und verwahren Sie sie, um sie später an den Frontteilen der 1-HE-Halterung anzubringen.
2. Richten Sie die Lüfteröffnungen auf der „langen Seite“ der Fronthalterungen des Kits mit den Lüfteröffnungen im Switch aus.

HINWEIS: Die Switchlüfteröffnungen dürfen nicht durch die Halterung verdeckt sein. Dies passiert, wenn die Halterung an der falschen Seite des Switches installiert wird.

3. Richten Sie die Schraublöcher der Halterung an den Schraublöchern im Switch aus.
4. Schrauben Sie die Front-Befestigungshalterungen unter Verwendung eines Kreuzschlitzschraubendrehers mit je zwei Schrauben auf beiden Seiten des Switches an.

5 Befestigen Sie vier Käfigmuttern oder Schnappmuttern so am Rackbefestigungsflansch an der Vorderseite des Rackschranks, dass sich die Mutter an der Innenseite des Racks befindet.

6 Bauen Sie den Switch in das Rack ein, indem die Bohrungen in der „kurzen Seite“ jeder Halterung an der entsprechenden Gruppe passender Bohrungen am Rackschrank ausgerichtet werden. Danach führen Sie die Sechskantverbundschrauben durch die Schlitze in der Halterung und dann durch die Bohrungen in der Montageschiene und in die Käfig- oder Schnappmuttern ein.

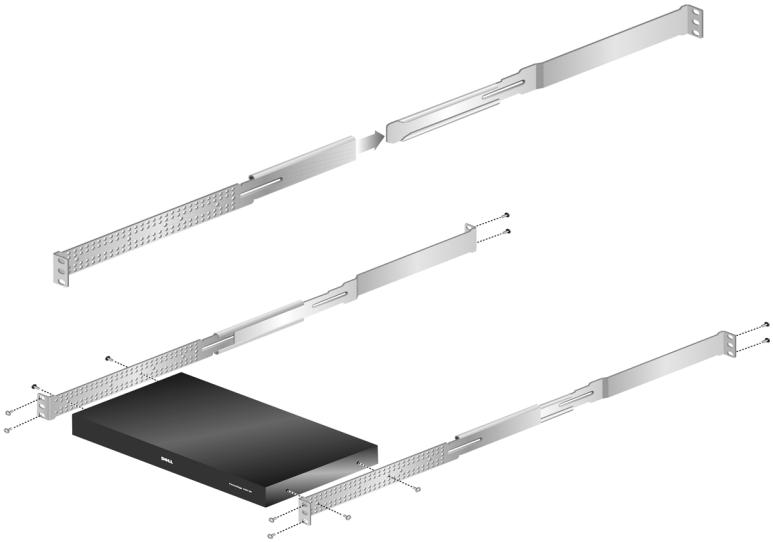
7 Befestigen Sie vier Käfigmuttern oder Schnappmuttern so am Rackbefestigungsflansch an der Rückseite des Rackschranks, dass sich die Mutter an der Innenseite des Racks befindet.

8 Schieben Sie die hinteren Halterungen in den Kanal der Fronthalterungen und stellen Sie sie auf die Tiefe des Racks ein.

9 Bringen Sie die hintere Halterung am Rack an, indem Sie die Bohrungen in der „kurzen Seite“ jeder Halterung an den passenden Bohrungen am Rackschrank ausrichten und dabei sicherstellen, dass der Switch gerade im Rack positioniert ist.

10 Führen Sie die Sechskantverbundschrauben durch die Schlitze in der Halterung und dann durch die Bohrungen in der Montageschiene und in die Käfig- oder Schnappmuttern ein.

Abbildung 2-2. Installation der 2161DS-2/4161DS Remote Console Switch 1-HE-Befestigungshalterung



So installieren Sie die 2321DS Remote Console Switch-Befestigungshalterung:

1. Lösen Sie die Flachrundkopfschraube an der rechten Seite des Switchgehäuses und positionieren und befestigen Sie die rechte Befestigungshalterung mit drei der mitgelieferten Senkkopfschrauben an der rechten Seite des Switchgehäuses.

HINWEIS: Die Switch-Lüfteröffnungen dürfen nicht durch die Halterung verdeckt sein. Dies passiert, wenn die Halterung an der falschen Seite des Switches installiert wird.

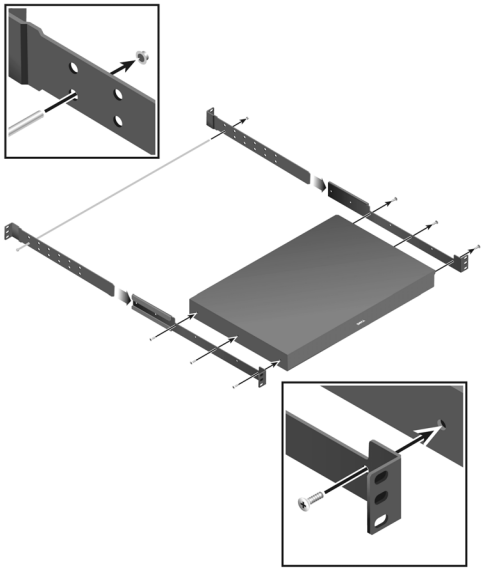
2. Wiederholen Sie den Vorgang für die linke Seite des Switchgehäuses.
3. Befestigen Sie eine Steckmutter an einem Ende der Kabelhalterungsstange. Positionieren Sie die Erweiterungen so, dass deren geschlitzte Befestigungsflansche in entgegengesetzte Richtungen zeigen.
4. Wählen Sie eine Positionsöffnung an der unteren Seite der Schiebererweiterungen aus. Schieben Sie die Kabelhalterungsstange durch die ausgewählte Bohrung und durch die Bohrung an der Erweiterung auf der anderen Seite.

5 Bringen Sie die letzte Steckmutter am anderen Ende der Kabelhalterungsstange an.

6 Schieben Sie die Erweiterung in die Baugruppe mit dem Switchgehäuse und der Halterung (siehe Abbildung). Richten Sie die Erweiterung so aus, dass sich die Kabelhalterungsstange in der unteren Zeile der Erweiterungsbohrungen befindet.

7 Platzieren Sie die gesamte Baugruppe mit Switchgehäuse und Halterung in einer horizontalen Position im Rack und setzen Sie die entsprechende Hardware in jeder der vier Halterungsecken ein (Hardware ist nicht im Lieferumfang enthalten).

Abbildung 2-3. Installation der 2321DS Remote Console Switch-Befestigungshalterung



Installation der Remote Console Switch-Einheit

Das folgende Diagramm zeigt eine mögliche Konfiguration für die Remote Console Switch-Einheit. Befolgen Sie die detaillierten Anleitungen im Anschluss an Abbildung 2-4, um den Remote Console Switch erfolgreich zu installieren.

Abbildung 2-4. Grundkonfiguration – Remote Console Switch

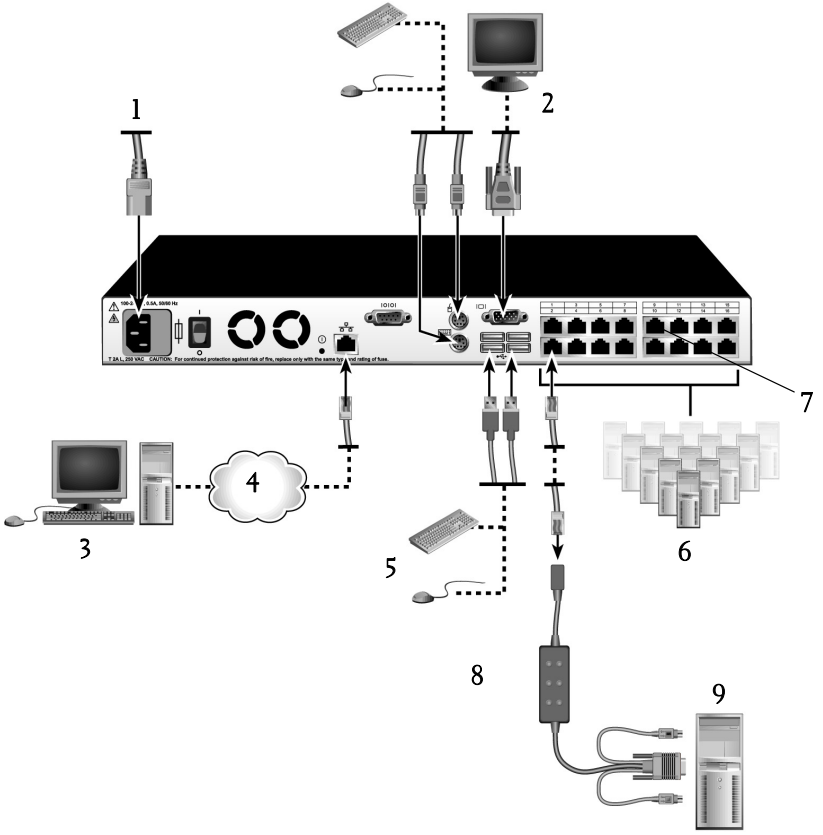


Tabelle 2-1. Beschreibung der Grundkonfiguration eines Remote Console Switches

Anzahl	Beschreibung	Anzahl	Beschreibung
1	Netzkabel	6	Server 2-16
2	Analoger Benutzer	7	ARI-Port
3	Digitaler Benutzer	8	SIP oder IQ-Modul
4	Netzwerk	9	Server 1
5	USB-Geräte		

VORSICHT: Zur Vermeidung von Elektroschocks oder Schäden an Ihrem Gerät muss das Netzkabel immer ordnungsgemäß geerdet sein. Der Masseanschluss ist ein wichtiges Sicherheitsmerkmal. Stecken Sie das Netzkabel in eine geerdete Schukosteckdose, die jederzeit leicht zugänglich sein muss. Um die Stromversorgung zu unterbrechen, ziehen Sie das Netzkabel entweder aus der Netzsteckdose oder aus dem Gerät.

HINWEIS: Verfügt die Stromquelle in Ihrem Gebäude über dreiphasigen Wechselstrom, stellen Sie sicher, dass Rechner und Monitor an der gleichen Phase angeschlossen sind. Somit können phasenbedingte Störungen beim Monitor und/oder bei der Tastatur vermieden werden.

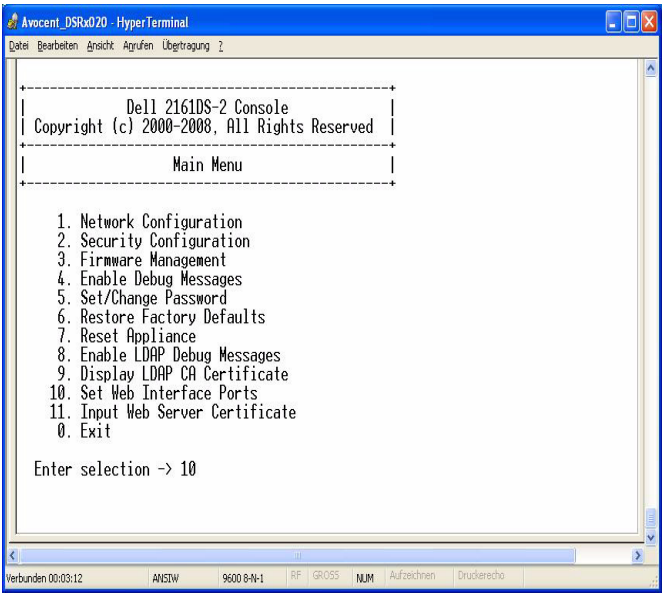
HINWEIS: Die maximale unterstützte Kabellänge zwischen Switch und Gerät beträgt 30 m.

So installieren Sie die Remote Console Switch-Hardware:

HINWEIS: Der Standard-Benutzername ist „Admin". Es ist kein Standard-Kennwort vorhanden.

1. Schließen Sie ein Terminal oder einen PC, auf dem Terminal-Emulationssoftware ausgeführt wird, mit dem mitgelieferten seriellen Kabel an den Konfigurationsport auf der Rückseite der Remote Console Switch-Einheit an. Das Terminal muss wie folgt eingestellt werden: 9600 Baud, 8 Bit, 1 Stoppbit, keine Parität und keine Datenflusskontrolle.
2. Schließen Sie das mitgelieferte Stromkabel an die Rückseite der Remote Console Switch-Einheit und dann an eine geeignete Stromquelle an.
3. Sobald der Strom eingeschaltet wird, blinkt die Stromversorgungsanzeige an der Rückseite der Einheit ca. 30 Sekunden lang, während ein Selbsttest ausgeführt wird. Betätigen Sie die <Eingabetaste>, um das Hauptmenü aufzurufen.

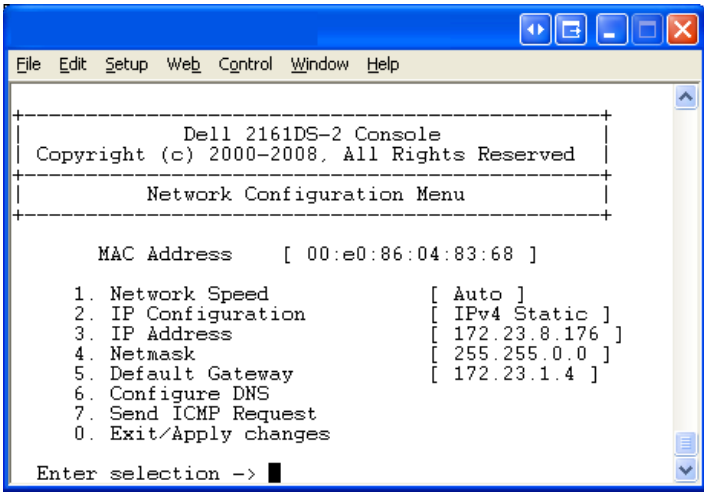
Abbildung 2-5. Hauptmenü



So konfigurieren Sie die Remote Console Switch Hardware:

1 Sie sehen das **Hauptmenü** mit elf Optionen. Wählen Sie Option 1 aus: **Netzwerkkonfiguration**.

Abbildung 2-6. Menü für die Netzwerkkonfiguration



2 Wählen Sie Option 1 aus, um die Netzwerkgeschwindigkeit einzustellen. Sobald Sie die Auswahl bestätigen, wird wieder das Menü **Network Configuration** angezeigt.

3 Wählen Sie Option 2 aus, um das Menü **IP-Configuration** zu öffnen.

4 Geben Sie die entsprechende Zahl ein, um einen der folgenden IP-Adresstypen auszuwählen: 1: **Keine**, 2: **Statische IPv4**, 3: **Dynamische IPv4**, 4: **Statische IPv6** oder 5: **Dynamische IPv6**.

Zur einfacheren Konfiguration empfiehlt Dell die Verwendung einer statischen IP-Adresse.

5 Wählen Sie nacheinander die Optionen 3 - 5 der **Terminal Applications** aus, um die Konfiguration des Remote Console Switches für IP-Adresse, Netzmaske und Standard-Gateway abzuschließen.

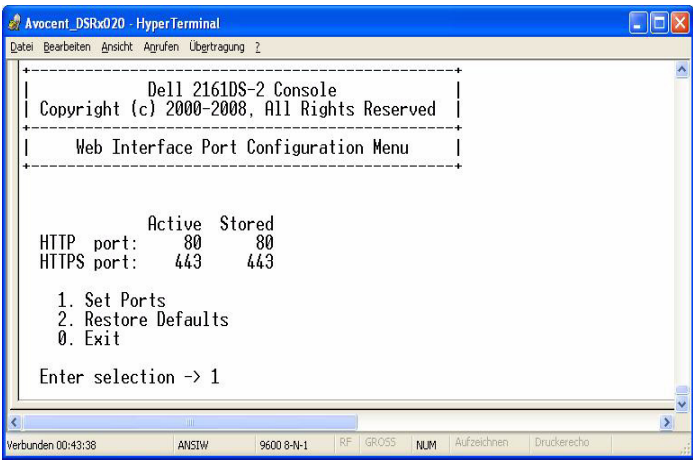
6 Geben Sie zum Abschluss Ø ein, um zum Hauptmenü zurückzukehren.

HINWEIS: Es kann auch eine Netzwerkkonfiguration durchgeführt werden. Siehe „Steuern des Systems über die Analogports“ auf Seite 35.

So konfigurieren Sie die HTTP- und HTTPS-Ports:

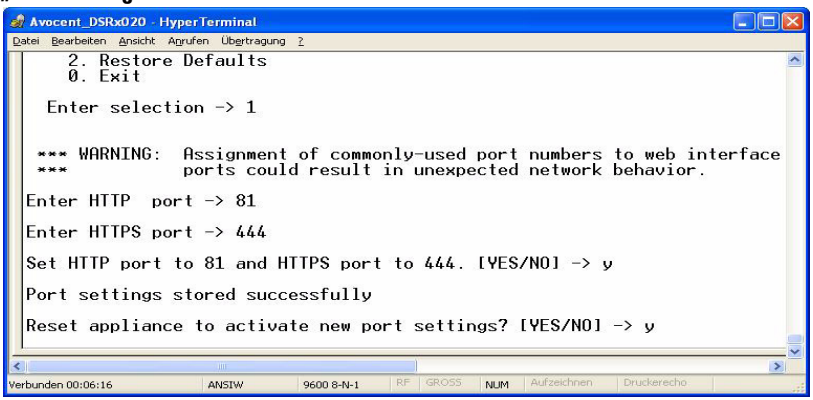
1 Sie sehen das **Hauptmenü** mit elf Optionen. Wählen Sie Option 10 aus, **Set Web Interface Ports**, um das Menü **Web Interface Port Configuration** zu öffnen.

Abbildung 2-7. Menü für die Konfiguration von Weboberflächenports



2 Wählen Sie Option 1 aus, um die Portnummern festzulegen. Geben Sie die Portnummern ein, die Sie für den HTTP-Port und den HTTPS-Port verwenden möchten.

Abbildung 2-8. Menü für die Konfiguration von Weboberflächenports – Option „Ports festlegen"



3 Wenn die Werte für Ihr Netzwerk richtig sind, geben Sie <Y> ein und betätigen Sie die <Eingabetaste>.

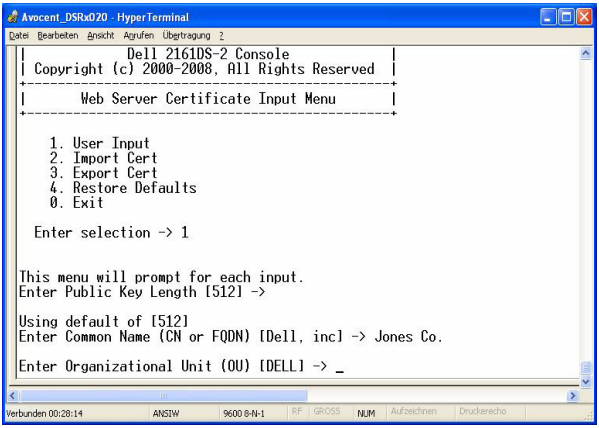
HINWEIS: Sie müssen den Remote Console Switch neu starten, um diese Portnummern zu verwenden.

HINWEIS: Wenn Sie die Portnummern des Remote Console Switches ändern, müssen Sie diese auch in der Remote Console Switch-Software ändern (siehe „Eigenschaften des Switch-Netzwerks“ in der Bedienungsanleitung der Dell Remote Console Switch-Software oder in der in der Software integrierten Hilfe) bzw. der Weboberfläche (siehe „Starten der integrierten Weboberfläche“ auf Seite 34).

So geben Sie ein Webzertifikat ein und installieren es:

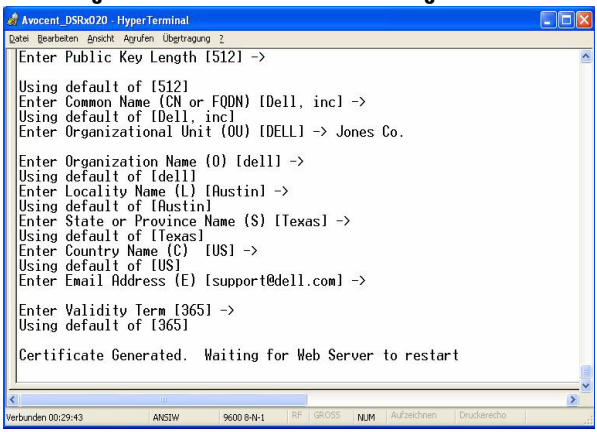
1 Sie sehen das **Hauptmenü** mit elf Optionen. Wählen Sie Option 11 aus, **Input Web Server Certificate**, um das Menü **Input Web Server Certificate** zu öffnen.

Abbildung 2-9. Menü für die Eingabe des Webserverzertifikats



2 Wählen Sie Option 1 aus: **User Input**.

Abbildung 2-10. Menü für die Benutzereingabe



3 Betätigen Sie entweder die <Eingabetaste>, um die Standardoptionen zu akzeptieren, oder geben Sie den entsprechenden Text in den nachfolgenden Feldern ein:

   a **Public Key Length**: Anzahl der für das Zertifikat gewünschten Bits.

   b **Common Name**: Ihr Name. (Da es sich um Ihr Root-Zertifikat handelt, sollten Sie einen geeigneten Namen verwenden, z. B. „Firma_Name Zertifizierungsstelle.“)

   c **Organizational Unit** (optional): Name der Organisationseinheit (z. B. Marketing).

   d **Organization Name**: Der genaue, nicht abgekürzte Firmenname Ihrer Organisation.

   e **Locality Name**: Der Ort, in dem sich der Firmensitz befindet.

   f **State or Province Name**: Der nicht abgekürzte Bundesstaat, in dem sich der Firmensitz befindet.

   g **Country Name**: Der aus zwei Buchstaben bestehende ISO-Code für Ihr Land.

   h **Email Address**: Die Kontakt-E-Mail-Adresse für die Zertifizierungsstelle.

   i **Validity Term**: Gültigkeitsdauer des Zertifikats in Tagen.

4 Betätigen Sie die <Eingabetaste>. Warten Sie den Neustart des Webservers ab, bevor Sie fortfahren.

So importieren und installieren Sie ein Webzertifikat:

1. Sie sehen das **Hauptmenü** mit elf Optionen. Wählen Sie Option 11 aus, **Input Web Server Certificate**, um das Menü **Input Web Server Certificate** zu öffnen.
2. Wählen Sie Option 2 aus: **Import Cert**. Laden Sie dann eine Firmenzertifikatdatei (*.pem) herunter. Warten Sie den Neustart des Webservers ab, bevor Sie fortfahren.

So exportieren Sie ein Webzertifikat:

1. Sie sehen das **Hauptmenü** mit elf Optionen. Wählen Sie Option 11 aus, **Input Web Server Certificate**, um das Menü **Input Web Server Certificate** zu öffnen.
2. Wählen Sie Option 3 aus, **Export Cert**, um das aktuelle Zertifikat an die serielle Konsole auszugeben. Das Format muss ähnlich wie der folgende Text aussehen:

```
„-----BEGIN CERTIFICATE-----
MIIDJzCCApCgAwIBAgIBADANBgkqhkiG9w0BAQQFADBxMQswC
QYDVQQGEwJVUzEQ
.............. Text aus Beispiel entfernt
.........................
3omoTQuBURERxg3vrwEzLqCUanQmw5BQJAVC6LT/DP7DNz/xi
pZoI+ZyaTgQEdR0
R0x0yYSaYETpMY53NMAVlCxETVkvkI2F/f+1sn+9Ik7GWBuPp
LbTmYfMoQ==
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQDI6KTaqoPfZhK7Wdd+Dzx03IVQlBqp+Vslt
n34YMDdpJ8mfqND
.............. Text aus Beispiel entfernt
.........................
b6KA7VfijVhIt3lKcYsCQEhOjqh07hI5OLmSHt3l1krGZTX+A
Cy1dlceZRkJDkyA
HqTleb5fx/i1Hu5ex99qQP9FSOP5fVsmVSRDkk2ites=
-----END RSA PRIVATE KEY-----“
```

So stellen Sie die werkseitigen Standardeinstellungen wieder her:

1. Sie sehen das **Hauptmenü** mit elf Optionen. Wählen Sie Option 11 aus, **Input Web Server Certificate**, um das Menü **Input Web Server Certificate** zu öffnen.
2. Wählen Sie Option 4 aus, **Restore Defaults**, um das aktuelle Zertifikat durch die werkseitigen Standardeinstellungen zu ersetzen.

Videooptimierung

Um eine optimale Videoqualität zu gewährleisten, konfigurieren Sie den Remote Console Switch mit denselben Einstellungen wie den Netzwerk-Switch. Wenn zum Beispiel der Remote Console Switch auf **Auto-Negotiate** eingestellt ist, muss der Netzwerk-Switch ebenfalls sowohl für die Geschwindigkeit als auch für Duplex auf **Auto-Negotiate** eingestellt sein. Wenn der Remote Console Switch auf 100 MB – Vollduplex eingestellt ist, muss der Netzwerk-Switch ebenfalls auf 100 MB – Vollduplex eingestellt werden.

Sobald Sie die Änderungen vorgenommen haben, müssen Sie ggf. die ARP-Tabellen (Address Resolution Protocol) im Netzwerk aktualisieren/leeren, bevor Sie eine neue Verbindung mit dem Remote Console Switch herstellen. Das trifft besonders dann zu, wenn der Remote Console Switch in der Stunde in Betrieb war, in der die Änderungen vorgenommen wurden.

So aktualisieren Sie die ARP-Tabelle:

Warten Sie ca. 10 Minuten, bis sich die ARP-Tabellen automatisch wiederaufgebaut haben.

– oder –

Löschen Sie den ARP-Tabelleneintrag in einer Video Session Viewer-Workstation und pingen Sie das Gerät an seiner IP-Adresse. Dies kann über ein DOS-Fenster erfolgen.

a. Geben Sie `ARP -d 1.2.3.4` ein.
   (dabei ist 1.2.3.4 die IP-Adresse des Remote Console Switches).
b. Geben Sie `PING 1.2.3.4` ein.

Wenn das PINGEN erfolgreich war, ist der Remote Console Switch einsatzbereit.

Mausbeschleunigung

HINWEIS: Dell empfiehlt, auf allen Microsoft® Windows®-Systemen, die an den Remote Console Switch angeschlossen sind, die standardmäßigen PS/2- oder USB-Maustreiber von Windows® zu verwenden.

Wenn Sie während einer Remote-Videositzung langsame Mausreaktionen feststellen, deaktivieren Sie die Mausbeschleunigung im Betriebssystem des Zielgeräts und stellen Sie die Mausgeschwindigkeit auf 50 % ein.

Anschließen eines SIPs

So schließen Sie ein SIP an jeden Server an:

1. Halten Sie die SIPs für Ihren Remote Console Switch bereit.
2. Wenn Sie eine PS/2-SIP-Verbindung verwenden, schließen Sie die farbkodierten Enden des SIPs an die entsprechenden Tastatur-, Monitor- und Mausports am ersten Server an, der mit diesem Remote Console Switch verbunden werden soll. Wenn Sie eine USB-Verbindung verwenden, schließen Sie den Stecker des SIPs an den USB-Port am ersten Server an, der mit dieser Remote Console Switch-Einheit verbunden werden soll (Abbildung 2-11).
3. Schließen Sie ein Kabelende des CAT 5-Kabels, mit dem das SIP mit der Remote Console Switch-Einheit verbunden werden soll, an den RJ-45-Stecker am SIP an (Abbildung 2-11).
4. Schließen Sie das andere Ende des CAT 5-Kabels an den gewünschten ARI-Port auf der Geräterückseite Ihrer Remote Console Switch-Einheit an.
5. Wiederholen Sie die Schritte 2 - 4 für alle Server, die angeschlossen werden sollen.

HINWEIS: Fahren Sie die Remote Console Switch-Einheit vor der Wartung herunter. Ziehen Sie stets das Stromversorgungskabel aus der Netzsteckdose.

HINWEIS: Zusätzlich zu den Dell SIPs kann der Remote Console Switch auch über IQ-Module, einschließlich Sun- und serieller IQ-Module, an Geräte angeschlossen werden.

Abbildung 2-11. Anschließen eines SIPs

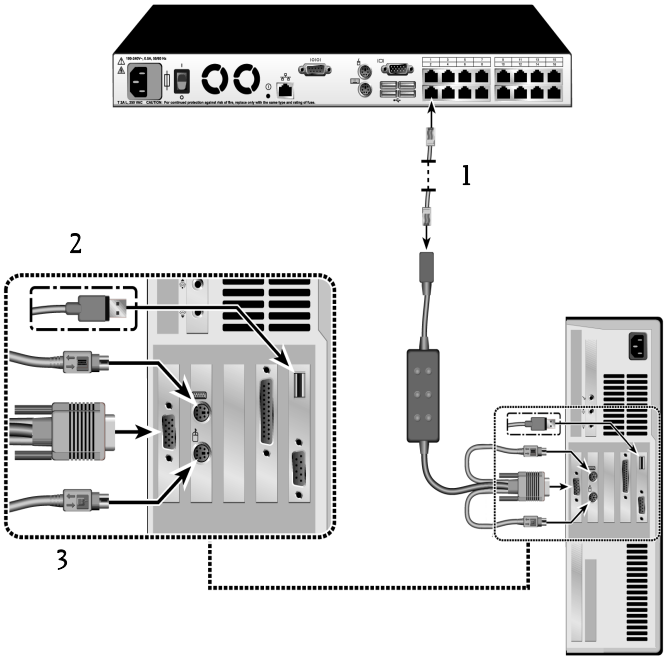


Tabelle 2-2. Beschreibung der SIP-Verbindungen

Anzahl	Beschreibung
1	CAT 5
2	USB-Verbindung
3	PS/2-Verbindung

Hinzufügen eines kaskadierten Switches

So fügen Sie einen kaskadierten Switch hinzu (optional):

HINWEIS: Der Remote Console Switch unterstützt den EL80-DT nicht.

1 Installieren Sie den Switch im Rack. Halten Sie ein CAT 5-Kabel bereit, über das die Remote Console Switch-Einheit mit dem kaskadierten Switch verbunden wird (Abbildung 2-13).

2 Schließen Sie ein Ende des Cat 5-Kabels an den ARI-Port am Console Switch an.

3 Schließen Sie das andere Ende des CAT 5-Kabels an den ACI-Port auf der Rückseite des kaskadierten Switches an.

4 Schließen Sie die Geräte gemäß den Empfehlungen des Switch-Herstellers an den kaskadierten Switch an.

5 Wiederholen Sie die Schritte 1 - 4 für alle kaskadierten Switches, die mit dem Remote Console Switch-System verbunden werden sollen.

Abbildung 2-12. Remote Console Switch mit einem analogen Cat 5-Switch

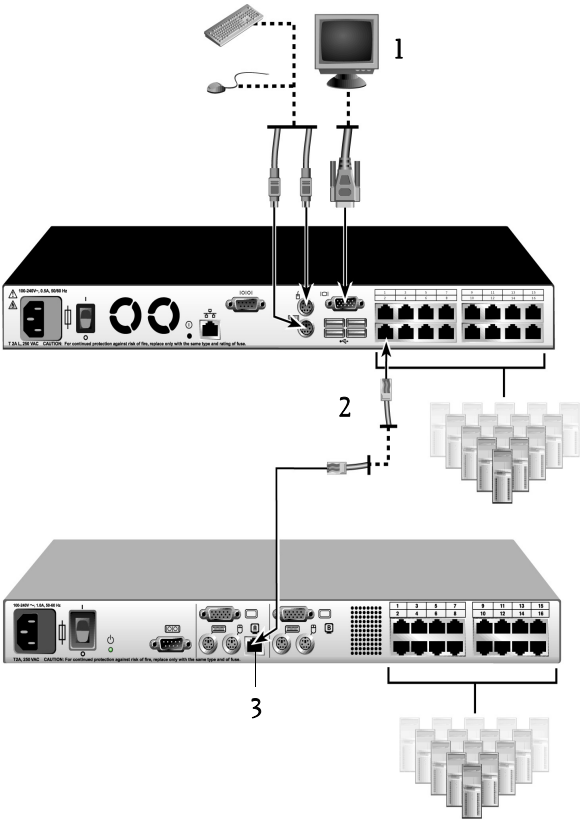


Tabelle 2-3. Remote Console Switch mit einem analogen Cat 5-Switch: Beschreibungen

Anzahl	Beschreibung
1	Lokaler Benutzer
2	CAT 5
3	ACI-Port

HINWEIS: Der Remote Console Switch unterstützt nur 1 Switch pro ARI-Port. Unter diesem ersten Switch kann kein weiterer Switch kaskadiert werden.

HINWEIS: Beim Kaskadieren mit einem Remote Console Switch werden analoge Console Switches mit 8 oder 16 Ports nicht als Primäreinheit in einer kaskadierten Konfiguration unterstützt. Der Remote Console Switch muss die Primäreinheit darstellen.

Kaskadieren mit Legacy-Switches

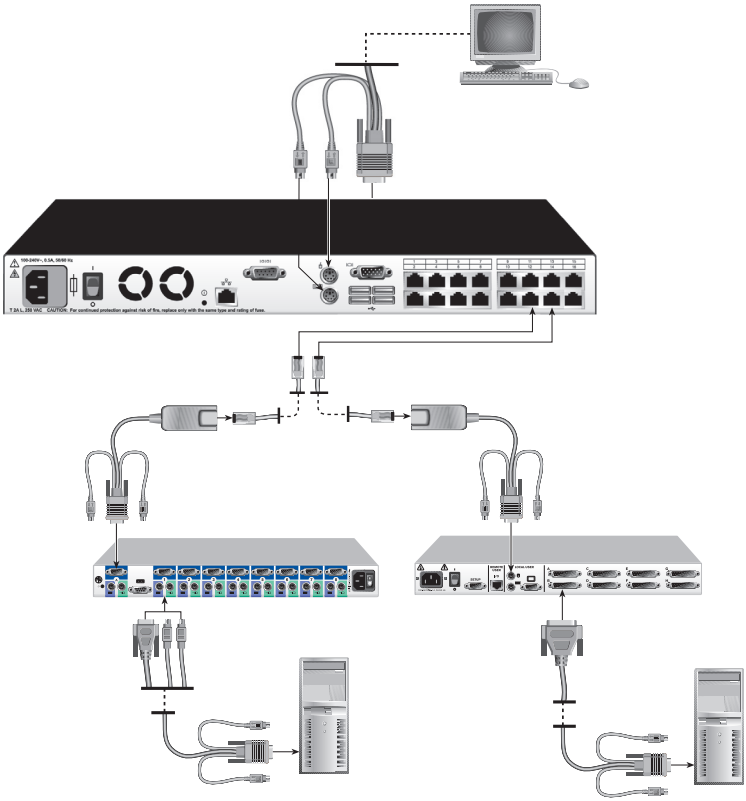
So fügen Sie einen Legacy-Switch hinzu (optional):

1. Installieren Sie den Switch im Rack. Halten Sie ein Cat 5-Kabel bereit, über das die Remote Console Switch-Einheit mit dem Legacy-Switch verbunden wird (Abbildung 2-13).
2. Schließen Sie ein Ende des Cat 5-Kabels an den ARI-Port am Console Switch an.
3. Schließen Sie das andere Ende des CAT 5-Kabels an ein Dell SIP oder IQ-Modul an.
4. Schließen Sie das SIP oder IQ-Modul gemäß den Empfehlungen des Switch-Herstellers an den Legacy-Switch an.
5. Wiederholen Sie die Schritte 1 - 4 für alle Legacy-Switches, die mit dem Remote Console Switch-System verbunden werden sollen.

HINWEIS: Der Remote Console Switch unterstützt nur 1 Switch pro ARI-Port. Unter diesem ersten Switch kann kein weiterer Switch kaskadiert werden.

HINWEIS: Beim Kaskadieren mit einem Remote Console Switch werden analoge Console Switches mit 8 oder 16 Ports nicht als Primäreinheit unterstützt. Der Remote Console Switch muss die Primäreinheit darstellen.

Abbildung 2-13. Kaskadierte Konfiguration eines Remote Console Switches mit Legacy Console Switches



Ein PEM hinzufügen (optional)

Mithilfe eines PEM (Port Expansion Module) kann jeder ARI-Port so erweitert werden, dass bis zu acht Geräte (statt nur eines Geräts) angeschlossen werden können.

HINWEIS: Die Funktionsweise des PEM ist passiv. Sobald ein Benutzer auf ein an das PEM angeschlossenes Gerät zugreift, werden daher alle weiteren Benutzer, die auf ein anderes am PEM angeschlossenes Gerät zugreifen möchten, blockiert.

HINWEIS: Eine Virtual Media-Sitzung kann nicht mit einem Server aufgebaut werden, der an ein PEM angeschlossen ist.

So fügen Sie ein PEM hinzu (optional):

1. Bauen Sie das PEM im Rack ein. Unter Verwendung von bis zu neun CAT 5-Kabeln verbinden Sie den Remote Console Switch über ein Kabel mit dem PEM und mithilfe der anderen acht Kabel verbinden Sie das PEM mit dem an jedes Gerät angeschlossenen SIP.
2. Schließen Sie ein Ende des CAT 5-Kabels, mit dem das PEM mit dem Remote Console Switch verbunden wird, an den RJ-45-Stecker an, der sich in geringem Abstand von den anderen Steckern am PEM befindet. Schließen Sie das andere Ende des CAT 5-Kabels an den gewünschten ARI-Port auf der Geräterückseite Ihrer Remote Console Switch-Einheit an.
3. Schließen Sie die CAT 5-Kabel, mit dem das PEM mit dem jeweiligen SIP eines Geräts verbunden wird, an einen der acht RJ-45-Stecker an, die auf der Rückseite des PEM gruppiert sind.
4. Schließen Sie das andere CAT 5-Kabelende an das erste SIP an.
5. Wiederholen Sie die Schritte 3 - 4 für alle Geräte, die verbunden werden sollen.

Abbildung 2-14. Konfiguration eines Remote Console Switches mit einem PEM

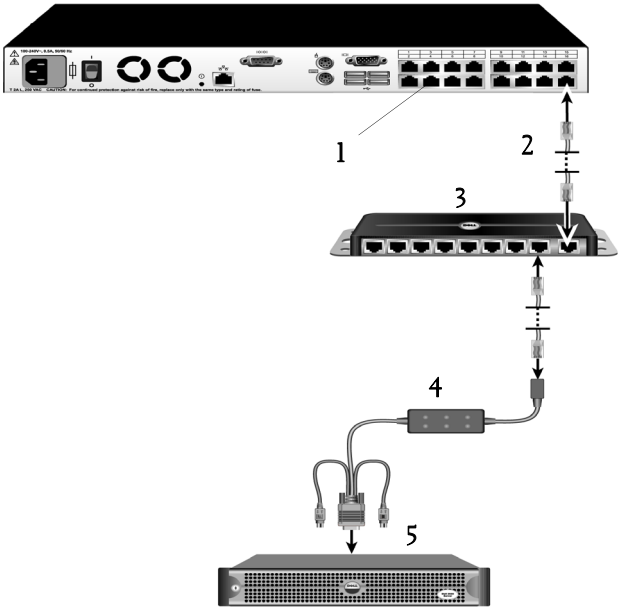


Tabelle 2-4. Konfiguration eines Remote Console Switches mit einem PEM – Beschreibung

Anzahl	Beschreibung
1	ARI-Port
2	CAT 5e
3	PEM
4	SIP oder IQ-Modul
5	Server

Anschließen an das Netzwerk

So stellen Sie die Verbindung zum Netzwerk her und fahren den Remote Console Switch hoch:

1. Schließen Sie das Netzwerkkabel vom LAN-Port auf der Rückseite des Remote Console Switches an Ihr Netzwerk an.

HINWEIS: Wenn Sie einen 2321DS Remote Console Switch verwenden, verfügen Sie über zwei redundante LAN-Ports. Wenn der erste LAN-Port ausfällt, übernimmt der zweite LAN-Port.

2. Fahren Sie alle angeschlossenen Systeme in beliebiger Reihenfolge hoch.
3. Schließen Sie Monitor-, Tastatur- und Mauskabelstecker an die entsprechenden Ports auf der Geräterückseite der Remote Console Switch-Einheit an.

Installation und Setup der integrierten Weboberfläche

Wenn Sie einen neuen Remote Console Switch installiert haben, können Sie die integrierte Weboberfläche verwenden, um Einheitenparameter zu konfigurieren und Videositzungen zu starten.

Unterstützte Browser

Die integrierte Weboberfläche unterstützt die folgenden Browser:

- Microsoft Internet Explorer® ab Version 6.x SP1
- Firefox ab Version 2.0

Starten der integrierten Weboberfläche

So starten Sie die integrierte Weboberfläche:

1. Öffnen Sie einen Webbrowser und geben Sie die IP-Adresse des Remote Console Switches ein. Sie können die IP-Adresse des Switches über die OSCAR Benutzeroberfläche oder den seriellen Port einrichten; weitere Informationen finden Sie unter „Steuern des Systems über die Analogports“ auf Seite 35.

HINWEIS: Wenn Sie die HTTP-/HTTPS-Standardports in der seriellen Konsole geändert haben und eine IPv4-Adresse verwenden, verwenden Sie dieses IP-Adressenformat: „https://<*ipadresse*>:<*port#*>“, wobei „*port#*“ die geänderte Portnummer in der seriellen Konsole darstellt. Wenn Sie eine IPv6-Adresse verwenden, verwenden Sie dieses Format: „https://<*ipadresse*>:<*port#*>“, wobei „*port#*“ die geänderte Portnummer in der seriellen Konsole darstellt. Wenn Sie eine IPv6-Adresse verwenden, müssen Sie die Adresse in eckigen Klammern angeben.

2. Das Anmeldefenster wird geöffnet. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein und klicken Sie auf **OK**.

3. Die integrierte Weboberfläche wird geöffnet und das Register **Verbindungen** wird angezeigt.

HINWEIS: Der Remote Console Switch versucht zu erkennen, ob Java auf Ihrem PC bereits installiert ist. Andernfalls müssen Sie es installieren, um die integrierte Weboberfläche verwenden zu können. Zudem müssen Sie die JNLP-Datei zu Java WebStart zuordnen.

HINWEIS: Um die integrierte Weboberfläche zu verwenden, ist mindestens JRE (Java Runtime Environment) Version 1.6.0_2 erforderlich.

HINWEIS: Wenn Sie einmal bei der integrierten Weboberfläche angemeldet sind, müssen Sie sich nicht noch einmal anmelden, wenn Sie neue Sitzungen starten, es sein denn, Sie haben sich abgemeldet oder Ihre Sitzung überschreitet das vom Administrator festgelegte Inaktivitäts-Timeout.

3

Steuern des Systems über die Analogports

Der Remote Console Switch beinhaltet Tastatur- und Mausports auf der Benutzerseite, über die Sie eine USB- oder PS/2-Tastatur und -Maus für den direkten Analogzugriff anschließen können. Der Remote Console Switch verwendet die leistungsstarke OSCAR-Benutzeroberfläche, die intuitive Menüs zur Konfiguration des Systems und zur Auswahl der Rechner bietet.

Anzeigen und Auswählen von Ports und Geräten

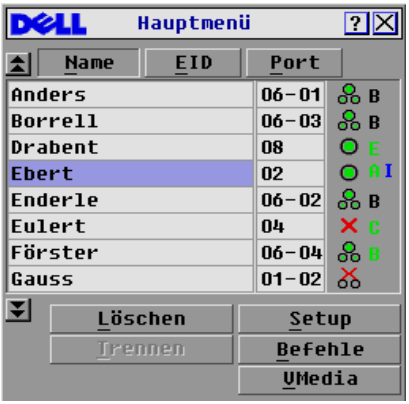
Über das Hauptmenü der OSCAR-Benutzeroberfläche können Geräte im Remote Console Switch-System angezeigt, konfiguriert und gesteuert werden. Sie können die Geräte nach Name, Port oder der in jedes SIP-Modul eingebetteten, eindeutigen elektronischen Kennnummer (EID) anzeigen.

Die Spalte „Port“ gibt den ARI-Port an, an den ein Gerät angeschlossen ist. Wenn Sie einen Switch vom primären Remote Console Switch kaskadieren und damit eine weitere Stufe erstellen, wird der ARI-Port in der Port-Nummerierung zuerst angezeigt, gefolgt von dem Switch-Port, an den das Gerät angeschlossen ist. In Abbildung 3-1 sind zum Beispiel die Geräte 06-01, 06-02, 06-03 und 06-04 an Switches angeschlossen. In der Port-Nummerierung wird zuerst der ARI-Port angezeigt und dann der Switch-Port, an den das Gerät angeschlossen ist. Wenn Sie einen Switch von einem PEM (Port Expansion Module) kaskadieren, werden ebenfalls mehrere Geräte an einem einzigen Port angezeigt.

So rufen Sie das Hauptmenü auf:

Betätigen Sie die Taste <Druck>, um OSCAR zu starten. Das **Hauptmenü** wird angezeigt.

Abbildung 3-1. Beispiel für ein Hauptmenü-Dialogfeld



HINWEIS: Sie können auch zweimal innerhalb einer Sekunde auf die Tasten <Strg>, <Alt> oder die <Umschalttaste> drücken, um die OSCAR-Benutzeroberfläche zu starten. Wann immer in diesem Kapitel die Taste <Druck> abgebildet ist, kann ebenfalls diese Tastenfolge verwendet werden.

Anzeigen des Switch-Status

Der Status der Geräte in Ihrem System wird in den rechten Spalten des **Hauptmenüs** angezeigt. In Tabelle 3-1 werden die verschiedenen Statussymbole beschrieben.

Tabelle 3-1. Statussymbole der OSCAR-Benutzeroberfläche

Symbol	Beschreibung
	SIP ist online.
	SIP ist offline oder funktioniert nicht ordnungsgemäß.
	Der angeschlossene Switch ist online.
	Der angeschlossene Switch ist offline oder funktioniert nicht ordnungsgemäß.
	SIP ist nicht verfügbar.

Tabelle 3-1. Statussymbole der OSCAR-Benutzeroberfläche (Fortsetzung)

Symbol	Beschreibung
A	(Grüner Buchstabe) Zeigt an, welcher Benutzerkanal momentan mit einem SIP verbunden ist.
A	(Schwarzer Buchstabe) Zeigt einen blockierten Pfad an. Beispiel: In Abbildung 3-1 zeigt Benutzer C den Eintrag Förster an, während dadurch der Zugriff auf Anders, Borell und Enderle blockiert wird, die an denselben ARI-Port angeschlossen sind.
I	(Blauer Buchstabe) Zeigt eine Virtual Media-Verbindung an.

Auswählen von Geräten

Wählen Sie Geräte über das **Hauptmenü** aus. Bei Auswahl eines Geräts konfiguriert die Einheit Tastatur und Maus auf die korrekten Einstellungen für das betreffende Gerät um.

So wählen Sie Geräte aus:

Doppelklicken Sie auf den Gerätenamen, die EID oder die Portnummer.
– oder –
Wenn die Geräte in der Liste nach Port geordnet sind (Schaltfläche **Port** ist aktiviert), geben Sie die Portnummer ein und betätigen Sie die <Eingabetaste>.
– oder –
Wenn die Geräte in der Liste nach Namen oder EID-Nummer geordnet sind (Schaltfläche **Name** oder **EID** ist aktiviert), geben Sie die Anfangsbuchstaben des Gerätenamens oder die EID-Nummer ein, um das Gerät eindeutig auszuwählen, und betätigen Sie die <Eingabetaste>.

HINWEIS: Sie können durch Betätigen der <Eingabetaste> eine Verbindung zum ausgewählten Gerät herstellen.

So wählen Sie das vorige Gerät aus:

Betätigen Sie erst die Taste <Druck> und anschließend die <Rücktaste>. Diese Tastenkombination dient zum Umschalten zwischen vorherigen und aktuellen Verbindungen.

So trennen Sie die Verbindung zwischen Benutzer und Gerät:

Betätigen Sie die Taste <Druck> und dann <Alt+0> oder klicken Sie auf **Trennen** in der OSCAR-Benutzeroberfläche. Dadurch wird der Benutzer freigegeben – es ist kein Gerät ausgewählt. Das Status-Flag auf Ihrem Desktop zeigt `Frei` an.

Soft Switching

Mithilfe von Soft Switching können Sie über eine Hotkey-Folge zwischen Geräten wechseln. Das Soft Switching eines Geräts kann durch Betätigen der Taste <Druck> und die nachfolgende Eingabe der Anfangsbuchstaben des Gerätenamens oder der Gerätenummer erfolgen. Wenn eine Zeitverzögerung eingestellt ist und Sie diese Tastenfolge vor Ablauf dieser Zeitspanne drücken, wird die OSCAR-Benutzeroberfläche nicht angezeigt.

So stellen Sie eine Zeitverzögerung ein:

1. Betätigen Sie die Taste <Druck>, um die OSCAR-Benutzeroberfläche aufzurufen. Das **Hauptmenü** wird angezeigt.
2. Klicken Sie auf **Setup – Menü**. Das Dialogfeld **Menü** wird angezeigt.
3. Geben Sie unter **Zeitverzögerung** die Anzahl von Sekunden an, die zwischen dem Betätigen der Taste <Druck> und der Anzeige des **Hauptmenüs** vergehen sollen.
4. Klicken Sie auf **OK**.

So wechseln Sie mit dem Soft Switching zu einem Gerät:

1. Betätigen Sie die Taste <Druck>, um ein Gerät auszuwählen. Wenn die Geräte in der Liste nach Port geordnet sind (Schaltfläche **Port** ist aktiviert), geben Sie die Portnummer ein und betätigen Sie die <Eingabetaste>.
   – oder –
   Wenn die Geräte in der Liste nach Namen oder EID-Nummer geordnet sind (Schaltfläche **Name** oder **EID** ist aktiviert), geben Sie die Anfangsbuchstaben des Gerätenamens oder die EID-Nummer ein, um das Gerät eindeutig auszuwählen, und betätigen Sie die <Eingabetaste>.
2. Betätigen Sie die Taste <Druck> und dann die <Rücktaste>, um zum vorherigen Gerät zurückzuschalten.

Navigation in der OSCAR-Benutzeroberfläche

Tabelle 3-2 veranschaulicht die Navigation in der OSCAR Benutzeroberfläche mit Tastatur und Maus.

HINWEIS: Sie können auch zweimal innerhalb einer Sekunde auf die Tasten <Strg>, <Alt> oder die <Umschalttaste> drücken, um die OSCAR-Benutzeroberfläche zu starten. Wann immer in diesem Kapitel die Taste <Druck> abgebildet ist, kann ebenfalls diese Tastenfolge verwendet werden.

Tabelle 3-2. OSCAR – Navigationsgrundlagen

Tastenanschlag	Funktion
<Druck>, Strg-Strg, Umschalt-Umschalt und/oder Alt-Alt	Aktivierungstastenfolge der OSCAR-Benutzeroberfläche. Standardmäßig sind <Druck> und Strg-Strg als Optionen für die Aktivierung der OSCAR-Benutzeroberfläche eingestellt. Umschalt-Umschalt und Alt-Alt müssen über die OSCAR-Benutzeroberfläche eingestellt werden, bevor sie verwendet werden können.
<Druck>	Betätigen Sie die Taste <Druck> zweimal, um den Tastenanschlag <Druck> an das momentan ausgewählte Gerät zu senden.
F1	Öffnet den Bildschirm **Hilfe** für das aktuelle Dialogfeld.
Esc	Schließt das aktuelle Dialogfeld, ohne die Änderungen zu speichern, und kehrt zum vorherigen Dialogfeld zurück. Im **Hauptmenü** schließt diese Taste die OSCAR-Benutzeroberfläche und kehrt zum Status-Flag zurück. In einem Meldungsfeld schließt diese Taste das Popup-Feld und kehrt zum aktuellen Dialogfeld zurück.
Alt+Hotkey	Öffnet Dialogfelder, wählt oder aktiviert Optionen und führt Aktionen aus, wenn die Taste in Verbindung mit unterstrichenen Buchstaben verwendet wird.
Alt+X	Schließt das aktuelle Dialogfeld und kehrt zum vorherigen Dialogfeld zurück.
Alt+O	Wählt die Schaltfläche **OK** aus und kehrt dann zum vorherigen Dialogfeld zurück.

Tabelle 3-2. OSCAR – Navigationsgrundlagen (Fortsetzung)

Tastenanschlag	Funktion
Klicken, Eingabetaste	In einem Textfeld wird der Text zum Bearbeiten ausgewählt und die Pfeil-nach-links- und Pfeil-nach-rechts-Tasten werden aktiviert, um den Cursor in die entsprechende Richtung zu bewegen. Betätigen Sie die <Eingabetaste>, um den gesamten Inhalt des Feldes auszuwählen.
Eingabetaste	Schließt ein Switching im Hauptmenü ab und verlässt die OSCAR-Benutzeroberfläche.
<Druck>, Rücktaste	Wechselt zurück zur vorherigen Auswahl.
<Druck>, Alt+0	Trennt einen Benutzer sofort vom Server; es ist kein Server ausgewählt. Das Status-Flag zeigt `Frei` an. (Dies gilt nur für die **0** auf der Tastatur, nicht für die 0 auf dem Ziffernblock.)
<Druck>, Pause	Aktiviert sofort den Bildschirmschonermodus und verhindert bei Kennwortschutz den Zugriff auf die entsprechende Konsole.
Pfeil-nach-oben/unten	Verschiebt den Cursor in einer Liste um eine Zeile nach oben bzw. nach unten.
Pfeil-nach-rechts/links	Verschiebt den Cursor beim Bearbeiten eines Textfelds innerhalb der Spalte.
Bild auf/Bild ab	Blättert in Namens- und Portlisten sowie auf Hilfeseiten seitenweise nach oben oder unten.
Pos1/Ende	Verschiebt den Cursor an den Anfang bzw. das Ende einer Liste.
Löschen	Löscht die aktuelle Auswahl in der Scan-Liste oder Zeichen in einem Textfeld.
Zifferntasten	Eingabe über Tastatur oder Ziffernblock.

Konfigurieren der Menüs der OSCAR-Benutzeroberfläche

Sie können Ihren Remote Console Switch über das Menü Setup der OSCAR-Benutzeroberfläche konfigurieren. Wählen Sie beim ersten Setup der Einheit die Schaltfläche Namen aus, um die Geräte durch eindeutige Namen zu identifizieren. Wählen Sie die anderen Setup-Funktionen aus, um routinemäßige Aufgaben im Zusammenhang mit den Geräten über das OSCAR-Menü zu verwalten. Siehe Tabelle 3-3.

Tabelle 3-3. Setup-Funktionen zur Verwaltung von routinemäßigen Aufgaben für Geräte

Funktion	Zweck
Menü	Wechseln der Sortierung für in der Liste angezeigte Geräte zwischen numerischer Anzeige nach Port- oder EID-Nummer und alphabetischer Anzeige nach Namen. Ändern der **Zeitverzögerung**, die festlegt, wie lange nach Betätigen der Taste <Druck> die OSCAR-Benutzeroberfläche angezeigt wird.
Sicherheit	Festlegen von Kennwörtern zur Einschränkung des Gerätezugriffs. Aktivieren des Bildschirmschoners.
Flag	Ändern der Anzeige, Anzeigedauer, Farbe oder Position des Status-Flags.
Sprache	Auswählen der Spracheinstellung für die Anzeige.
Geräte	Identifizieren der jeweiligen Anzahl von Ports an einem angeschlossenen kaskadierten Switch.
Namen	Identifizieren von Geräten durch eindeutige Namen.
Tastatur	Auswählen der länderspezifischen Tastatureinstellung.
Senden	Wird zur gleichzeitigen Steuerung mehrerer Geräte durch Tastatur- und Mausaktionen eingerichtet.
Scannen	Einrichten eines benutzerdefinierten Scan-Schemas für bis zu 100 Geräte.
Switch	Auswählen von Switch-Modus und Timeout für den Share-Modus.
Netzwerk	Auswählen von Netzwerkgeschwindigkeit, -übertragungsmodus und -konfiguration.
VMedia	Festlegen des Verhaltens der Einheit während einer Virtual Media-Sitzung.
PDUs (Nur für 2321DS Remote Console Switch.)	Zeigen Sie an, welche PDUs an Ihr System angeschlossen sind.

So rufen Sie das Menü „Setup“ auf:

1 Betätigen Sie die Taste <Druck>, um die OSCAR-Benutzeroberfläche aufzurufen. Das **Hauptmenü** wird angezeigt.

2 Klicken Sie auf **Setup**. Das Dialogfeld **Setup** wird angezeigt.

Abbildung 3-2. Dialogfeld „Setup"

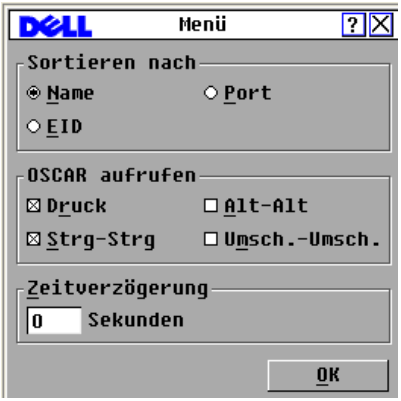
Ändern des Anzeigeverhaltens

Verwenden Sie das Dialogfeld **Menü**, um die Reihenfolge der angezeigten Geräte zu ändern, eine **Zeitverzögerung** für die OSCAR-Benutzeroberfläche einzustellen und die Tastenfolge zum Aufrufen der OSCAR-Benutzeroberfläche zu ändern. Die Einstellung für die Reihenfolge der angezeigten Geräte bestimmt, wie die Geräte in den verschiedenen Bildschirmen angezeigt werden, einschließlich des **Hauptmenüs** und der Dialogfelder **Geräte** und **Senden**.

So rufen Sie das Dialogfeld „Menü" auf:

1 Klicken Sie im **Hauptmenü** auf **Setup – Menü**. Das Dialogfeld **Menü** wird angezeigt.

Abbildung 3-3. Dialogfeld „Menü“



2 <Druck>, Strg-Strg, Alt-Alt und Umschalt-Umschalt können ausgewählt werden, um die OSCAR-Benutzeroberfläche zu starten. Es können eine oder alle der oben aufgeführten Tastenkombinationen gleichzeitig ausgewählt sein. Wenn nur eine Tastenkombination ausgewählt ist, kann diese Auswahl erst aufgehoben werden, nachdem eine zweite Tastenkombination ausgewählt wurde.

So wählen Sie die Standardreihenfolge der angezeigten Geräte aus:

1 Wählen Sie Name, um die Geräte in alphabetischer Reihenfolge nach Namen anzuzeigen.
– oder –
Wählen Sie EID, um die Geräte in numerischer Reihenfolge nach der EID-Nummer anzuzeigen.
– oder –
Wählen Sie Port aus, um die Geräte in numerischer Reihenfolge nach der Portnummer anzuzeigen.

2 Klicken Sie auf OK.

So stellen Sie eine Zeitverzögerung für die OSCAR-Benutzeroberfläche ein:

1 Geben Sie die Anzahl der Sekunden (0 bis 9) ein, um die der Start der OSCAR-Benutzeroberfläche verzögert werden soll, nachdem Sie die Taste <Druck> betätigt haben. Geben Sie `0` ein, um die OSCAR-Benutzeroberfläche ohne Verzögerung zu starten.

2 Klicken Sie auf OK.

Durch Einstellen einer **Zeitverzögerung** haben Sie die Möglichkeit, ein Soft Switching durchzuführen, ohne dass die OSCAR-Benutzeroberfläche angezeigt wird. Einzelheiten zum Soft Switching finden Sie unter „Soft Switching“ auf Seite 38 in diesem Kapitel.

Einstellen der Konsolensicherheit

Über die OSCAR-Benutzeroberfläche kann die Sicherheit Ihrer analogen Portkonsole eingestellt werden. Sie können einen Bildschirmschonermodus einrichten, der aktiviert wird, sobald Ihre Konsole während einer bestimmten Zeitspanne nicht verwendet wird. Sobald dieser Modus aktiviert ist, bleibt die Konsole gesperrt, bis Sie eine beliebige Taste betätigen oder die Maus bewegen. Sie müssen dann Ihr Kennwort eingeben, um weiterarbeiten zu können.

Über das Dialogfeld **Sicherheit** können Sie Ihre Konsole mit Kennwortschutz versehen, das Kennwort einstellen oder ändern sowie den Bildschirmschoner aktivieren.

So rufen Sie das Dialogfeld „Sicherheit“ auf:

1. Betätigen Sie die Taste <Druck>, um die OSCAR-Benutzeroberfläche aufzurufen. Das **Hauptmenü** wird angezeigt.
2. Klicken Sie auf **Setup – Sicherheit**. Das Dialogfeld **Sicherheit** wird angezeigt.

Abbildung 3-4. Dialogfeld „Sicherheit“

HINWEIS: Wenn die Felder Neu und Bestätigen sechs Asterisken enthalten, wurde bereits ein Kennwort eingerichtet.

So bestimmen oder ändern Sie Ihr Kennwort:

HINWEIS: Wenn Sie Ihr Kennwort verlieren oder vergessen, wenden Sie sich an den Kundendienst von Dell. Kontaktinformationen finden Sie in Anhang F: Technischer Kundendienst.

1. Klicken Sie in das Textfeld **Neu**.
2. Geben Sie das neue Kennwort in das Textfeld **Neu** ein. Kennwörter müssen sowohl numerische als auch alphanumerische Zeichen enthalten und dürfen maximal 12 Zeichen lang sein. Außerdem wird zwischen Groß- und Kleinschreibung unterschieden. Zulässige Zeichen sind: A bis Z, a bis z, 0 bis 9, Bindestrich.
3. Geben Sie das Kennwort im Feld **Bestätigen** erneut ein.
4. Klicken Sie auf **OK**, wenn nur das Kennwort geändert werden soll, und schließen Sie danach das Dialogfeld.

So schützen Sie die Konsole mit einem Kennwort:

1. Richten Sie ein Kennwort gemäß der Beschreibung im vorherigen Verfahren ein.
2. Aktivieren Sie das Kontrollkästchen **Bildschirmschoner**.
3. Geben Sie die Anzahl von Minuten für die **Wartezeit** (1 bis 99) ein, nach deren Ablauf die Aktivierung des Kennwortschutzes und der Bildschirmschonerfunktion erfolgen soll.
4. Wählen Sie im Feld „Modus“ die Option **Energie** aus, wenn Ihr Monitor den ENERGY STAR® Richtlinien entspricht; andernfalls wählen Sie **Bildschirm**.

VORSICHT: Bei Monitoren, die nicht den EnergyStar® Richtlinien entsprechen, kann die Auswahl des Energie-Modus zu Schäden am Monitor führen.

5. (Optional) Klicken Sie auf **Test**, um den Bildschirmschonertest auszuführen. Dieser dauert 10 Sekunden und kehrt danach zum Dialogfeld **Sicherheit** zurück.
6. Klicken Sie auf **OK**.

So melden Sie sich bei Ihrer Konsole an:

1. Betätigen Sie eine beliebige Taste oder bewegen Sie die Maus.
2. Das Dialogfeld **Kennwort** wird angezeigt. Geben Sie Ihr Kennwort ein und klicken Sie auf **OK**.
3. Das **Hauptmenü** wird angezeigt, wenn das richtige Kennwort eingegeben wurde.

So entfernen Sie den Kennwortschutz für Ihre Benutzerkonsole:

1. Klicken Sie im **Hauptmenü** auf **Setup – Sicherheit**.
2. Klicken Sie im Dialogfeld **Sicherheit** in das Textfeld **Neu**. Lassen Sie das Feld leer. Betätigen Sie die <Eingabetaste>.
3. Klicken Sie in das Feld **Bestätigen**. Lassen Sie das Feld leer.
4. Klicken Sie auf **OK**, um das Kennwort zu entfernen.

So aktivieren Sie den Bildschirmschonermodus ohne Kennwortschutz:

1. Wenn bei Ihrer Konsole kein Kennwort erforderlich ist, um das Dialogfeld **Sicherheit** aufzurufen, fahren Sie mit Schritt 2 fort.
   – oder –
   Wenn Ihre Konsole durch ein Kennwort geschützt ist, kehren Sie zum vorhergehenden Verfahren zurück und fahren danach mit Schritt 2 fort.
2. Aktivieren Sie das Kontrollkästchen **Bildschirmschoner**.
3. Geben Sie die Anzahl der Minuten (1 bis 99) ein, um die Wartezeit für die Aktivierung des Bildschirmschoners einzustellen.
4. Wählen Sie **Energie**, wenn Ihr Monitor den ENERGY STAR® Richtlinien entspricht; ansonsten wählen Sie **Bildschirm**.

VORSICHT: Bei Monitoren, die nicht den EnergyStar® Richtlinien entsprechen, kann die Auswahl des Energie-Modus zu Schäden am Monitor führen.

5. (Optional) Klicken Sie auf **Test**, um den Bildschirmschonertest auszuführen. Dieser dauert 10 Sekunden und kehrt danach zum Dialogfeld **Sicherheit** zurück.
6. Klicken Sie auf **OK**.

HINWEIS: Wenn der Bildschirmschonermodus aktiviert wird, wird die Verbindung zwischen Benutzer und Gerät unterbrochen; es ist kein Gerät ausgewählt. Das Status-Flag zeigt den Status „Frei" an.

So beenden Sie den Bildschirmschonermodus:

Betätigen Sie eine beliebige Taste oder bewegen Sie die Maus. Das **Hauptmenü** wird angezeigt, und alle vorherigen Geräteverbindungen werden wiederhergestellt, sobald das richtige Kennwort für die Einheit eingegeben wurde.

So deaktivieren Sie den Bildschirmschoner:

1. Deaktivieren Sie im Dialogfeld **Sicherheit** das Kontrollkästchen **Bildschirmschoner**.

2 Klicken Sie auf **OK**.

So schalten Sie den Bildschirmschoner sofort ein:

Betätigen Sie die Taste <Druck> und danach <Pause>.

Steuern des Status-Flags

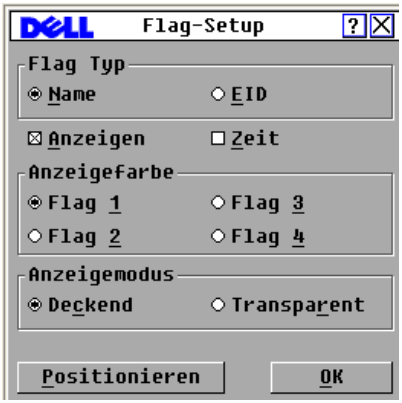
Das Status-Flag wird auf Ihrem Desktop angezeigt und gibt den Namen oder die EID-Nummer des ausgewählten Geräts oder den Status des ausgewählten Ports an. Mit dem Dialogfeld **Flag** können Sie das Status-Flag so konfigurieren, dass es Gerätenamen oder EID-Nummern anzeigt. Außerdem können Sie in diesem Dialogfeld die Farbe des Status-Flags ändern, festlegen, ob es deckend oder transparent sein soll, sowie Zeit und Position der Anzeige auf dem Desktop bestimmen.

So rufen Sie das Dialogfeld „Flag“ auf:

1 Betätigen Sie die Taste <Druck>, um die OSCAR-Benutzeroberfläche aufzurufen. Das **Hauptmenü** wird angezeigt.

2 Klicken Sie auf **Setup – Flag**. Das Dialogfeld **Flag** wird angezeigt.

Abbildung 3-5. Dialogfeld „Flag“



So legen Sie fest, wie das Status-Flags dargestellt werden soll:

1 Wählen Sie **Name** oder **EID** aus, um zu bestimmen, welche Informationen angezeigt werden.

2 Wählen Sie **Anzeigen** aus, um das Status-Flag durchgehend anzuzeigen.

3 (Optional) Wählen Sie **Zeit** aus, um das Status-Flag nur jeweils fünf Sekunden nach dem Umschalten anzuzeigen.

4 Wählen Sie unter **Anzeigefarbe** eine Farbe für das Status-Flag aus.

5 Wählen Sie unter **Anzeigemodus** entweder **Deckend** für ein Status-Flag in deckender Farbe aus oder **Transparent**, wenn der Desktop durch das Status-Flag sichtbar bleiben soll.

6 So positionieren Sie ein Status-Flag auf dem Desktop:

   a Klicken Sie auf **Positionieren**, um den Bildschirm **Positionieren** anzuzeigen.

   b Klicken Sie auf die Titelleiste und ziehen Sie sie an die gewünschte Position.
   – oder –
   Verwenden Sie die Pfeil-nach-rechts/links-Tasten, um das Status-Flag an die gewünschte Position zu verschieben, und betätigen Sie dann die <Eingabetaste>.

   c Klicken Sie mit der rechten Maustaste, um zum Dialogfeld **Flag** zurückzukehren.

HINWEIS: Änderungen an der Status-Flag-Position werden erst gespeichert, wenn Sie im Dialogfeld Flag auf „OK" klicken.

7 Klicken Sie auf **OK**, um die Einstellungen zu speichern.
– oder –
Klicken Sie auf **X**, um den Vorgang abzubrechen, ohne die Änderungen zu speichern.

Einstellen der Sprache für die Benutzeroberfläche

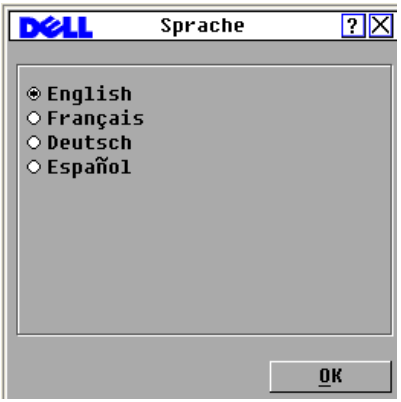
Sie können für die OSCAR-Benutzeroberfläche eine von vier unterstützten Sprachen im Dialogfeld **Sprache** auswählen.

So ändern Sie die Sprache für die OSCAR-Benutzeroberfläche:

1 Betätigen Sie die Taste <Druck>, um die OSCAR-Benutzeroberfläche aufzurufen. Das **Hauptmenü** wird angezeigt.

2 Klicken Sie auf **Setup – Sprache**. Das Dialogfeld **Sprache** wird angezeigt.

Abbildung 3-6. Dialogfeld „Sprache“



3 Klicken Sie auf die Sprache, in der die OSCAR-Benutzeroberfläche angezeigt werden soll.

4 Klicken Sie auf **OK**, um die Änderungen zu übernehmen und zum Dialogfeld **Setup** zurückzukehren. Das Dialogfeld **Setup** wird nun in der gewählten Sprache angezeigt.

Zuweisen von Gerätetypen

Der Remote Console Switch erkennt kaskadierte KVM-Switches automatisch, Sie müssen jedoch die Anzahl der Ports am kaskadierten Switch im Dialogfeld **Geräte** angeben. Auf dem Bildschirm wird in der Kategorie **Typ** Sw-8 oder Sw-24 für den kaskadierten Switch angezeigt. Wenn Sie Switches in der Liste auswählen, wird die Schaltfläche **Ändern** verfügbar, damit Sie dem Switch die entsprechende Anzahl an Ports zuweisen können.

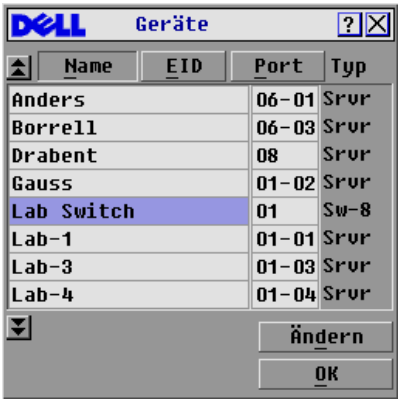
HINWEIS: Die Schaltfläche „Ändern“ ist nur verfügbar, wenn ein konfigurierbarer Switch ausgewählt wird.

So rufen Sie das Dialogfeld „Geräte“ auf:

1 Betätigen Sie die Taste <Druck>, um die OSCAR-Benutzeroberfläche aufzurufen. Das **Hauptmenü** wird angezeigt.

2 Klicken Sie auf **Setup – Geräte**. Das Dialogfeld **Geräte** wird angezeigt.

Abbildung 3-7. Dialogfeld „Geräte“



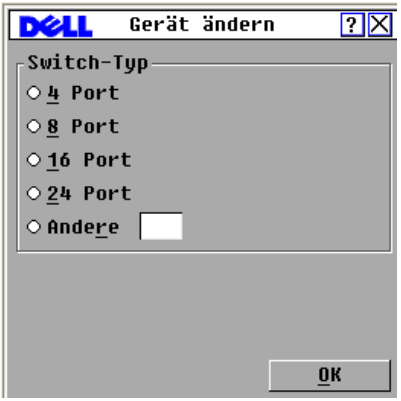
Wenn der Remote Console Switch einen kaskadierten Switch erkennt, ändert sich die Port-Nummerierung so, dass jedes Gerät unter diesem Switch dargestellt werden kann. Wenn der Switch beispielsweise an ARI-Port 6 angeschlossen ist, wird der Switch-Port als „06“ aufgeführt, und jedes untergeordnete Gerät ist nachfolgend als „06-01“, „06-02“ usw. nummeriert.

HINWEIS: Änderungen im Dialogfeld Gerät ändern werden erst dann gespeichert, wenn Sie im Dialogfeld Geräte auf OK klicken.

So weisen Sie einen Gerätetyp zu:

1. Wählen Sie die gewünschte Portnummer im Dialogfeld **Geräte** aus.
2. Klicken Sie auf **Ändern**. Das Dialogfeld **Gerät ändern** wird angezeigt.

Abbildung 3-8. Dialogfeld „Gerät ändern“



3. Geben Sie die von dem kaskadierten Switch unterstützte Portanzahl ein, oder wählen Sie die entsprechende Anzahl aus und klicken Sie auf **OK**.
4. Führen Sie die Schritte 1 bis 3 für jeden Port aus, dem ein Gerätetyp zugewiesen werden soll.
5. Klicken Sie im Dialogfeld **Geräte** auf **OK**, um die Einstellungen zu speichern.

Zuweisen von Gerätenamen

Verwenden Sie das Dialogfeld **Namen**, um individuelle Geräte nach dem Namen und nicht nach der Portnummer zu identifizieren. Die Liste der **Namen** ist immer nach Port geordnet. Namen werden im SIP-Modul gespeichert. Selbst wenn SIP/Server an einen anderen ARI-Port angeschlossen wird, erkennt der Switch den Namen und die Konfiguration.

HINWEIS: Wenn ein Gerät ausgeschaltet ist, wird das entsprechende SIP-Modul nicht mehr in der Namensliste angezeigt.

So rufen Sie das Dialogfeld **Namen** auf:

1. Betätigen Sie die Taste <Druck>, um die OSCAR-Benutzeroberfläche aufzurufen. Das **Hauptmenü** wird angezeigt.
2. Klicken Sie auf **Setup – Namen**. Das Dialogfeld **Namen** wird angezeigt.

HINWEIS: Wenn sich die Serverliste ändert, wird der Mauszeiger als Sanduhrsymbol dargestellt, während sich die Liste automatisch aktualisiert. Erst nach abgeschlossener Aktualisierung der Liste werden wieder Tastatur- und Mauseingaben akzeptiert.

HINWEIS: Die EID-Nummer wird als Standardname verwendet, wenn einem SIP-Modul kein Name zugewiesen ist.

So weisen Sie Gerätenamen zu:

1. Wählen Sie im Dialogfeld **Namen** einen Gerätenamen oder eine Portnummer aus, und klicken Sie auf **Ändern**. Das Dialogfeld **Namen ändern** wird angezeigt.
2. Geben Sie im Feld **Neuer Name** den gewünschten Namen ein. Gerätenamen können bis zu 15 Zeichen umfassen. Zu den zulässigen Zeichen gehören: A bis Z, a bis z, 0 bis 9, Leerzeichen und Bindestrich.
3. Klicken Sie auf **OK**, um den neuen Namen in das Dialogfeld **Namen** zu übernehmen. Die Auswahl wird erst dann gespeichert, wenn im Dialogfeld **Namen** auf **OK** geklickt wird.
4. Wiederholen Sie die Schritte 1 bis 3 für jedes Gerät im System.
5. Klicken Sie im Dialogfeld **Namen** auf **OK**, um die Änderungen zu speichern.
   – oder –
   Klicken Sie auf **X** oder betätigen Sie die Taste <Esc>, um das Dialogfeld zu schließen, ohne die Änderungen zu speichern.

Konfigurieren von Netzwerkeinstellungen

Sie können die Netzwerkeinstellungen für den Remote Console Switch über den seriellen Port oder über das Dialogfeld **Netzwerk** ändern.

Im Dialogfeld **Netzwerk** können Sie entweder den Modus **IPv4** (Standard) oder **IPv6** auswählen. Sie können die folgenden Netzwerkeinstellungen ändern: **IP-Adresse**, **Netzmaske** (im **IPv4**-Modus) oder **Präfixlänge** (im **IPv6**-Modus) und **Gateway**. Darüber hinaus können Sie die **Netzwerkgeschwindigkeit** und den **Übertragungsmodus** auswählen und festlegen, ob dem Remote Console Switch eine **statische** IP-Adresse (Standard) oder ggf. eine **dynamische** IP-Adresse zugewiesen wird.

Abbildung 3-9. Dialogfeld „Netzwerk“ (IPv4-Modus)

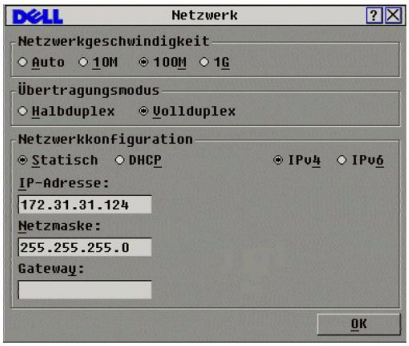
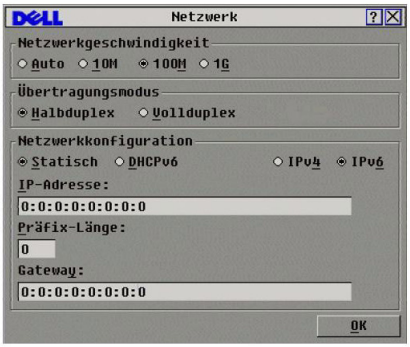


Abbildung 3-10. Dialogfeld „Netzwerk“ (IPv6-Modus)



Wenn Sie Änderungen an den Netzwerkeinstellungen vorgenommen haben, klicken Sie auf OK. Der Remote Console Switch wird neu gestartet.

Konfigurieren von Virtual Media-Einstellungen

Anweisungen zur Konfiguration von Virtual Media-Einstellungen finden Sie unter „Virtual Media“ auf Seite 93.

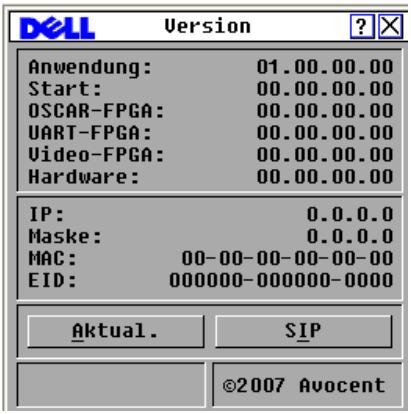
Anzeigen von Versionsinformationen

Über die OSCAR-Benutzeroberfläche können Sie die Versionen des Remote Console Switches und der Firmware des SIP-Moduls anzeigen. Halten Sie die Firmware für eine optimale Leistung des Systems immer auf dem neuesten Stand. Weitere Informationen finden Sie im Abschnitt „Anhang D: FLASH-Aktualisierungen“ auf Seite 225.

So zeigen Sie Versionsinformationen an:

1. Betätigen Sie die Taste <Druck>, um die OSCAR-Benutzeroberfläche aufzurufen. Das **Hauptmenü** wird angezeigt.
2. Klicken Sie auf **Befehle – Versionen anzeigen**. Das Dialogfeld **Version** wird angezeigt. Die Subsystemversionen der Einheit werden in der oberen Hälfte des Dialogfelds aufgeführt.

Abbildung 3-11. Dialogfeld „Version“



3. Klicken Sie auf die Schaltfläche **SIP**, um Versionsinformationen zu individuellen SIP-Modulen anzuzeigen. Das Dialogfeld **SIP-Auswahl** wird angezeigt.
4. Wählen Sie ein SIP-Modul zur Ansicht aus, und klicken Sie auf die Schaltfläche **Version**. Das Dialogfeld **SIP-Version** wird angezeigt.
5. Klicken Sie auf **X**, um das Dialogfeld **SIP-Version** zu schließen.

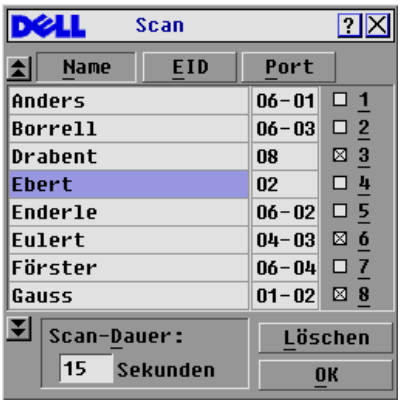
Scannen des Systems

Im Scan-Modus scannt die Einheit automatisch nacheinander alle Ports (ein Gerät nach dem anderen). Sie können bis zu 100 Geräte scannen, wobei Sie angeben, welche Geräte gescannt werden sollen und wie lange (in Sekunden) jedes Gerät angezeigt wird. Die Scan-Reihenfolge wird von der Position des Geräts in der Liste bestimmt. Die Liste wird immer in der Scan-Reihenfolge angezeigt. Es besteht jedoch die Möglichkeit, den Gerätenamen oder die EID-Nummer durch Betätigen der entsprechenden Schaltfläche anzuzeigen.

So fügen Sie der Scan-Liste Geräte hinzu:

1. Betätigen Sie die Taste <Druck>, um die OSCAR-Benutzeroberfläche aufzurufen. Das **Hauptmenü** wird angezeigt.
2. Klicken Sie auf **Setup – Scan**. Das Dialogfeld **Scannen** wird angezeigt.

Abbildung 3-12. Dialogfeld „Scannen“



3. Das Dialogfeld enthält eine Liste aller an die Einheit angeschlossenen Geräte. Aktivieren Sie das Kontrollkästchen neben den Geräten, die Sie scannen möchten.
   – oder –
   Doppelklicken Sie auf einen Gerätenamen oder Port.
   – oder –
   Drücken Sie <Alt> und die Nummer des Geräts, das gescannt werden soll. Sie können bis zu 16 Geräte aus der gesamten Liste auswählen.
4. Geben Sie im Feld **Zeit** die Anzahl der Sekunden (3 bis 99) ein, die verstreichen sollen, bevor das nächste Gerät in der Scan-Liste gescannt wird.

5 Klicken Sie auf **OK**.

So entfernen Sie ein Gerät aus der Scan-Liste:

1 Wählen Sie im Dialogfeld **Scannen** das Gerät, das entfernt werden soll.
– oder –
Doppelklicken Sie auf den Gerätenamen oder Port.
– oder –
Klicken Sie auf die Schaltfläche **Löschen**, um alle Geräte aus der Scan-Liste zu entfernen.

2 Klicken Sie auf **OK**.

So starten Sie den Scan-Modus:

1 Betätigen Sie die Taste <Druck>, um die OSCAR-Benutzeroberfläche aufzurufen. Das **Hauptmenü** wird angezeigt.

2 Klicken Sie auf **Befehle**. Das Dialogfeld **Befehle** wird angezeigt.

3 Aktivieren Sie im Dialogfeld **Befehle** das Kontrollkästchen **Scan aktiviert**.

4 Klicken Sie auf **X**, um das Dialogfeld **Befehle** zu schließen.

HINWEIS: Wenn Sie auf die Schaltfläche „Hinzufügen/Entfernen" klicken, während ein Gerät markiert ist, ändert sich jeweils der Status des Kontrollkästchens für das markierte Gerät.

So beenden Sie den Scan-Modus:

1 Wählen Sie ein Gerät aus, wenn die OSCAR-Benutzeroberfläche geöffnet ist.
– oder –
Bewegen Sie die Maus oder betätigen Sie eine beliebige Taste auf der Tastatur, wenn OSCAR nicht geöffnet ist. Das Scannen wird am aktuell ausgewählten Gerät angehalten.
– oder –
Betätigen Sie die Taste <Druck>. Das **Hauptmenü** wird angezeigt.

2 Klicken Sie auf **Befehle**. Das Dialogfeld **Befehle** wird angezeigt.

3 Deaktivieren Sie das Kontrollkästchen **Scan aktiviert**.

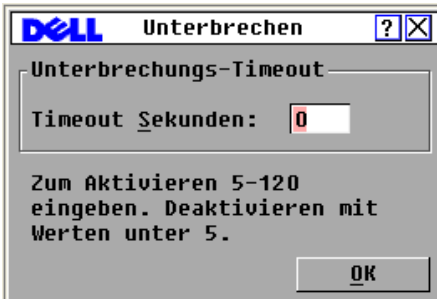
Einstellen der Unterbrechungswarnmeldung

Administratoren und Benutzer mit den gleichen oder höheren Zugriffsrechten als der aktuelle Benutzer können KVM-Sitzungen unterbrechen (trennen) und die Steuerung des Zielgeräts übernehmen. Sie können auswählen, ob der ursprüngliche Benutzer in einer Warnmeldung darauf hingewiesen werden soll, dass die Sitzung unterbrochen wird. Außerdem können Sie festlegen, wie lange die Einheit auf eine Reaktion des ursprünglichen Benutzers auf die Warnmeldung wartet.

So können Sie die Einstellungen für die Unterbrechungswarnmeldung anzeigen und ändern:

1. Betätigen Sie die Taste <Druck>, um OSCAR zu starten. Das **Hauptmenü** wird angezeigt.
2. Klicken Sie auf **Setup > Unterbrechen**.
3. Geben Sie die gewünschte Anzahl an Sekunden in das Feld **Timeout Sekunden** ein.
   - Wenn Sie einen Wert zwischen 0 und 4 Sekunden eingeben, wird der ursprüngliche Benutzer nicht gewarnt, bevor die Sitzung unterbrochen wird.
   - Wenn Sie einen Wert zwischen 5 und 120 Sekunden eingeben, wird der ursprüngliche Benutzer gewarnt. In diesem Fall kann der Benutzer das Zielgerät während der im Feld **Timeout Sekunden** angegebenen Zeitdauer weiterhin verwenden. Die Sitzung wird unterbrochen, wenn der Benutzer auf **OK** klickt oder wenn der angegebene Zeitraum abläuft.

Abbildung 3-13. Dialogfeld „Unterbrechen“



4. Klicken Sie auf **OK**, um die Einstellungen zu speichern.

Anzeigen von Konfigurationsinformationen

Sie können die Konfiguration Ihres Remote Console Switches im Dialogfeld **Konfiguration** anzeigen. Dieses Dialogfeld bietet einen schnellen Zugriff auf die von Ihnen vorgenommenen Einstellungen und ermöglicht das Hinzufügen weiterer Funktionen, indem Sie auf die Schaltfläche **Lizenzschlüssel** klicken und den Lizenzschlüssel für eventuelle zusätzliche Funktionen eingeben.

HINWEIS: Wenn die Firmware keine Funktionen enthält, die eine Lizenz erfordern, ist die Schaltfläche nicht verfügbar.

So zeigen Sie die Systemkonfiguration an:

1. Betätigen Sie die Taste <Druck>, um die OSCAR-Benutzeroberfläche aufzurufen. Das **Hauptmenü** wird angezeigt.
2. Klicken Sie auf **Befehle – Konfiguration anzeigen**. Das Dialogfeld **Konfiguration** wird angezeigt.
3. Klicken Sie auf **Lizenzschlüssel**, um einen Lizenzschlüssel hinzuzufügen und eine neue Funktion zu aktivieren, oder klicken Sie auf **X**, um das Dialogfeld **Konfiguration** zu schließen und zum Dialogfeld **Setup** zurückzukehren.

Ausführen der Systemdiagnose

Die Systemintegrität kann mit dem Befehl **Diagnosetests** geprüft werden. Mit diesem Befehl werden die Subsysteme auf dem Main Board (Speicher, Kommunikation, Switch-Steuerung und Videokanäle) für jeden System-Controller überprüft. Wenn Sie die Option **Diagnosetests** auswählen, wird eine Warnmeldung angezeigt, dass alle Benutzer (remote und lokal) getrennt werden. Klicken Sie zur Bestätigung und zum Starten des Tests auf **OK**.

Das Dialogfeld **Diagnosetests** wird angezeigt. In der oberen Hälfte des Dialogfelds werden die Hardware-Tests angezeigt. In der unteren Hälfte werden die getesteten SIP-Module in drei Kategorien eingeteilt: Online, Offline und Suspekt.

HINWEIS: Ein SIP-Modul wird ggf. während der Aktualisierung als offline angezeigt.

Abbildung 3-14. Dialogfeld „Diagnosetests“

Nach Abschluss der einzelnen Tests wird jeweils das Symbol für einen fehlerfreien (grüner Kreis) bzw. einen fehlerhaften Test (rotes X) auf der linken Seite der getesteten Einheit angezeigt. In der folgenden Tabelle werden die einzelnen Tests näher beschrieben.

Tabelle 3-4. Beschreibung der Diagnosetests

Test	Beschreibung
Firmware-CRCs	Meldet den Zustand der Switch-Firmwaredatei.
Remotebenutzervideo	Meldet, ob digitale Videokanäle installiert, aber nicht funktionsfähig sind.
LAN-Verbindung	Zeigt an, ob die LAN-Verbindung aktiv ist und ob seit der letzten Ausführung der Diagnosetests Datenverkehr verzeichnet wurde.
SIP-Module online	Gibt die Gesamtanzahl der momentan angeschlossenen und eingeschalteten SIP-Module an.
SIP-Module offline	Gibt die Anzahl der SIP-Module an, die bislang erfolgreich angeschlossen wurden und ausgeschaltet sind.
Suspekte SIP-Module	Gibt die Anzahl der SIP-Module an, die erkannt wurden, aber entweder für eine Verbindung nicht verfügbar sind oder während des Ping-Tests Pakete verloren haben.

So führen Sie die Diagnosetests aus:

1. Betätigen Sie die Taste <Druck>, um die OSCAR-Benutzeroberfläche aufzurufen. Das **Hauptmenü** wird angezeigt.
2. Klicken Sie auf **Befehle – Diagnosetests**. In einer Warnmeldung werden Sie darauf hingewiesen, dass alle Benutzerverbindungen getrennt werden.
3. Klicken Sie auf **OK**, um die Diagnosetests zu starten.
   – oder –
   Klicken Sie auf **X** oder betätigen Sie die Taste <Esc>, um das Dialogfeld zu beenden, ohne Diagnosetests auszuführen.
4. Alle Benutzerverbindungen werden getrennt und das Dialogfeld **Diagnosetests** wird angezeigt.
5. Nach Abschluss der einzelnen Tests wird jeweils ein Symbol für einen fehlerfreien (grüner Kreis) bzw. fehlerhaften Test (rotes X) angezeigt. Der Test ist beendet, wenn das Symbol für den letzten Test angezeigt wird.

Senden an Server

Der analoge Benutzer kann in einem System mehrere Server gleichzeitig steuern, um sicherzustellen, dass alle ausgewählten Server identische Eingaben erhalten. Sie können Tastenanschläge und/oder Mausbewegungen unabhängig voneinander senden.

HINWEIS: Sie können an bis zu 16 Geräte gleichzeitig senden, und zwar an jeweils ein Gerät pro ARI-Port.

HINWEIS: Senden von Tastenanschlägen – Der Tastaturstatus muss für alle Geräte, an die gesendet wird, identisch sein, damit die Tastenanschläge auf dieselbe Weise interpretiert werden. Besonders ist darauf zu achten, dass sich die <Feststell-> und <Num-Taste> bei allen Tastaturen im gleichen Modus befinden. Die Einheit versucht zwar, die Tastenanschläge simultan an die ausgewählten Geräte zu senden, es kann aber vorkommen, dass Geräte die Übertragung blockieren und somit verzögern.

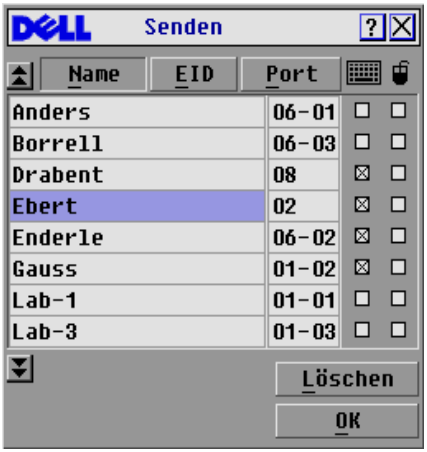
HINWEIS: Mausbewegungen senden – Für das ordnungsgemäße Arbeiten der Maus müssen auf allen Systemen die gleichen Maustreiber, Desktops (identisch platzierte Symbole) und Bildschirmauflösungen installiert sein. Außerdem muss sich die Maus in genau der gleichen Position auf allen Bildschirmen befinden. Da diese Voraussetzungen nur sehr schwer zu erfüllen sind, kann das Senden von Mausaktionen an mehrere Systeme zu unvorhersehbaren Ergebnissen führen.

So greifen Sie auf das Dialogfeld „Senden“ zu:

1 Betätigen Sie die Taste <Druck>, um die OSCAR-Benutzeroberfläche aufzurufen. Das **Hauptmenü** wird angezeigt.

2 Klicken Sie auf **Setup – Senden**. Das Dialogfeld **Senden** wird angezeigt.

Abbildung 3-15. Dialogfeld „Senden“



So senden Sie an die ausgewählten Geräte:

1 Aktivieren Sie im Dialogfeld **Senden** die Kontrollkästchen für Maus und/oder Tastatur bei den Geräten, die die gesendeten Befehle empfangen sollen.
– oder –
Drücken Sie den *Pfeil-nach-oben* oder den *Pfeil-nach-unten*, um den Cursor zum Zielgerät zu bewegen. Drücken Sie anschließend <Alt+K>, um das Kontrollkästchen für die Tastatur zu aktivieren, und/oder <Alt+M>, um das Kontrollkästchen für die Maus zu aktivieren. Wiederholen Sie diesen Vorgang für weitere Geräte.

2 Klicken Sie auf **OK**, um die Einstellungen zu speichern und zum Dialogfeld **Setup** zurückzukehren. Klicken Sie auf **X** oder betätigen Sie die Taste <Esc>, um zum **Hauptmenü** zurückzukehren.

3 Klicken Sie auf **Befehle**. Das Dialogfeld **Befehle** wird angezeigt.

4 Aktivieren Sie das Kontrollkästchen **Senden aktiviert**, um das Senden zu aktivieren. Das Dialogfeld zur Bestätigung/Ablehnung von **Senden aktiviert** wird angezeigt.

5 Klicken Sie auf **OK**, um das Senden zu aktivieren. Klicken Sie auf **X**, oder betätigen Sie die Taste <Esc>, um den Vorgang abzubrechen und zum Dialogfeld **Befehle** zurückzukehren.

6 Sobald das Senden aktiviert ist, können Sie an der Benutzerkonsole die Informationen eingeben und/oder die Mausbewegungen vornehmen, die gesendet werden sollen. Es kann nur auf Geräte in der Liste zugegriffen werden.

HINWEIS: Wenn der Sendemodus aktiviert ist, wird der Zugriff für alle anderen Benutzer blockiert.

So deaktivieren Sie das Senden:

Deaktivieren Sie im Dialogfeld **Befehle** das Kontrollkästchen **Senden aktiviert**.

Stromüberwachungsgeräte

Sie können unterstützte PDUs über die OSCAR-Oberfläche steuern.

HINWEIS: Diese Funktion ist nur für den 2321DS Remote Console Switch verfügbar.

Fenster „Strom“

Über das Fenster **Strom** können Sie anzeigen, welche Ausgänge welche Geräte steuern und ob der Ausgang aktiviert oder deaktiviert ist. Sie können den Strom für ein ausgewähltes Gerät einschalten, ausschalten oder aus- und wieder einschalten. Der Status der einzelnen Ausgänge wird durch ein oder mehrere Statussymbole in der rechten Spalte angegeben. Die folgende Tabelle beschreibt die Statussymbole.

Tabelle 3-5. Statussymbole im Fenster „Strom“

Symbol	Beschreibung
	Ausgang ist ein.
	Ausgang ist aus.

Symbol	Beschreibung
	Warten bis Ausgang einschaltet.
	Warten bis Ausgang ausschaltet.

So schalten Sie den Strom für ein Gerät ein, aus oder aus- und wieder ein:

1. Betätigen Sie die Taste <Druck>, um die OSCAR-Benutzeroberfläche aufzurufen. Das **Hauptmenü** wird angezeigt.
2. Klicken Sie auf **Befehle – Strom**.
3. Wählen Sie das Gerät aus, das gesteuert werden soll.

HINWEIS: Es können mehrere Geräte ausgewählt werden.

4. Klicken Sie auf **Ein**, **Aus** oder auf **Neustart**.

Fenster „PDUs“

Im Fenster **PDUs** können Sie anzeigen, welche PDUs an Ihr System angeschlossen sind. Der Status der einzelnen PDUs wird durch ein oder mehrere Statussymbole in der rechten Spalte angegeben. Die folgende Tabelle beschreibt die Statussymbole.

Tabelle 3-6. Statussymbole im Fenster „PDUs“

Symbol	Beschreibung
	Ausgang ist online.
	Ausgang ist offline.
	Ausgang ist überlastet.

So zeigen Sie angeschlossene PDUs an:

Öffnen Sie das Fenster **PDUs**. Das Fenster enthält eine Auflistung aller PDUs, die an Ihr System angeschlossen sind.

Fenster „PDU-Einstellungen“

Ausgehend vom Fenster **PDUs** können Sie das Fenster **PDU-Einstellungen** anzeigen, in dem Sie PDU-Parameter anzeigen und ändern können.

So zeigen Sie PDU-Einstellungen an bzw. ändern diese:

1. Betätigen Sie die Taste <Druck>, um die OSCAR-Benutzeroberfläche aufzurufen. Das **Hauptmenü** wird angezeigt.
2. Klicken Sie auf **Setup – PDUs**.
3. Führen Sie einen der folgenden Schritte aus:

   Wählen Sie einen PDU-Namen aus und klicken Sie dann auf **Einstellungen**, um das Fenster **PDU-Einstellungen** zu öffnen.

   – oder –

   Wählen Sie einen PDU-Namen aus und betätigen Sie dann die <Eingabetaste>, um das Fenster **PDU-Einstellungen** zu öffnen.

   – oder –

   Doppelklicken Sie auf den PDU-Namen, um das Fenster **PDU-Einstellungen** zu öffnen.
4. Führen Sie einen der folgenden Schritte aus:
   a. Geben Sie im Feld **Name** den PDU-Namen ein.
   b. Geben Sie im Feld **Verzögerung zwischen Aus- und Einschalten** die Anzahl der Sekunden ein, die der Remote Console Switch zwischen dem Aus- und Einschalten warten soll.
5. Klicken Sie auf **OK**.

Fenster „PDU-Eingänge“

Im Fenster **Eingänge** können Sie Eingangsparameter anzeigen und ändern.

HINWEIS: Sie können nur Eingangsparameter für eine PDU ändern, die aktuell online ist.

So zeigen Sie die Einstellungen für einen **PDU-Eingang** an bzw. ändern diese:

1. Betätigen Sie die Taste <Druck>, um die OSCAR-Benutzeroberfläche aufzurufen. Das **Hauptmenü** wird angezeigt.
2. Klicken Sie auf **Setup – PDUs**.

3 Führen Sie einen der folgenden Schritte aus:

Wählen Sie einen PDU-Namen aus und klicken Sie dann auf **Einstellungen**, um das Fenster **PDU-Einstellungen** zu öffnen.

– oder –

Wählen Sie einen PDU-Namen aus und betätigen Sie dann die <Eingabetaste>, um das Fenster **PDU-Einstellungen** zu öffnen.

– oder –

Doppelklicken Sie auf den PDU-Namen, um das Fenster **PDU-Einstellungen** zu öffnen.

4 Klicken Sie auf **Eingänge**.

5 Geben Sie eine ganze Zahl in den Feldern **Min. Ampere** bzw. **Max. Ampere** ein.

6 Klicken Sie auf **OK**.

Fenster „PDU-Ausgänge“

Im Fenster **Ausgänge** können Sie einen Ausgang auswählen und das Fenster **Ausgangs-Einstellungen** öffnen, um ausgangsspezifische Parameter festzulegen.

HINWEIS: Sie können nur Ausgangsparameter für eine PDU ändern, die aktuell online ist.

So zeigen Sie die Einstellungen für einen **PDU-Ausgang** an bzw. ändern diese:

1 Betätigen Sie die Taste <Druck>, um die OSCAR-Benutzeroberfläche aufzurufen. Das **Hauptmenü** wird angezeigt.

2 Klicken Sie auf **Setup – PDUs**.

3 Führen Sie einen der folgenden Schritte aus:

Wählen Sie einen PDU-Namen aus und klicken Sie dann auf **Einstellungen**, um das Fenster **PDU-Einstellungen** zu öffnen.

– oder –

Wählen Sie einen PDU-Namen aus und betätigen Sie dann die <Eingabetaste>, um das Fenster **PDU-Einstellungen** zu öffnen.

– oder –

Doppelklicken Sie auf den PDU-Namen, um das Fenster **PDU-Einstellungen** zu öffnen.

4 Klicken Sie auf **Ausgänge**.

5 Führen Sie einen der folgenden Schritte aus:

Wählen Sie einen Ausgang aus und klicken Sie dann auf **Einstellungen**, um das Fenster **Ausgangs-Einstellungen** zu öffnen.

– oder –

Wählen Sie einen Ausgang aus und betätigen Sie dann die <Eingabetaste>, um das Fenster **Ausgangs-Einstellungen** zu öffnen.

– oder –

Doppelklicken Sie auf einen Ausgang und öffnen Sie das Fenster **Ausgangs-Einstellungen**.

6 Wählen Sie den Ausgang aus, der geändert werden soll.

7 Führen Sie einen der folgenden Schritte aus:

a Geben Sie im Feld **Name** den Namen des Ausgangs ein.

b Geben Sie im Feld **Intervall Strom Ein** die Anzahl der Sekunden ein, die der Remote Console Switch zwischen dem Ein- und Ausschalten warten soll.

HINWEIS: Das **Intervall Strom Ein** muss eine ganze Zahl zwischen 0 und 7200 sein.

8 Klicken Sie auf **OK**.

4

Verwenden des Viewers

Über den Viewer können Sie eine Verbindung zu einem Server im Remote Console Switch-System herstellen. Der **Viewer** ermöglicht die vollständige Steuerung von Tastatur, Monitor und Maus eines Servers.

Sie können zudem eine benutzerdefinierte Serverliste prüfen, indem Sie einzelne Server für die Anzeige der **Miniaturansichten des Viewers** aktivieren. Diese Ansicht enthält eine Reihe von Miniaturansichten, die kleine, skalierte, nicht interaktive Versionen der Bildschirmanzeige eines Servers darstellen. Weitere Informationen finden Sie unter „Anzeigen von mehreren Servern über den Scan-Modus“ auf Seite 80.

Sie können den Viewer über die Remote Console Switch Software oder über die integrierte Weboberfläche aufrufen. Dieses Kapitel beschreibt die Verwendung des Viewers über die integrierte Weboberfläche. Anweisungen zur Verwendung des Viewers über die Remote Console Switch-Software finden Sie in der Bedienungsanleitung der Dell Remote Console Switch-Software oder in der in die Software integrierten Hilfe.

Zugriff auf Server über die integrierte Weboberfläche

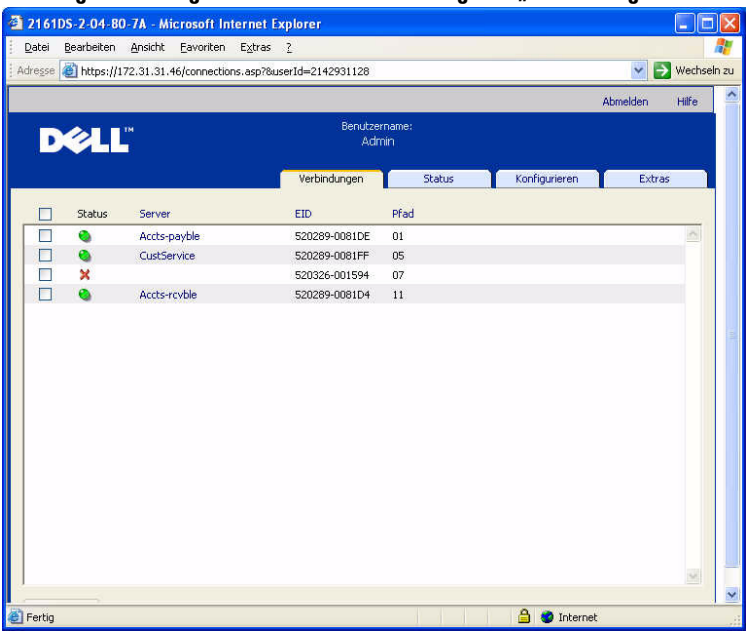
Über das Register **Verbindungen** auf der integrierten Weboberfläche können Sie die angeschlossenen Server und ihren Status anzeigen. Klicken Sie auf einen Servernamen, um den Viewer zu starten.

Anweisungen zum Starten der integrierten Weboberfläche finden Sie unter „Starten der integrierten Weboberfläche“ auf Seite 34.

Tabelle 4-1. Server-Statussymbole der integrierten Weboberfläche

Symbol	Beschreibung
	Server ist online
	Server ist offline
	Server ist nicht verfügbar

Abbildung 4-1. Integrierte Weboberfläche – Register „Verbindungen“



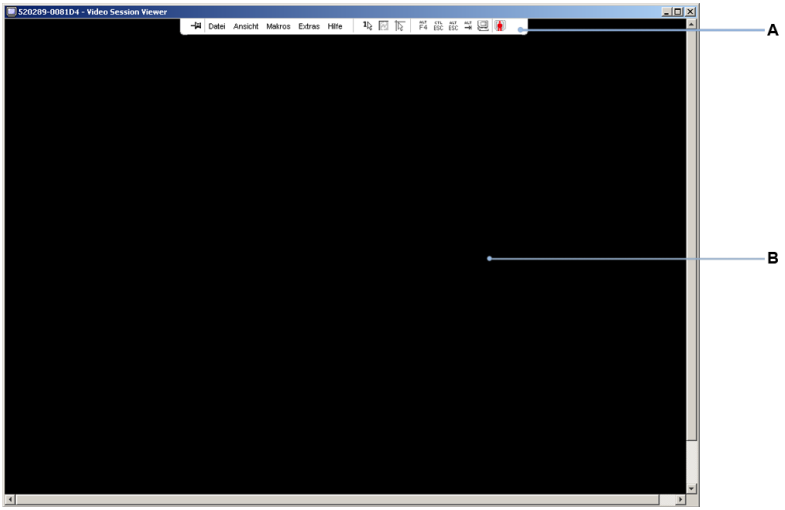
Interaktion mit dem angezeigten Server

Sobald Sie eine Verbindung mit einem Server hergestellt haben, wird das Desktop-Fenster dieses Servers auf Ihrem Bildschirm angezeigt. Dieses Desktop-Fenster wird in einem separaten Fenster geöffnet. Sie sehen zwei Cursor: den lokalen Cursor und den Cursor des Servers. Sie müssen die beiden Cursor möglicherweise aufeinander ausrichten, wenn sie sich nicht zusammen bewegen, oder bei springenden Cursorbewegungen die Bildschirmeinstellungen anpassen. Von diesem Fenster aus können Sie wie bei einem direkten Zugriff auf alle normalen Funktionen dieses Servers zugreifen. Sie können außerdem Viewer-spezifische Tasks durchführen, wie beispielsweise spezielle Makrobefehle an den Server senden.

HINWEIS: Wenn Sie während einer Remote-Videositzung langsame Mausreaktionen feststellen, deaktivieren Sie die Mausbeschleunigung im Betriebssystem des Zielgeräts und stellen Sie die Mausgeschwindigkeit auf 50 % ein.

Funktionen des Viewer-Fensters

Abbildung 4-2. Viewer-Fenster

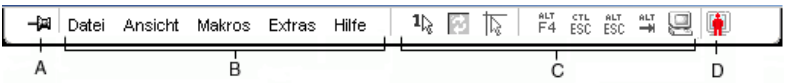


A **Menüleiste:** Zugriff auf viele Funktionen des Viewers.

B **Server-Desktop, auf den zugegriffen wird:** Interagieren Sie über dieses Fenster mit dem Server.

Viewer-Menüleiste

Abbildung 4-3. Viewer-Menüleiste



A **Pin:** Klicken Sie auf den Pin, um die Menüleiste in Position zu halten. Dadurch wird gewährleistet, dass die Menüleiste nicht ausgeblendet wird, wenn Sie den Mauszeiger von der Menüleiste weg bewegen.

B **Menüoptionen:** Die Menüs bieten Zugriff auf Funktionen, die über den Viewer zur Verfügung stehen.

C **Schaltflächen der Symbolleiste:** Sie können der Symbolleiste bis zu zehn Schaltflächen hinzufügen. Mithilfe dieser Schaltflächen wird der schnelle Zugriff auf die festgelegten Funktionen und Tastaturmakros ermöglicht. Standardmäßig werden die Schaltflächen „Lokalen Cursor ausrichten“, „Bildschirm aktualisieren“ und „Einzelcursor-Modus“ angezeigt.

D **Verbindungsstatusanzeige:** Die Verbindungsstatusanzeige gibt an, auf welche Weise der Benutzer für diesen Server mit der Einheit verbunden ist. Weitere Informationen finden Sie im Abschnitt „Teilen der Verbindung“ auf Seite 90.

Verbindungsstatusanzeige	Teilungs-Modus
	Exklusivmodus
	Aktive Verbindung (normale, nicht-exklusive Sitzung ohne Teilen)
	Aktives Teilen (Primärbenutzer)
	Aktives Teilen (Sekundärbenutzer)
	Passives Teilen
	Tarnmodus

Anpassen des Viewers

Sie können die **Viewer**-Einstellungen an Ihre Anforderungen anpassen, einschließlich der Einstellungen für Bildschirmauflösung, Symbolleiste und Tastaturmakros.

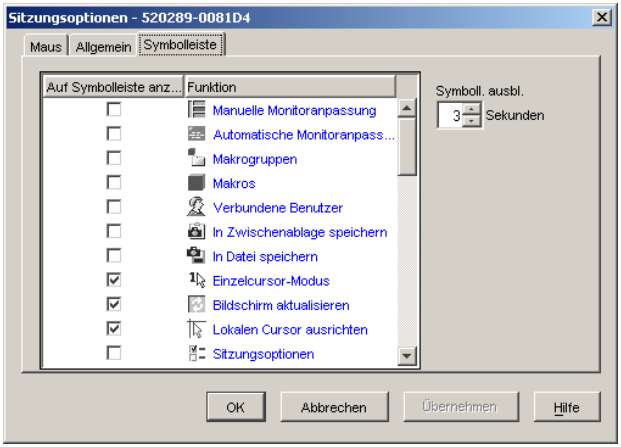
Anpassen der Viewer-Symbolleiste

Sie können der Symbolleiste bis zu zehn Schaltflächen hinzufügen. Mithilfe dieser Schaltflächen wird der schnelle Zugriff auf die festgelegten Funktionen und Tastaturmakros ermöglicht. Standardmäßig werden die Schaltflächen **Lokalen Cursor ausrichten**, **Bildschirm aktualisieren** und **Einzelcursor-Modus** angezeigt.

So fügen Sie der Symbolleiste Schaltflächen hinzu:

1. Wählen Sie im Menü **Extras** im **Viewer** den Befehl **Sitzungsoptionen**. Die Symbolleiste „Sitzungsoptionen“ wird angezeigt.
2. Klicken Sie auf das Register **Symbolleiste**.
3. Klicken Sie auf die Schaltflächen, die der **Viewer**-Symbolleiste hinzugefügt werden sollen.
4. Klicken Sie auf **OK**, um die Änderungen zu übernehmen und zum Hauptfenster des **Viewers** zurückzukehren.

Abbildung 4-4. Dialogfeld „Sitzungsoptionen“ – Register „Symbolleiste“



Einstellen der Zeitverzögerung für das Ausblenden der Symbolleiste

Die Symbolleiste wird ausgeblendet, sobald Sie den Mauszeiger wegbewegen, es sei denn, die Schaltfläche **Pin** wurde aktiviert. Sie können die Zeitdauer zwischen Bewegen des Mauszeigers und Ausblenden der Symbolleiste anpassen, indem Sie die **Verzögerung für das Ausblenden der Symbolleiste** festlegen.

So ändern Sie die **Verzögerung nach dem Ausblenden der Symbolleiste**:

1. Wählen Sie im Menü **Extras** im **Viewer** den Befehl **Sitzungsoptionen**. Die Symbolleiste „Sitzungsoptionen“ wird angezeigt.
2. Klicken Sie auf das Register **Symbolleiste**.
3. Geben Sie im Feld für die **Verzögerung nach dem Ausblenden der Symbolleiste** an, wie viele Sekunden die Symbolleiste angezeigt werden soll, nachdem der Mauszeiger wegbewegt wurde.
   – oder –
   Verwenden Sie die Schaltflächen **Nach oben** und **Nach unten**, um die Anzahl von Sekunden zu erhöhen oder zu verringern, die die Symbolleiste angezeigt werden soll, nachdem der Mauszeiger wegbewegt wurde.
4. Klicken Sie auf **OK**, um die vorgenommenen Änderungen zu übernehmen und zum Hauptfenster des **Viewers** zurückzukehren.

Vergrößern und Aktualisieren des Viewers

Standardmäßig werden drei Schaltflächen in der Viewer-Symbolleiste angezeigt, mit denen Sie die Anzeige des Viewers anpassen können. Mit der ersten Schaltfläche kann der Viewer auf den Einzelcursor-Modus eingestellt werden. Dadurch kann die Maus im Viewer so verwendet werden, als wäre sie die Maus am Server. Wenn der Viewer auf den Einzelcursor-Modus eingestellt ist, wird der lokale Cursor nicht angezeigt.

HINWEIS: Der Einzelcursor-Modus funktioniert nur auf Windows-Plattformen.

Mithilfe der zweiten Schaltfläche können die Mauszeiger aufeinander ausgerichtet werden und die dritte Schaltfläche ermöglicht die Aktualisierung des Bildschirms.

Abbildung 4-5. Viewer-Symbolleiste – Schaltflächen zum Anpassen der Anzeige

So stellen Sie den Viewer auf den Einzelcursor-Modus ein:

Klicken Sie in der Viewer-Symbolleiste auf die Schaltfläche Einzelcursor-Modus.

So richten Sie die Mauszeiger aufeinander aus:

Klicken Sie in der Viewer-Symbolleiste auf Lokalen Cursor ausrichten.
Der lokale Cursor wird auf den Cursor des Remote-Servers ausgerichtet.

So aktualisieren Sie den Bildschirm:

Klicken Sie in der Viewer-Symbolleiste auf die Schaltfläche Bildschirm aktualisieren.
– oder –
Wählen Sie im Viewer-Menü Ansicht – Aktualisieren aus. Die digitalisierte Bildschirmdarstellung wird vollständig neu generiert.

So gelangen Sie in den Vollbildmodus:

Klicken Sie in der oberen rechten Ecke des Viewers auf die Schaltfläche Maximieren.
– oder –
Wählen Sie im Viewer-Menü Ansicht – Vollbild aus. Das Desktop-Fenster wird ausgeblendet und nur der Server-Desktop, auf den gerade zugegriffen wird, ist sichtbar. Der Bildschirm wird auf eine Größe von maximal 1024 x 768 eingestellt. Wenn der Desktop eine höhere Auflösung besitzt, wird ein schwarzer Rahmen um das Vollbild angezeigt. Die unverankerte Symbolleiste wird angezeigt.

So verlassen Sie den Vollbildmodus:

Betätigen Sie <Esc>, um den Vollbildmodus zu verlassen und zum Desktop-Fenster zurückzukehren.

Anpassen der Viewer-Auflösung

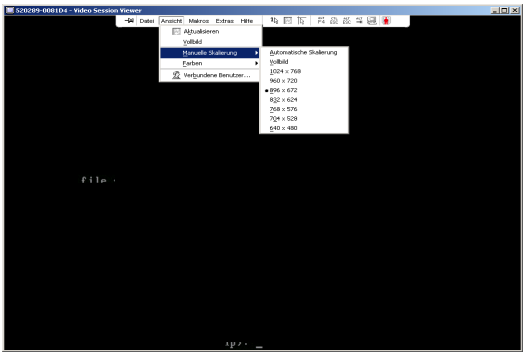
Wenn die **Automatische Skalierung** aktiviert ist, passt sich die Anzeige automatisch an, wenn die Größe des **Viewer**-Fensters während einer Sitzung verändert wird. Wenn Sie im Teilungs-Modus auf einen Kanal zugreifen, passt sich die Anzeige dahingehend an, dass sie mit der vom Primärbenutzer des Kanals ausgewählten Eingangsauflösung übereinstimmt. Dadurch wird verhindert, dass die Anzeige des Primärbenutzers beeinträchtigt wird. Wenn sich die Auflösung während einer Sitzung verändert, wird die Anzeige automatisch angepasst.

Wenn **Vollbild** ausgewählt ist, passt sich der **Viewer** an die Bildschirmauflösung des Servers an und stellt die Bildgröße bis zu einer Auflösung von maximal 1024 x 768 entsprechend ein.

So passen Sie die Größe des **Viewer**-Fensters an:

Wählen Sie in der Menüleiste **Ansicht – Skalierung – Automatische Skalierung** aus, damit die Bildschirmanzeige des Servers automatisch skaliert wird.
– oder –
Wählen Sie in der Menüleiste **Ansicht – Skalierung – Vollbild**.
– oder –
Wählen Sie eine Bildschirmauflösung aus dem Untermenü **Manuelle Skalierung** aus.

Abbildung 4-6. Viewer-Skalierung



Anpassen der Videoqualität

Der Viewer bietet Ihnen die Möglichkeit, Monitoranpassungen sowohl automatisch als auch manuell vorzunehmen. Im Allgemeinen wird die Videoqualität durch die Automatische Monitoranpassung auf die bestmögliche Ansicht optimiert. Möglicherweise möchten Sie aber die Videoqualität an besondere Anforderungen anpassen. Verwenden Sie für größere Änderungen der Einstellungen den Schieberegler und für die Feinabstimmung die Schaltflächen Plus (+) und Minus (–). Weitere Informationen zur manuellen Monitoranpassung finden Sie unter Abbildung 4-7.

Anpassen der Farbtiefe

HINWEIS: Der Befehl „Farben" kann nur vom Primärbenutzer verwendet werden. Er steht anderen Benutzern, die im Teilungs-Modus an der Sitzung teilnehmen, nicht zur Verfügung.

HINWEIS: Wenn die Option „Aktualisierung im Hintergrund" im Dialogfeld „Sitzungsoptionen" aktiviert ist, wird die Farbtiefe automatisch auf die optimale verfügbare Farbe eingestellt und kann nicht verändert werden.

Mit dem Untermenü Farben können Sie die Farbtiefen einstellen, mit denen das Digitalbild komprimiert werden kann. Die Remote Console Switches unterstützen den DVC-Algorithmus (Dambrackas Video Compression), der es Benutzern der RCS Software ermöglicht, die Anzahl der sichtbaren Farben in einem Remote-Sitzungsfenster anzupassen. Sie können auswählen, ob viele Farben für eine möglichst getreue Darstellung angezeigt werden, oder weniger Farben, um das über das Netzwerk übertragene Datenvolumen zu reduzieren.

Für die Anzeige des Viewer-Fensters sind folgende Optionen möglich: Optimale verfügbare Farbe (langsamere Aktualisierung), Optimale Kompression (schnellste Aktualisierung), eine Kombination aus Optimaler Farbe und Optimaler Kompression sowie Grauskala.

Die Farbtiefen von einzelnen Ports und Kanälen können durch Auswahl des Befehls Ansicht – Farben in einem Remote-Sitzungsfenster festgelegt werden. Diese Einstellungen werden für jeden Port und Kanal einzeln gespeichert.

So stellen Sie die Farbtiefe ein:

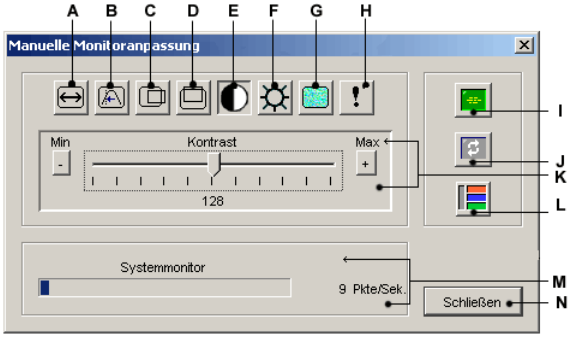
Wählen Sie im Menü Ansicht den Befehl Farben und dann im Untermenü Farben die gewünschte Farbtiefe aus.

So passen Sie die Videoqualität des **Viewer** -Fensters manuell an:

1. Wählen Sie im **Viewer**-Menü **Extras – Manuelle Monitoranpassung** aus. Das Dialogfeld **Manuelle Monitoranpassung** wird angezeigt.
2. Klicken Sie auf das Symbol des Merkmals, das Sie ändern möchten.
3. Verwenden Sie den Schieberegler oder klicken Sie auf die Schaltfläche **Minus (–)** oder **Plus (+)**, um die Parameter für jedes geklickte Symbol einzustellen. Die Einstellungen werden sofort im **Viewer**-Fenster sichtbar.
4. Wenn Sie den Vorgang beendet haben, klicken Sie auf **Schließen**, um das Dialogfeld **Manuelle Monitoranpassung** zu verlassen.

Optionen des Dialogfelds „Manuelle Monitoranpassung“

Abbildung 4-7. Dialogfeld „Manuelle Monitoranpassung“



A Image-Aufnahmebreite

B Feineinstellung für Pixel-Sampling

C Horizontale Image-Aufnahme

D Vertikale Image-Aufnahme

E Kontrast

F Helligkeit

G Rauschschwelle

H Prioritätsschwelle

I Automatische Monitoranpassung

J Bildschirm aktualisieren

K Schieberegler

L Testbild

M Systemmonitor

N Schaltfläche „Schließen“

Minimieren der Farbverfälschungen von Remote-Videositzungen

Beim Aufbau von Remote-Videositzungen können Pixel-Farbverfälschungen aufgrund bestimmter Netzwerkbedingungen auftreten. Dieses Problem tritt meistens bei deckenden Hintergrundfarben auf. Es kann durch die Verwendung eines schwarzen Hintergrunds minimiert werden. Wenn ein farbiger Hintergrund verwendet wird, tritt eine Farbverfälschung oder Weißfärbung bei einer geringen Anzahl von Pixeln auf.

So minimieren Sie die Farbverfälschung der Remote-Video-Pixel:

1. Wählen Sie im Viewer-Menü Extras – Manuelle Monitoranpassung aus. Das Dialogfeld Manuelle Monitoranpassung wird angezeigt.
2. Wählen Sie Kontrast oder Helligkeit aus.
3. Passen Sie den Kontrast und die Helligkeit stufenweise an, bis sich die Bildqualität verbessert.
4. Die Einstellung der Rauschschwelle kann ebenso in Feinabstimmung unter Extras – Manuelle Monitoranpassung erfolgen.

HINWEIS: Die Absenkung der Rauschschwelle auf Null verursacht eine konstante Bildaktualisierung, starke Netzwerkauslastung und ein flackerndes Bild. Dell empfiehlt, die Rauschschwelle auf den höchsten Wert einzustellen, mit dem eine effiziente Systemleistung erreicht und gleichzeitig die Pixelfarben des Mauszeigerpfads wiederhergestellt werden können.

HINWEIS: Verwenden Sie bei der Einstellung der Rauschschwelle für größere Änderungen den Schieberegler und für die Feinabstimmung die Schaltflächen Plus (+) und Minus (–).

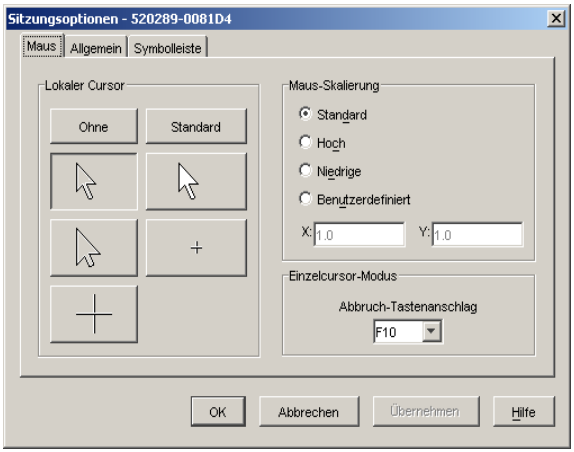
Verbessern der Farbanzeige des Bildschirmhintergrunds

Bei der Ansicht von Zielservern können Farbverschiebungen auftreten, wenn fotografische Aufnahmen oder farbintensive verlaufende Hintergründe ausgewählt wurden. Es wird empfohlen, für eine optimale Anzeigequalität und -leistung eine deckende Hintergrundfarbe über das Betriebssystem einzustellen.

Anpassen der Maus

Mit dem **Viewer** können Sie zwischen fünf verschiedenen Mauszeigeroptionen wählen, die Maus-Skalierung einrichten und Ihre Maus resynchronisieren, falls die Synchronisation nicht mehr stimmt. Dell empfiehlt, den lokalen Cursor durch Einstellen der Option **Lokaler Cursor** auf **Keine** auszuschalten. Hierdurch wird nur noch ein Cursor, der Remote-Cursor, auf dem Bildschirm angezeigt, was die Navigation vereinfacht.

Abbildung 4-8. Viewer-Dialogfeld „Sitzungsoptionen – Maus“



Einstellen der Maus-Skalierung

Sie können zwischen drei voreingestellten Optionen für die Maus-Skalierung wählen oder Ihre eigene Skalierung einrichten. Die drei Voreinstellungen sind: **Standard (1:1), Hoch (2:1) und Niedrig (1:2)**. Bei einem Skalierverhältnis von 1:1 sendet jede Mausbewegung auf dem Desktop-Fenster die gleiche Mausbewegung an den Server. Bei einer Skalierung von 2:1 sendet die gleiche Mausbewegung eine zweifache Mausbewegung. Eine Skalierung von 1:2 bewirkt eine Halbierung des Wertes.

So stellen Sie eine benutzerdefinierte Maus-Skalierung ein:

1. Wählen Sie im **Viewer**-Menü **Extras – Sitzungsoptionen** aus. Das Dialogfeld **Sitzungsoptionen** wird angezeigt.
2. Klicken Sie auf das Register **Maus**.

3 Klicken Sie auf das Optionsfeld **Benutzerdefiniert**. Die Felder **X** und **Y** werden verfügbar.

4 Geben Sie die Werte für die Maus-Skalierung in die Felder **X** und **Y** ein. Jede Mausbewegung wird mit den entsprechenden X- und Y-Skalierungsfaktoren multipliziert. Der zulässige Eingabebereich liegt zwischen 0.25 und 3.00.

Minimieren des Mausspureffekts

Wenn sich der Mauszeiger während einer Remote-Videositzung über den Bildschirm bewegt, behalten einige Pixel eine Farbverfälschung bei. Dieser Zustand wird als Mausspureffekt bezeichnet und wird von verschiedenen Stufen von Netzwerk- und anderem Rauschen in verschiedenen Umgebungen verursacht. Zur Minimierung des Mausspureffekts müssen Sie möglicherweise die **Rauschschwelle** im Dialogfeld **Manuelle Monitoranpassung** absenken.

So reduzieren Sie die Rauschschwelle:

1 Wählen Sie im **Viewer**-Menü **Extras – Manuelle Monitoranpassung** aus. Das Dialogfeld **Manuelle Monitoranpassung** wird angezeigt.

2 Klicken Sie auf das Symbol **Rauschschwelle einstellen**, um die Rauschschwelle entsprechend anzupassen.

3 Bewegen Sie den Schieberegler mithilfe der Maus zur Mitte der Skala und danach auf Null.

4 Verwenden Sie die Schaltflächen **Plus (+)** und **Minus (–)** am Ende des Schiebereglers, um eine Feineinstellung der Rauschschwelle auf knapp über Null zu erreichen.

HINWEIS: Durch das Einstellen der Rauschschwelle auf Null wird das Bild konstant aktualisiert, das Netzwerk stark belastet und das Bild flackert. Es wird empfohlen, die Rauschschwelle auf den höchsten Wert einzustellen, mit dem eine effiziente Systemleistung erreicht und gleichzeitig die Pixelfarben des Mauszeigerpfads wiederhergestellt werden können.

HINWEIS: Verwenden Sie bei der Einstellung der Rauschschwelle für größere Änderungen den Schieberegler und für die Feinabstimmung die Schaltflächen Plus (+) und Minus (–) an den Enden des Schiebereglers.

Verbessern der Mausleistung

Wenn Sie während einer Remote-Videositzung langsame Mausreaktionen feststellen oder die Mauszeiger nicht mehr synchronisiert sind, sollten Sie die Mausbeschleunigung im Betriebssystem des Zielservers deaktivieren.

Microsoft Windows:

- Deaktivieren Sie die Mausbeschleunigung.
- Stellen Sie die Mausgeschwindigkeit so ein, dass sich der Schieberegler genau in der Mitte befindet.

HINWEIS: Detaillierte Anweisungen finden Sie in der Produktdokumentation zu Ihrem Windows Betriebssystem.

Red Hat Linux:

1. Wählen Sie die Maus-Einstellungen von der Desktop-Steuerung aus.
2. Stellen Sie die Beschleunigung auf 1.0 ein.
3. Übernehmen Sie die Änderungen und resynchronisieren Sie die Maus über die Schaltfläche Lokalen Cursor/Maus ausrichten im Viewer.

Anzeigen von mehreren Servern über den Scan-Modus

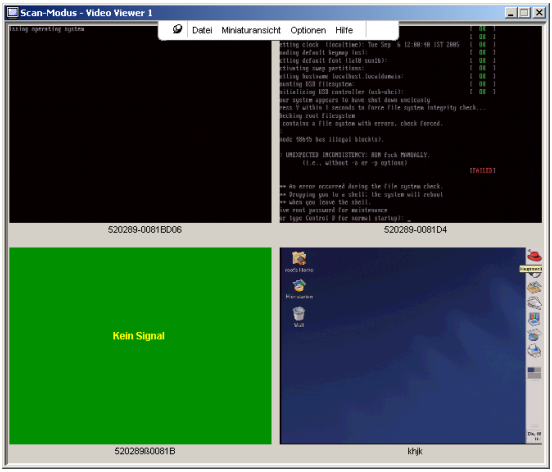
Mit dem Viewer können Sie mehrere Server gleichzeitig in den Miniaturansichten des Scan-Modus anzeigen. Diese Ansicht enthält eine Reihe von Miniaturansichten, die kleine, skalierte, nicht interaktive Versionen der Bildschirmanzeige eines Servers darstellen. Unter jeder Miniaturansicht werden der Servername sowie eine Statusanzeige dargestellt.

Scannen der Server

Mithilfe der Miniaturansichten können Sie eine Scan-Sequenz für bis zu 16 Server festlegen, um Ihre Server zu überwachen. Der Scan-Modus wechselt von einer Miniaturansicht zur nächsten, meldet sich an einem Server an und zeigt eine aktualisierte Bildschirmanzeige des Servers für eine benutzerdefinierte Zeit an (Anzeigezeit pro Server), bevor er sich von diesem Server abmeldet und zur nächsten Miniaturansicht übergeht. Sie können zudem eine Scan-Zeitverzögerung zwischen den Miniaturansichten eingeben (Zeit zwischen Servern). Während der Zeitverzögerung wird die letzte Miniaturansicht für alle Server in der Scan-Sequenz angezeigt; Sie sind jedoch an keinem dieser Server angemeldet.

Der Serverstatus wird unter jedem Rahmen durch eine Statusanzeige dargestellt. Die Größe der Miniaturansichten hängt von der Anzahl der Server in der Scan-Liste ab.

Abbildung 4-9. Viewer – Miniaturansichten



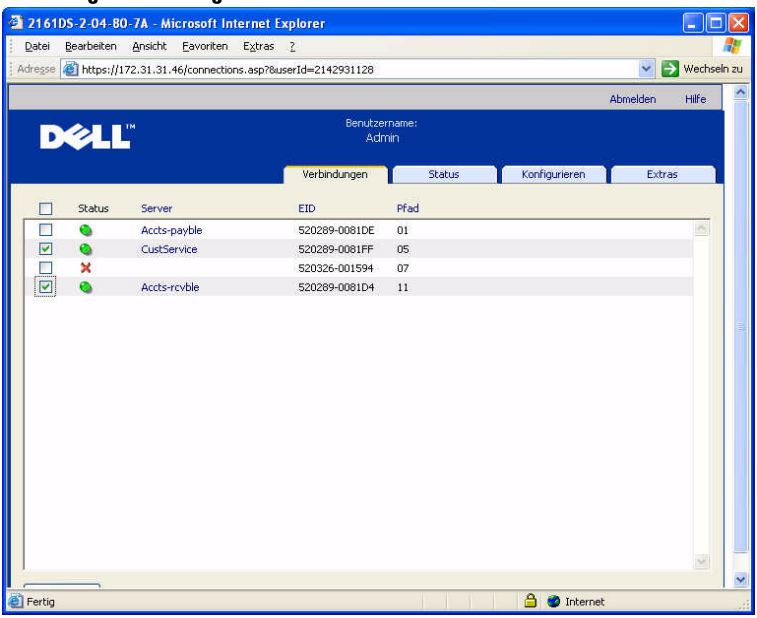
Der Scan-Modus hat eine niedrigere Priorität als eine aktive Verbindung. Wenn eine interaktive Sitzung mit einem Server besteht, wird dieser Server in der Scan-Sequenz übergangen und der Scan-Modus geht zum nächsten Server über. Es wird keine Fehlermeldung beim Anmelden angezeigt. Nach Beendigung der interaktiven Sitzung wird die Miniaturansicht wieder in die Scan-Sequenz aufgenommen. Falls ein anderer Benutzer eine aktive Verbindung mit einem Server hat, wird dieser Server übersprungen und ein rotes „X“ in der Statusanzeige unter dem Bildrahmen angezeigt.

Die Remote Console Switch Software kann die angeschlossenen Server von mehreren Remote Console Switches scannen, die integrierte Weboberfläche dagegen nur die angeschlossenen Servers eines einzelnen Remote Console Switches.

HINWEIS: Anweisungen zur Verwendung der Remote Console Switch-Software finden Sie in der Bedienungsanleitung der Dell Remote Console Switch-Software oder in der in die Software integrierten Hilfe.

Zugriff auf den Scan-Modus über die integrierte Weboberfläche

Abbildung 4-10. Integrierte Weboberfläche – Server scannen



So greifen Sie über die integrierte Weboberfläche auf den Scan-Modus zu:

1. Klicken Sie auf der integrierten Weboberfläche auf das Register **Verbindungen**.
2. Markieren Sie die Kontrollkästchen neben den Servern, die Sie scannen möchten.
3. Klicken Sie auf **Scannen**.

Statusanzeigen der Miniaturansicht

Die grüne LED zeigt an, dass ein Server momentan gescannt wird. Das rote X bedeutet, dass der letzte Scan des Servers nicht erfolgreich war. Das heißt, dass der Scan aufgrund von Zugriffsrechten oder Pfadfehlern (der Serverpfad auf dem Remote Console Switch war nicht verfügbar) oder aus anderen Gründen nicht durchgeführt werden konnte. Wenn Sie den Mauszeiger über dem roten X platzieren, wird eine QuickInfo angezeigt, die den Grund für den Fehler angibt.

Einrichten der Einstellungen für den Scan-Modus

So richten Sie die Einstellungen für den Scan-Modus ein:

1. Wählen Sie in der Anzeige der Miniaturansichten **Optionen – Einstellungen** aus. Das Dialogfeld **Einstellungen für Scan-Modus** wird angezeigt.
2. Geben Sie in das Feld **Anzeigezeit pro Server** die Zeitdauer (10 bis 60 Sekunden) ein, während der jede Miniaturansicht während des Scans aktiv sein soll.
3. Geben Sie in das Feld **Zeit zwischen Servern** die Zeitdauer (5 bis 60 Sekunden) ein, während der der Scan angehalten wird, bevor er zum nächsten Server übergeht.
4. Klicken Sie auf **OK**.

Navigation in den Miniaturansichten

Wenn eine bestimmte Miniaturansicht und das Menü **Miniaturansicht** markiert werden, kann eine interaktive Sitzung zu diesem Server gestartet, dieser Server zu der Scan-Sequenz hinzugefügt oder die Anmeldeberechtigungen für diesen Server eingestellt werden. Mit dem Menü **Optionen** kann auf die Scan-Einstellungen zugegriffen sowie das Scannen unterbrochen und die Größe der Miniaturansichten für alle Server eingestellt werden.

So starten Sie eine Server-Videositzung:

1. Wählen Sie eine Server-Miniaturansicht aus.
2. Wählen Sie in der Anzeige der Miniaturansichten **Miniaturansicht – [Servername] – Interaktive Sitzung anzeigen** aus.
   – oder –

   Klicken Sie mit der rechten Maustaste auf eine Server-Miniaturansicht und wählen Sie **Interaktive Sitzung anzeigen** aus. Der Server-Bildschirm wird in einem interaktiven **Viewer**-Fenster gestartet.

So aktivieren oder deaktivieren Sie einen Server in der Scan-Sequenz:

1. Wählen Sie eine Server-Miniaturansicht aus.
2. Wählen Sie in der Anzeige der Miniaturansichten **Miniaturansicht – [Servername] – Aktivieren** aus.
   – oder –

   Klicken Sie mit der rechten Maustaste auf eine Server-Miniaturansicht und wählen Sie **Aktivieren** aus. Dieser Server wird nun in die Scan-Sequenz der Server-Miniaturansichten aufgenommen oder daraus ausgeschlossen.

HINWEIS: Die Menüoption „Aktivieren“ wird bei jeder Auswahl zwischen markiert (aktiviert) und nicht markiert (deaktiviert) umgeschaltet.

HINWEIS: Wenn ein Benutzer auf einen Server zugreift, wird die Menüoption „Aktivieren“ für diese Server-Miniaturansicht deaktiviert.

So halten Sie eine Scan-Sequenz an und starten sie erneut:

Wählen Sie in der Anzeige der Miniaturansichten **Optionen – Scan anhalten** aus. Die Scan-Sequenz wird an der aktuellen Miniaturansicht angehalten, wenn die Anzeige der Miniaturansichten gerade einen aktiven Scan durchführt, oder sie startet den Scan erneut, wenn er gerade angehalten wurde.

So ändern Sie die Größe der Miniaturansichten:

1. Wählen Sie in der Anzeige der Miniaturansichten **Optionen – Größe der Miniaturansicht** aus.
2. Wählen Sie die gewünschte Größe der Miniaturansicht im Menü aus.

Mit Makros Tastenanschläge an Server senden

Mit dem Viewer-Menü **Makros** können auf einfache Weise mehrere Tastenanschläge an den Server gesendet werden. Der Viewer stellt eine Liste mit einer Auswahl von Standardtastenanschlägen für Microsoft Windows-Systeme, Linux-Systeme und für Sun-Systeme zur Verfügung.

So wählen Sie das verwendete System aus:

Klicken Sie im Viewer auf das Menü **Makros**. Klicken Sie auf **Im Menü anzeigen** und wählen Sie entweder **Windows**, **Sun** oder **Linux** aus.

So senden Sie Tastenanschläge an den Server:

Klicken Sie im Viewer auf das Menü **Makros** und wählen Sie den Namen des Makros aus, das die Tastenanschläge enthält, die Sie an den Server senden möchten. Abbildung 4-11, Abbildung 4-12 und Abbildung 4-13 zeigen die Standardmakros.

Abbildung 4-11. Erweitertes Viewer-Menü „Makros“ – Option „Windows“

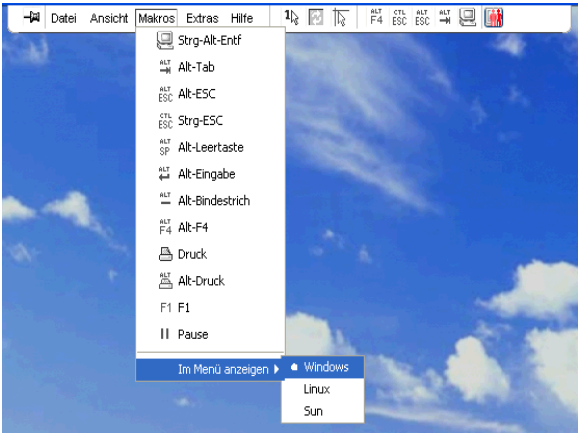


Abbildung 4-12. Erweitertes Viewer-Menü „Makros“ – Option „Linux“

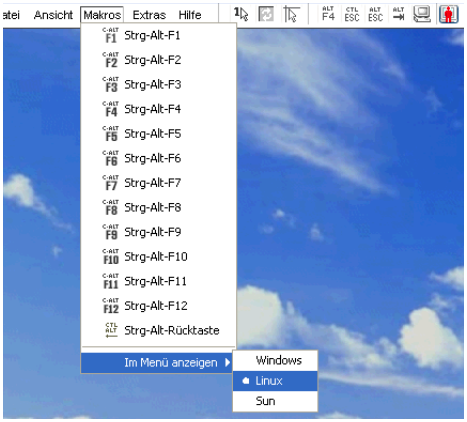
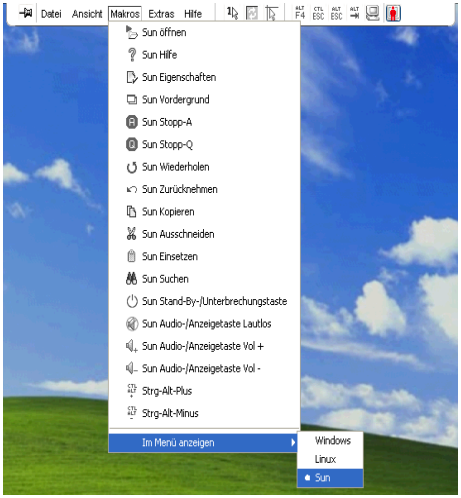


Abbildung 4-13. Erweitertes Viewer-Menü „Makros“ – Option „Sun“

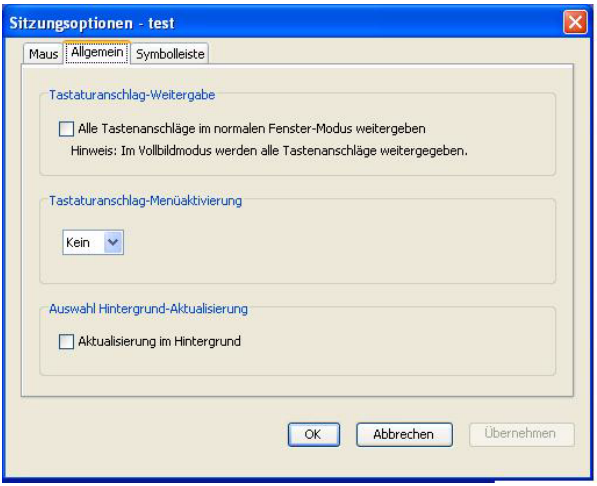


Sitzungsoptionen – Register „Allgemein“

Über das Register **Allgemein** im Dialogfeld „Sitzungsoptionen“ steuern Sie die Option **Tastaturanschlag-Weitergabe**, wenn Sie sich nicht im Vollbildmodus befinden, sowie die **Tastaturanschlag-Menüaktivierung** sowie die **Aktualisierung im Hintergrund**.

Durch Aktivieren oder Deaktivieren des Kontrollkästchens **Tastaturanschlag-Weitergabe** können Sie bestimmen, ob der Modus **Tastaturanschlag-Weitergabe** aktiviert sein soll. Standardmäßig ist die Option **Tastaturanschlag-Weitergabe** nicht aktiviert.

Abbildung 4-14. Sitzungsoptionen – Register „Allgemein“



In der Liste **Tastaturanschlag-Menüaktivierung** können Sie einen Tastenanschlag auswählen, durch den die Symbolleiste aktiviert wird.

Mit dem Kontrollkästchen Aktualisierung im Hintergrund **können Sie festlegen, ob Aktualisierungen im Hintergrund vorgenommen werden sollen**. Wenn diese Option ausgewählt ist, wird ein konstanter Datenfluss vom Gerät zum **Viewer** gesendet, unabhängig davon, ob Änderungen auf dem Gerät vorgenommen wurden oder nicht.

So ändern Sie Sitzungsoptionen:

1. Wählen Sie im Menü **Extras** im **Viewer** den Befehl **Sitzungsoptionen**. Die Symbolleiste „Sitzungsoptionen“ wird angezeigt.
2. Klicken Sie auf das Register **Allgemein**.
3. Ändern Sie die Sitzungsoptionen wie gewünscht.
4. Klicken Sie auf **OK**.

Bildschirmaufzeichnung

Mit dem **Viewer** können Sie den Inhalt des Bildschirms aufzeichnen und in einer Datei speichern oder in die Zwischenablage kopieren.

So speichern Sie den Bildschirminhalt als Datei:

1. Wählen Sie im **Viewer** die Befehle **Datei – In Datei speichern**. Das Dialogfeld **Speichern** wird angezeigt.
2. Suchen Sie in der Verzeichnisstruktur nach dem gewünschten Speicherort für die Datei.
3. Geben Sie im Feld **Dateiname** einen Dateinamen ein und klicken Sie auf **Speichern**.

So kopieren Sie den Bildschirminhalt in die Zwischenablage:

Wählen Sie im **Viewer** die Befehle **Datei – In Zwischenablage speichern**. Die Bildschirmdarstellung wird in der Zwischenablage gespeichert und kann in ein Dokument oder eine Bildbearbeitungsanwendung eingefügt werden.

HINWEIS: Die Funktion „In Zwischenablage speichern" ist unter Linux nicht verfügbar.

Trennung

Durch Trennen (oder exklusives Starten) von Sitzungen können Benutzer mit den entsprechenden Zugriffsberechtigungen die Steuerung eines Servers von einem anderen Benutzer mit weniger oder gleichen Berechtigungen übernehmen.

HINWEIS: Eine Warnmeldung wird an alle Benutzer gesendet, die an der Verbindung teilnehmen, aber nur der Primärbenutzer kann eine Trennanforderung zurückweisen (falls zugelassen).

In Tabelle 4-2 werden die Trennungsszenarien sowie detaillierte Angaben zur möglichen Zurückweisung von Trennanforderungen aufgelistet. Informationen über das Trennen von Virtual Media-Sitzungen sowie reservierte und gesperrte Virtual Media-Sitzungen finden Sie unter „Virtual Media" auf Seite 93.

Tabelle 4-2. Trennungsszenarien

Aktueller Benutzer	Trennung durch	Trennung kann zurückgewiesen werden
Remote-Benutzer	Lokaler Benutzer	Nein
Remote-Benutzer	Remote-Administrator	Nein
Remote-Benutzer	Remote Console Switch-Administrator	Nein

Tabelle 4-2. Trennungsszenarien (Fortsetzung)

Aktueller Benutzer	Trennung durch	Trennung kann zurückgewiesen werden
Remote Console Switch-Administrator	Lokaler Benutzer	Ja
Remote Console Switch-Administrator	Remote Console Switch-Administrator	Ja
Remote-Administrator	Lokaler Benutzer	Nein
Remote-Administrator	Remote-Administrator	Ja
Remote-Administrator	Remote Console Switch-Administrator	Nein
Lokaler Benutzer	Remote-Administrator	Ja
Lokaler Benutzer	Remote Console Switch-Administrator	Ja

Trennen einer Remote-Benutzer-Verbindung durch einen Remote-Administrator

Wenn ein Remote-Administrator versucht, auf einen Server zuzugreifen, der von einem Remote-Benutzer verwendet wird, wird der Administrator in einer Nachricht gebeten, so lange zu warten, bis der Benutzer über die Trennung seiner Sitzung informiert wurde. Der Remote-Benutzer kann die Trennanforderung nicht zurückweisen und die Sitzung wird getrennt. Die gewährte Zeitdauer vor Trennung der Sitzung wird in den Einstellungen Timeout der exklusiven Videositzung im Dialogfeld für die Sitzungen festgelegt. Weitere Informationen finden Sie im Abschnitt „Anzeigen und Konfigurieren der Remote Console Switch-Parameter“ auf Seite 106.

HINWEIS: Wenn der angezeigte Server an einen Avocent Switch angeschlossen ist, wird keine Zeitdauer angezeigt.

Trennung der Verbindung eines lokalen Benutzers/Remote-Administrators durch einen Remote-Administrator

Wenn ein Administrator versucht, auf einen Server zuzugreifen, der von einem lokalen Benutzer oder einem anderen Remote-Administrator mit gleichen Berechtigungen verwendet wird, kann der aktuelle Benutzer die Trennanforderung annehmen oder ablehnen. Der verbundene lokale Benutzer oder Remote-Administrator wird in einer Nachricht gefragt, ob er die Trennanforderung annehmen möchte. Wird die Trennanforderung zurückgewiesen, wird der Remote-Administrator mit einer Meldung informiert, dass seine Anfrage zurückgewiesen wurde und kein Zugriff auf den Server möglich ist.

HINWEIS: Falls der angezeigte Server an einen Avocent Switch angeschlossen ist, hat der Benutzer keine Möglichkeit, die Unterbrechung anzunehmen oder abzulehnen.

HINWEIS: Falls eine Trennanforderung zurückgewiesen werden kann, wird das Dialogfeld „Trennanforderung für die Sitzung" angezeigt. In diesem Dialogfeld können Sie die Trennanforderung akzeptieren, indem Sie auf die Schaltfläche „Akzeptieren" klicken, oder zurückweisen, indem Sie auf die Schaltfläche „Nicht akzeptieren" klicken oder das Dialogfeld schließen.

Teilen der Verbindung

Das Teilen der Verbindung ermöglicht mehreren Benutzern die gleichzeitige Interaktion mit einem Zielgerät. Als Primärbenutzer werden Sie u. U. über ein Dialogfeld benachrichtigt, dass ein anderer Benutzer Ihre Verbindung teilen möchte. Sie können **Ja** wählen, um das Teilen der Verbindung zu akzeptieren, **Nein**, um die Anfrage zurückzuweisen, oder Sie klicken auf das Feld **Passiv-Teilen**, um dem neuen Benutzer das Teilen der Verbindung zu gestatten, ohne ihm jedoch Steuerungsmöglichkeiten einzuräumen.

Wenn Sie versuchen, eine Videositzung mit einem Gerät zu öffnen, das bereits von einem anderen Benutzer angezeigt wird, werden Sie benachrichtigt, dass das Gerät bereits angezeigt wird. Je nach Konfiguration der Teilungseinstellungen wird Ihnen gegebenenfalls die Option angeboten, die Videositzung zu teilen oder zu trennen. Eventuell erhalten Sie auch die Möglichkeit, eine Videositzung im Tarnmodus zu öffnen.

HINWEIS: Getarnte Videositzungen sind passive Videositzungen, bei denen der Primärbenutzer nicht weiß, dass ein Sekundärbenutzer existiert. Die Möglichkeit, eine Videositzung im Tarnmodus zu öffnen, ist abhängig von den Benutzerberechtigungen. Wenn ein Benutzer die Berechtigung zum Trennen der Verbindung eines anderen Benutzers hat, kann er auch eine getarnte Videositzung öffnen.

Der Zugriff auf das Gerät ist abhängig vom Typ der Verbindung zwischen dem aktuellen Benutzer und dem Gerät. Es gibt zwei Arten von Benutzern in Videositzungen: einen Primärbenutzer und bis zu elf simultane Sekundärbenutzer (eine 2161DS-2- oder 4161DS-Einheit unterstützt bis zu zwölf simultane Sitzungen über alle angeschlossenen Server verteilt). Nur der Primärbenutzer kann Trennanforderungen für alle Benutzer, die eine Verbindung teilen, annehmen oder zurückweisen. Der Primärbenutzer verfügt außerdem über die Steuerungsmöglichkeiten für Videoparameter und Bildschirmauflösung der Videositzung.

Sekundärbenutzer können entweder „aktive Benutzer" sein, d. h., sie können Maus- und Tastaturdaten eingeben, oder „passive Benutzer", die keine Maus- und Tastaturdaten eingeben können.

Wenn die Option **Automatisches Teilen** am Remote Console Switch aktiviert ist, benötigen Sekundärbenutzer nicht die Erlaubnis des Primärbenutzers, um an einer Sitzung teilzunehmen.

Wenn der Primärbenutzer die Sitzung verlässt, wird der Sekundärbenutzer mit aktiven Benutzerrechten, dessen Verbindung am längsten besteht, zum Primärbenutzer. Wenn der Primärbenutzer die Sitzung verlässt und keine Sekundärbenutzer mit aktiven Benutzerrechten an der Sitzung teilnehmen, wird die Sitzung geschlossen.

Weitere Informationen zur Konfiguration der Verbindungsteilung finden Sie unter „Anzeigen und Konfigurieren der Remote Console Switch-Parameter" auf Seite 106.

Exklusivmodus

Der **Exklusivmodus** ermöglicht Ihnen die exklusive Steuerung einer Videositzung. Wenn Sie sich im **Exklusivmodus** befinden, kann kein anderer Benutzer an der Sitzung teilnehmen (es sei denn, er befindet sich im **Tarnmodus**). Wenn bereits andere Benutzer an der Sitzung teilnehmen, wenn Sie den **Exklusivmodus** auswählen, werden Sie darauf aufmerksam gemacht, dass die anderen Benutzer durch Auswahl des **Exklusivmodus** von der Sitzung getrennt werden.

HINWEIS: Nur der Primärbenutzer kann eine Exklusivsitzung anfordern. Nehmen weitere Benutzer an der Sitzung teil, wenn der Exklusivmodus angefordert wird, werden sie unabhängig von der Zugriffsebene des Primärbenutzers getrennt.

So öffnen Sie eine Videositzung im **Exklusivmodus**:

Wählen Sie im **Viewer** die Befehle **Extras – Exklusivmodus**.

5

Virtual Media

Virtual Media ermöglicht das Anzeigen von auf virtuellen Speichergeräten gespeicherten Daten auf einem beliebigen Server. Außerdem können die Daten von den Speichergeräten auf den Server verschoben oder kopiert werden und umgekehrt. Remote-Systeme lassen sich effizienter verwalten, indem die Installation und Wiederherstellung von Betriebssystemen, die Wiederherstellung oder Duplizierung von Festplatten sowie BIOS-Aktualisierungen und Server-Backups über Remote-Zugriff ermöglicht werden. Virtual Media-Geräte können direkt über die USB-Ports an die Einheit angeschlossen werden. Auch der Remote-Zugriff auf Virtual Media ist möglich. Nutzen Sie die Virtual Media-Unterstützung, um USB-Speichergeräte an die Einheit anzuschließen und diese Geräte für verbundene Einheiten verfügbar zu machen.

Jeder Benutzer, der an einer KVM-Sitzung teilnimmt, kann auf alle Speichergeräte zugreifen, die diesem Zielgerät zugeordnet sind. Um dem Sicherheitsrisiko nicht autorisierter Benutzerzugriffe vorzubeugen, können Sie eine Virtual Media-Sitzung für eine KVM-Sitzung reservieren.

Um das Speichermedium in einem Virtual Media-Gerät zu wechseln, müssen Sie zunächst die Zuordnung des Virtual Media-Geräts aufheben. Dann können Sie das neue Speichermedium einlegen und das Virtual Media-Gerät erneut zuordnen. Das Speichergerät ist dann in der neuen Virtual Media-Sitzung verfügbar.

HINWEIS: Um Virtual Media auf einem gegebenen Server zu nutzen, muss ein USB2-SIP oder ein Avocent PS2M- oder USB2IQ-Modul für die Verbindung zwischen diesem Server und der KVM-Switch verwendet werden.

HINWEIS: Eine Virtual Media-Sitzung kann nicht mit einem Server aufgebaut werden, der an ein PEM angeschlossen ist.

Dieses Kapitel beschreibt, wie Sie Virtual Media von der OSCAR-Benutzeroberfläche und der integrierten Weboberfläche konfigurieren und aufrufen. Virtual Media ist auch in der Remote Console Switch-Software verfügbar. Anweisungen zur Verwendung der Remote Console Switch-Software finden Sie in der Bedienungsanleitung des Dell Remote Console Switchs oder in der in die Software integrierten Hilfe.

Gängige Begriffe im Zusammenhang mit Virtual Media

- Virtual Media: Ein USB-Speichergerät, das an die Einheit angeschlossen und allen Zielgeräten zur Verfügung gestellt werden kann, die mit der Einheit verbunden sind.
- Virtual Media-Sitzung: Zwei USB-Verbindungen über ein einziges Kabel; diese Verbindungen werden vom Rechner als ein USB-CD-Laufwerk, USB-DVD-Laufwerk oder ein USB-Massenspeichergerät erkannt.
- Lokale Virtual Media-Sitzung: Virtual Media-Sitzung, bei der Geräte verwendet werden, die direkt an den USB-Port einer Einheit angeschlossen sind.
- Virtual Media-Remote-Sitzung: Virtual Media-Sitzung, bei der Geräte verwendet werden, die direkt an den Client-Computer angeschlossen sind.
- Gesperrt: Eine Virtual Media-Sitzung, die für eine bestimmte KVM-Sitzung reserviert ist. Wenn die KVM-Sitzung beendet wird, endet auch die Virtual Media-Sitzung. (Falls die KVM-Sitzung beispielsweise unterbrochen, von einem Benutzer beendet oder angehalten wird, weil sich der Bildschirmschoner einschaltet, beendet die Einheit die zugehörige Virtual Media-Sitzung.) Bei Beenden einer gesperrten Virtual Media-Sitzung wird die entsprechende KVM-Sitzung allerdings nicht beendet.
- Reserviert: Eine Virtual Media-Sitzung, auf die nur durch einen bestimmten Benutzernamen oder einen Administrator zugegriffen werden kann; sie kann auch nur über diesen Zugriff beendet werden. Wenn sowohl „Gesperrt“ als auch „Reserviert“ ausgewählt werden, ist die Sitzung reserviert.

Konfigurieren von Virtual Media per Lokalzugriff

Der Administrator am lokalen Port (d. h. alle Benutzer, die Zugriff auf den lokalen Benutzer-Port haben) ist in der Lage, Virtual Media auf allen Servern, die an ein USB2-SIP angeschlossen sind, zu aktivieren und zu deaktivieren. Diese Einstellung bleibt in der Einheit nach dem Aus- und Einschalten erhalten.

Aktivieren/Deaktivieren von Virtual Media mithilfe der OSCAR-Benutzeroberfläche

Lokale Administratoren können Virtual Media auf allen Servern über das jeweils zugehörige SIP aktivieren und deaktivieren. Diese Einstellung bleibt in der Einheit auch nach dem Aus- und Einschalten erhalten.

Im Dialogfeld VMedia Setup wird der Name der einzelnen Virtual Media-SIPs in Verbindung mit einem Kontrollkästchen angezeigt, das festlegt, ob Virtual Media für das jeweilige SIP aktiviert oder deaktiviert ist. Wenn zu diesem Zeitpunkt eine Virtual Media-Sitzung aktiv ist, wird der Buchstabe des Benutzers in blau rechts neben dem Kontrollkästchen angezeigt.

HINWEIS: Der lokale Benutzer muss zunächst alle aktiven Virtual Media-Sitzungen über den Bildschirm „Befehle – Benutzerstatus“ trennen, um Virtual Media auf einem Server deaktivieren zu können.

Abbildung 5-1. Dialogfeld „VMedia Setup“

So aktivieren/deaktivieren Sie Virtual Media:

1. Betätigen Sie die Taste <Druck>, um die OSCAR-Benutzeroberfläche aufzurufen. Das Hauptmenü wird angezeigt.
2. Klicken Sie auf Setup – VMedia.

3 Markieren Sie das entsprechende Kontrollkästchen, um Virtual Media für das jeweilige SIP zu aktivieren.
– oder –
Heben Sie die Markierung des entsprechenden Kontrollkästchens auf, um Virtual Media für dieses SIP zu deaktivieren.

4 Klicken Sie auf **OK**, um die ausgewählten Optionen zu übernehmen und zum Dialogfeld **Setup** zurückzukehren.

Einrichten von Virtual Media-Optionen mithilfe der OSCAR-Benutzeroberfläche

Mithilfe der Optionen im Dialogfeld **Virtual Media** können Sie das Verhalten der Einheit während einer Virtual Media-Sitzung festlegen. In Tabelle 5-1 werden die Optionen beschrieben, die für Virtual Media-Sitzungen eingerichtet werden können.

Abbildung 5-2. Dialogfeld „Virtual Media“

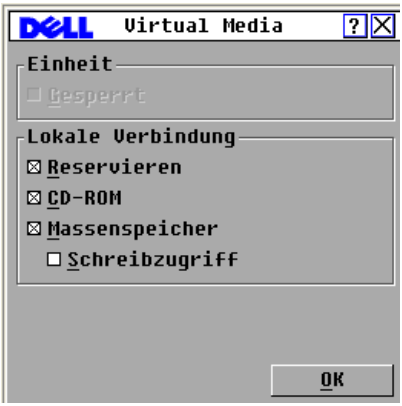


Tabelle 5-1. Virtual Media-Optionen – OSCAR-Benutzeroberfläche

Funktion	Zweck
Gesperrt	Synchronisiert die KVM- und Virtual Media-Sitzungen: Wenn ein Benutzer eine KVM-Verbindung trennt, wird dadurch auch die Virtual Media-Verbindung zu diesem Server getrennt. Auch die Verbindung eines lokalen Benutzers, der versucht, zu einem anderen Server zu wechseln, wird getrennt.

Tabelle 5-1. Virtual Media-Optionen – OSCAR-Benutzeroberfläche (Fortsetzung)

Funktion	Zweck
Reservieren	Gewährleistet, dass der Zugriff auf eine Virtual Media-Verbindung nur mit Ihrem Benutzernamen möglich ist und kein anderer Benutzer eine KVM-Verbindung zu diesem Server herstellen kann. Wenn die zugehörige KVM-Sitzung getrennt wird, wird die Virtual Media-Sitzung je nachdem, ob die Einstellung „Gesperrt“ im Dialogfeld „Virtual Media“ aktiviert ist oder nicht, ebenfalls getrennt.
CD-ROM	Ermöglicht Virtual Media-Sitzungen mit dem ersten erkannten CD-ROM-Laufwerk. Aktivieren Sie dieses Kontrollkästchen, um eine Virtual Media-Verbindung zwischen einem CD-ROM-Laufwerk und einem Server herzustellen. Deaktivieren Sie das Kontrollkästchen, um eine Virtual Media-Verbindung zwischen einem CD-ROM-Laufwerk und einem Server zu beenden.
DVD-ROM	Ermöglicht Virtual Media-Sitzungen mit dem ersten erkannten DVD-ROM-Laufwerk. Aktivieren Sie dieses Kontrollkästchen, um eine VM-Verbindung zwischen einem DVD-ROM-Laufwerk und einem Server herzustellen. Deaktivieren Sie das Kontrollkästchen, um die VM-Verbindung zwischen einem DVD-ROM-Laufwerk und einem Server zu beenden. Es werden nur DVD-ROM-Daten von Virtual Media unterstützt. Das Abspielen von DVD-Filmen wird über Virtual Media nicht unterstützt.
Massenspeicher	Ermöglicht Virtual Media-Sitzungen mit dem ersten erkannten Massenspeicherlaufwerk. Aktivieren Sie dieses Kontrollkästchen, um eine Virtual Media-Verbindung zwischen einem Massenspeichergerät und einem Server herzustellen. Deaktivieren Sie das Kontrollkästchen, um eine Virtual Media-Verbindung zwischen einem Massenspeichergerät und einem Server zu beenden.
Schreibzugriff	Ermöglicht es einem Zielserver, während einer Virtual Media-Sitzung Daten auf das Virtual Media-Gerät zu schreiben. Der Lesezugriff ist während einer VM-Sitzung immer zulässig.

So richten Sie Virtual Media-Optionen über die OSCAR-Benutzeroberfläche ein:

1. Betätigen Sie die Taste <Druck>, um die OSCAR-Benutzeroberfläche aufzurufen. Das **Hauptmenü** wird angezeigt.
2. Schließen Sie ein Virtual Media-Gerät am USB-Port des Switches an.
3. Klicken Sie auf **VMedia**.

4 Klicken Sie auf das jeweilige Kontrollkästchen, um die einzelnen Optionen zu aktivieren bzw. deaktivieren. Informationen zu den einzelnen Einstellungen finden Sie in Tabelle 5-1.

5 Klicken Sie auf OK, um die ausgewählten Optionen zu übernehmen und zum Hauptmenü zurückzukehren.

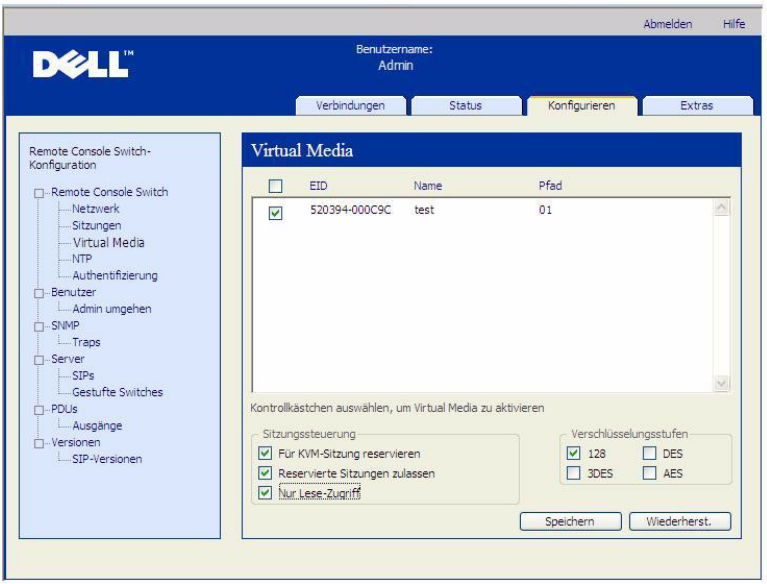
Konfigurieren von Virtual Media per Remote-Zugriff

Virtual Media kann auch über die integrierte Weboberfläche konfiguriert werden. Die integrierte Weboberfläche bietet Optionen, die mit denen der OSCAR-Benutzeroberfläche vergleichbar sind. Benutzer können Virtual Media auf allen Servern über das jeweils zugehörige SIP aktivieren und deaktivieren. Diese Einstellung bleibt in der Einheit auch nach dem Aus- und Einschalten erhalten.

Aktivieren/Deaktivieren von Virtual Media mithilfe der integrierten Weboberfläche

Auf dem Virtual Media-Konfigurationsbildschirm der integrierten Weboberfläche werden die EID, der Name und der Verbindungspfad für die einzelnen Virtual Media-SIPs in Verbindung mit einem Kontrollkästchen angezeigt, das festlegt, ob Virtual Media für das jeweilige SIP aktiviert oder deaktiviert ist.

Abbildung 5-3. Fenster „Virtual Media“ – Integrierte Weboberfläche



So aktivieren/deaktivieren Sie Virtual Media:

1. Klicken Sie auf das Register **Konfigurieren** und dann auf **Remote Console Switch – Virtual Media**.
2. Markieren Sie das entsprechende Kontrollkästchen, um Virtual Media für das jeweilige SIP zu aktivieren.
   – oder –
   Heben Sie die Markierung des entsprechenden Kontrollkästchens auf, um Virtual Media für dieses SIP zu deaktivieren.
3. Klicken Sie auf **Speichern**.

Einrichten von Virtual Media-Optionen über die integrierte Weboberfläche

Mithilfe der Optionen im Virtual Media-Konfigurationsbildschirm der integrierten Weboberfläche können Sie das Verhalten der Einheit während einer Virtual Media-Sitzung festlegen. In Tabelle 5-2 werden die Optionen beschrieben, die für Virtual Media-Sitzungen eingerichtet werden können.

Tabelle 5-2. Virtual Media-Optionen – Integrierte Weboberfläche

Funktion	Zweck
Für KVM-Sitzung reservieren	Synchronisiert die KVM- und Virtual Media-Sitzungen: Wenn ein Benutzer eine KVM-Verbindung trennt, wird dadurch auch die Virtual Media-Verbindung zu diesem Server getrennt. Auch die Verbindung eines lokalen Benutzers, der versucht, zu einem anderen Server zu wechseln, wird getrennt.
Reservierte Sitzungen zulassen	Gewährleistet, dass der Zugriff auf eine Virtual Media-Verbindung nur mit Ihrem Benutzernamen möglich ist und kein anderer Benutzer eine KVM-Verbindung zu diesem Server herstellen kann.
Nur Lese-Zugriff	Verhindert, dass ein Zielserver während der Virtual Media-Sitzung Daten auf das Virtual Media-Laufwerk schreiben kann.
Verschlüsselungs-stufen	Ermöglicht es dem Benutzer auszuwählen, welche der SSL-Verschlüsselungsstufen (128-Bit, DES, 3DES oder AES) von der Virtual Media-Sitzung unterstützt werden sollen.

So richten Sie Virtual Media-Optionen über die integrierte Weboberfläche ein:

1. Klicken Sie auf das Register Konfigurieren und dann auf Remote Console Switch – Virtual Media.
2. Klicken Sie auf das jeweilige Kontrollkästchen, um die einzelnen Optionen zu aktivieren bzw. deaktivieren. Informationen zu den einzelnen Einstellungen finden Sie in Tabelle 5-2.
3. Klicken Sie auf Speichern.

Starten von Virtual Media

Virtual Media wird mithilfe des Viewers remote über die Einheit aufgerufen. Mit dem Virtual Media Client kann der Benutzer dem virtuellen Laufwerk auf dem Zielserver ein lokales Laufwerk zuordnen.

So starten Sie Virtual Media:

1. Starten Sie den Viewer über die integrierte Weboberfläche. (Weitere Informationen finden Sie unter „Verwenden des Viewers“ auf Seite 67.)
2. Wählen Sie **Extras – Virtual Media** aus.

Abbildung 5-4. Dell Virtual Media Client – Keine Verbindung angezeigt

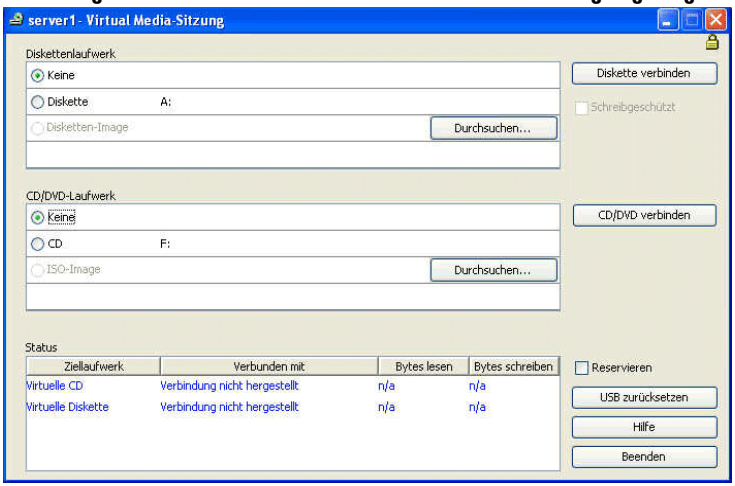
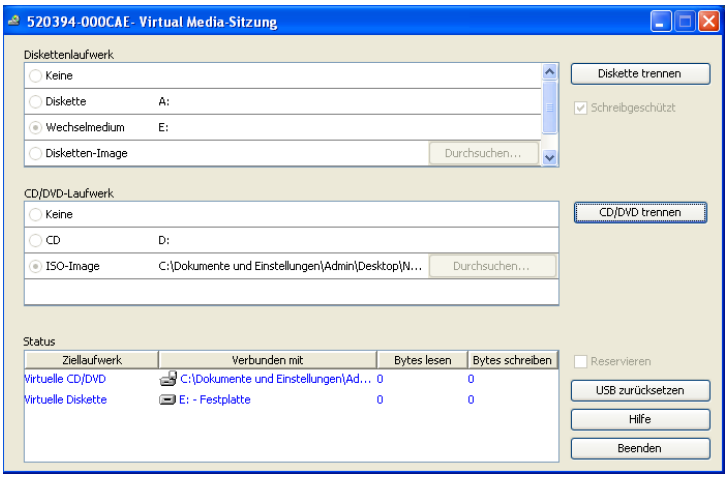


Abbildung 5-5. Dell Virtual Media Client – Zwei Verbindungen angezeigt



Für die Zuordnung auf dem Zielserver stehen zwei Geräte zur Verfügung: ein Disketten-/Flash-Laufwerk und ein CD/DVD-Laufwerk. Der Virtual Media Client ermöglicht die gleichzeitige Zuordnung von jeweils einem Laufwerk pro Option. Alternativ gestattet der Virtual Media Client ebenfalls die Zuordnung einer Disketten-Image-Datei (*.img) oder einer CD-Image-Datei (*.iso) zu einem virtuellen Gerät.

Die Virtual Media-Benutzeroberfläche ist in drei Hauptbereiche unterteilt: die Bereiche „Diskettenlaufwerk“, „CD/DVD-Laufwerk“ und „Status“. Wenn die Virtual Media-Sitzung für eine KVM-Sitzung reserviert ist, wird rechts oben auf dem Virtual Media Client-Bildschirm ein Vorhängeschloss angezeigt.

Virtuelles Diskettenlaufwerk

Im Bereich „Diskettenlaufwerk“ kann ein Benutzer auswählen, welches Laufwerk dem virtuellen Diskettenlaufwerk zugeordnet werden soll. Es stehen Optionsfelder zur Auswahl des Gerätetyps (Diskette, Wechselmedium oder Disketten-Image) sowie eine Schaltfläche „Durchsuchen“ zur Auswahl der *.img-Image-Datei zur Verfügung. Es kann immer nur ein Gerät im Bereich „Diskettenlaufwerk“ ausgewählt werden.

Durch Aktivieren des Kontrollkästchens „Schreibgeschützt“ hat der Benutzer die Möglichkeit zu verhindern, dass der Zielserver Daten auf das lokale Laufwerk schreiben kann. Wenn der Administrator alle Geräte mit Schreibschutz konfiguriert hat, ist dieses Kontrollkästchen aktiviert und nicht verfügbar.

So verbinden Sie eine Diskette mit dem Virtual Media-Laufwerk:

1. Wählen Sie entweder **Diskette** oder **Wechselmedium** aus.
2. (Optional) Aktivieren Sie **Schreibgeschützt**.
3. Klicken Sie auf **Diskette verbinden**.

So verbinden Sie ein Disketten-Image mit dem Virtual Media-Laufwerk:

1. Wählen Sie **Disketten-Image** aus.
2. Klicken Sie auf **Durchsuchen** und wählen Sie die gewünschte *.img-Image-Datei aus.

HINWEIS: Image-Dateien sind immer schreibgeschützt.

3. Klicken Sie auf **Diskette verbinden**.

So trennen Sie ein Speichermedium oder eine Image-Datei vom Virtual Media-Gerät:

Klicken Sie auf **Diskette trennen**.

Virtuelles CD/DVD-Laufwerk

Im Bereich „CD/DVD-Laufwerk“ kann ein Benutzer auswählen, welches Laufwerk dem virtuellen CD/DVD-Laufwerk zugeordnet werden soll. Es stehen Optionsfelder zur Auswahl des Gerätetyps (CD/DVD oder ISO-Image) sowie eine Schaltfläche „Durchsuchen“ zur Auswahl der *.iso-Image-Datei zur Verfügung. Es kann immer nur ein Gerät im Bereich „CD/DVD-Laufwerk“ ausgewählt werden.

So verbinden Sie ein CD/DVD-Speichermedium mit dem Virtual Media-Laufwerk:

1. Wählen Sie **CD** aus.
2. (Optional) Aktivieren Sie **Schreibgeschützt**.
3. Klicken Sie auf **CD/DVD verbinden**.

So verbinden Sie eine CD/DVD-Image-Datei mit dem Virtual Media-Laufwerk:

1. Wählen Sie **ISO-Image** aus.
2. Klicken Sie auf **Durchsuchen** und wählen Sie die gewünschte *.iso-Image-Datei aus.

HINWEIS: Image-Dateien sind immer schreibgeschützt.

3. Klicken Sie auf **CD/DVD verbinden**.

So trennen Sie ein Speichermedium oder eine Image-Datei vom Virtual Media-Gerät:

Klicken Sie auf **CD/DVD trennen**.

Virtual Media-Verbindungsstatus

Im Bereich „Status“ werden bestimmte Informationen über die Virtual Media-Verbindungen angezeigt. Wenn keine aktuelle Verbindung besteht, wird in den Spalten „Keine Verbindung“ bzw. „n/a“ angezeigt.

Wenn eine aktuelle Verbindung besteht, werden im Bereich „Status“ die folgenden Informationen angezeigt:

- Ziellaufwerk: das mit dem Zielserver verbundene virtuelle Gerät
- Verbunden mit: der Name des lokalen Laufwerks, das mit dem virtuellen Gerät verbunden ist
- Bytes lesen: die Anzahl der Bytes, die der Zielserver vom lokalen Gerät liest
- Bytes schreiben: die Anzahl der Bytes, die der Zielserver auf das lokale Gerät schreibt

Reservieren einer Virtual Media-Sitzung

Wenn Sie eine Virtual Media-Sitzung weiterführen möchten, nachdem die KVM-Sitzung beendet wurde, können Sie die Virtual Media-Sitzung reservieren. Wenn die Virtual Media-Sitzung reserviert wurde, bleibt sie aktiv, auch wenn die zugehörige KVM-Sitzung beendet wird. Außerdem kann nur der Benutzer, für den die Sitzung reserviert wurde, auf die Virtual Media-Sitzung zugreifen.

So reservieren Sie eine Virtual Media-Sitzung:

Aktivieren Sie das Kontrollkästchen **Reservieren**.

Zurücksetzen des USB-Busses

Mit dieser Funktion werden alle USB-Geräte auf dem Zielgerät einschließlich Tastatur und Maus zurückgesetzt. Sie sollte daher nur verwendet werden, wenn das Zielgerät nicht reagiert.

So setzen Sie den USB-Bus zurück:

Wählen Sie **USB zurücksetzen** aus.

6

Verwalten des Remote Console Switches mithilfe der integrierten Weboberfläche

Sobald Sie einen neuen Remote Console Switch installiert haben, können Sie über die integrierte Weboberfläche Einheitenparameter anzeigen und konfigurieren, Zugriffs- und Steuerungsrechte zuweisen, aktive Videositzungen anzeigen und steuern und zahlreiche Steuerungsfunktionen wie Neustart und Aktualisierung Ihres Remote Console Switches ausführen. Die integrierte Weboberfläche hat vier Register: Verbindungen, Konfigurieren, Status, und Extras.

Anweisungen zum Starten der integrierten Weboberfläche finden Sie unter „Starten der integrierten Weboberfläche“ auf Seite 34. Informationen über das Register „Verbindungen“ finden Sie unter „Zugriff auf Server über die integrierte Weboberfläche“ auf Seite 67.

HINWEIS: Die integrierte Weboberfläche wird von den 2161DS Remote Console Switches nicht unterstützt, weswegen diese Switchmodelle nicht migriert werden können. Verwenden Sie die Remote Console Software zur Verwaltung der 2161 Remote Console Switches. Informationen hierzu finden Sie in der Bedienungsanleitung der Dell Remote Console Switch-Software oder in der Softwarehilfe. Alle anderen Remote Console Switches unterstützen die integrierte Weboberfläche und können migriert werden. Weitere Informationen finden Sie unter „Migration von Remote Console Switches zur integrierten Weboberfläche“ auf Seite 142.

Migration von Switches von der Remote Console Switch Software

Wenn Sie bereits Remote Console Switches installiert haben, die die integrierte Weboberfläche unterstützen, können Sie die Switches von der Remote Console Switch Software auf die integrierte Weboberfläche migrieren. Zu diesem Zweck befolgen Sie die Anweisungen unter „Aktualisieren der Firmware“ auf Seite 125, „Migration von Remote Console Switches zur integrierten Weboberfläche“ auf Seite 142 und „Verwenden des Resynchronisations-Assistenten“ auf Seite 143.

WICHTIGER HINWEIS: Wenn die Migration eines Remote Console Switches durchgeführt wurde, werden die Switches nicht mehr über die Remote Console Switch Software-EVA verwaltet, sondern über die integrierte Weboberfläche. Sie können die Remote Console Switch Software dennoch weiterhin verwenden, um Servereigenschaften zu ändern, die lokale Datenbank zu verwalten, Ihr System zu organisieren und Verbindungen zu KVM-Sitzungen herzustellen. Weitere Informationen hierzu finden Sie in der Bedienungsanleitung der Dell Remote Console Switch-Software.

Anzeigen und Konfigurieren der Remote Console Switch-Parameter

Über das Register **Konfigurieren** kann eine Liste von Kategorien angezeigt werden, die zahlreiche Parameter für Ihren Remote Console Switch enthält. Wenn eine Kategorie in der Liste ausgewählt wird, werden die mit dieser Kategorie verbundenen Parameter aus der Einheit gelesen. Danach können Sie diese Parameter ändern und die Änderungen sicher an den Remote Console Switch zurücksenden.

Ändern der Remote Console Switch-Parameter

In der Kategorie **Remote Console Switch** können Sie den Produkttyp und die Seriennummer des Remote Console Switches anzeigen.

Wenn Sie die Unterkategorie **Netzwerk** auswählen, können Sie den Modus **IPv4** (Standard) oder den Modus **IPv6** auswählen. Sie können die folgenden Netzwerkeinstellungen ändern: **IP-Adresse**, **Subnetzmaske** (im IPv4-Modus) oder **Präfixlänge** (im IPv6-Modus) und **Gateway**. Darüber hinaus können Sie die **LAN-Geschwindigkeit** auswählen und bis zu drei IP-Adressen für DNS-Server angeben. Sie können auch auswählen, ob dem Remote Console Switch eine **statische** IP-Adresse (Standard) oder ggf. eine **dynamische** IP-Adresse zugewiesen wird.

HINWEIS: Nach Ändern der Netzwerkeinstellungen wird die Schaltfläche „Neustart erforderlich“ auf allen Seiten angezeigt um darauf hinzuweisen, dass der Switch neu gestartet werden muss, bevor die Änderungen in Kraft treten. Klicken Sie auf die Schaltfläche, um den Switch neu zu starten.

Die Unterkategorie **Sitzungen** dient der Steuerung von Videositzungen.

Durch Aktivieren der Option **Timeout für die Videositzung** können Sie festlegen, dass der Remote Console Switch eine inaktive Videositzung nach einer bestimmten Anzahl von Minuten schließt. Mit der Option **Timeout der exklusiven Videositzung** können Sie die Zeitdauer (5 - 120 Sekunden) bestimmen, während der eine Trennungswarnmeldung angezeigt wird, bevor eine Videositzung getrennt wird. Weitere Informationen zum Trennen von Sitzungen finden Sie unter „Trennung“ auf Seite 88. Wird diese Option nicht aktiviert, werden Sitzungen ohne Warnung getrennt.

Mithilfe der Option **Verschlüsselungsstufen** können Sie die Verschlüsselungsart bestimmen, die für Video-, Tastatur- und Maussitzungen verwendet werden soll. Wenn eine neue Client-Verbindung angefordert wird, können Sie mehrere Methoden auswählen. Der Remote Console Switch verwendet die höchste aktivierte Verschlüsselungsstufe.

Die Optionen unter **Verbindung teilen** zeigen an, welche Teilungsoptionen aktiviert sind. Die Optionen **Teilungs-Modus aktivieren**, **Automatisches Teilen**, **Exklusive Verbindungen** und **Getarnte Verbindungen** sind alle markiert, wenn die jeweilige Option aktiviert ist. Die Optionen **Automatisches Teilen**, **Exklusive Verbindungen** und **Getarnte Verbindungen** sind nur verfügbar, wenn **Teilungs-Modus aktivieren** ausgewählt ist. Weitere Informationen finden Sie unter „Teilen der Verbindung“ auf Seite 90.

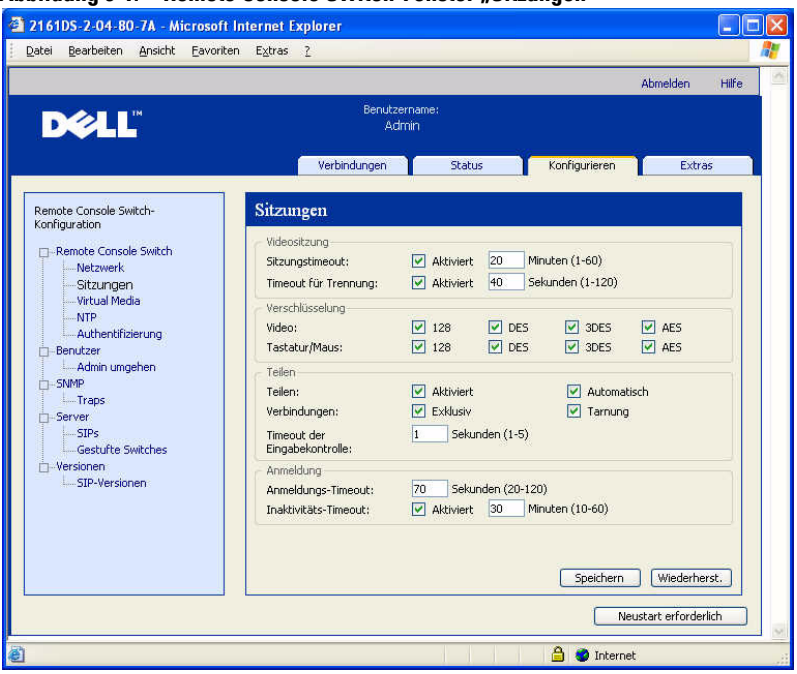
Die Option **Timeout der Eingabekontrolle** steuert die Zeitdauer, die zwischen Eingaben in einer aktiven Sitzung liegen darf, bevor eine andere Sitzung die Steuerung übernimmt. Es können Werte von 1 bis 5 Sekunden eingegeben werden. Die Option ist nur verfügbar, wenn der **Teilungs-Modus** aktiviert ist.

Mit der Option **Login Timeout** wird die zulässige Zeitdauer angegeben, während der ein LDAP-Server auf eine Anmeldungsanforderung reagieren muss. Die Standardzeit beträgt 30 Sekunden, aber manche WANs benötigen ggf. mehr Zeit.

Durch Aktivieren der Option **Inaktivitäts-Timeout** können Sie festlegen, wie lange eine inaktive Sitzung der integrierten Weboberfläche geöffnet bleiben soll. Wenn die festgelegte Zeitdauer abläuft, bevor der Benutzer zu einer anderen Webseite navigiert oder Änderungen vornimmt, wird die Sitzung geschlossen und das Anmeldungsfenster angezeigt.

HINWEIS: Änderungen an den Sitzungsparametern werden nicht auf bestehende Verbindungen angewendet, sondern treten erst bei zukünftigen Verbindungsanforderungen in Kraft.

Abbildung 6-1. Remote Console Switch-Fenster „Sitzungen“



Einrichten von Benutzerkonten

Wenn Sie die Kategorie **Benutzer** auswählen, ruft die integrierte Weboberfläche Benutzernamen und aktuelle Zugriffsebenen vom Remote Console Switch ab und zeigt diese Liste an. In dieser Liste können Sie Benutzer hinzufügen, ändern oder löschen. Sie können drei Zugriffsebenen vergeben: **Benutzer, Benutzeradministrator** und **Remote Console Switch-Administrator**. Mit den Zugriffsebenen **Benutzer** und **Remote Console Switch-Administrator** können Sie einem Benutzer individuelle Server-Zugriffsrechte zuweisen.

Tabelle 6-1. Zugriffsrechte für Benutzer

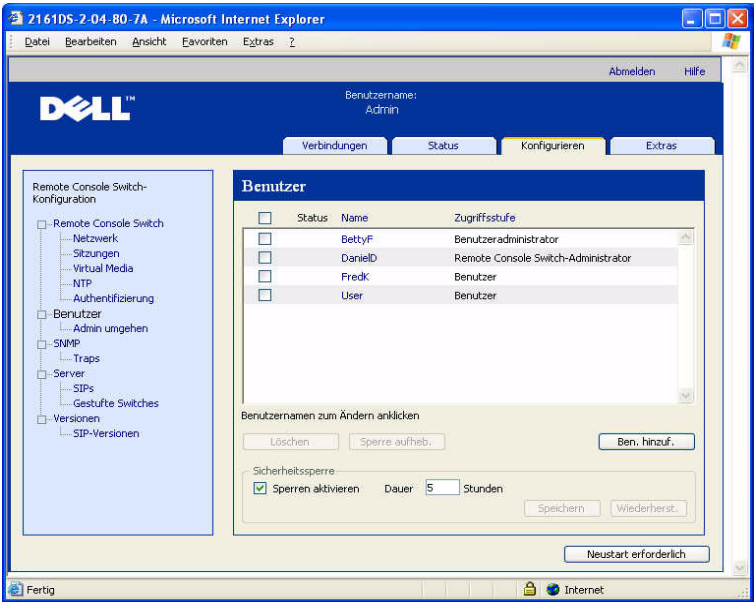
Betrieb	Remote Console Switch-Administrator	Benutzeradmi-nistrator	Benutzer
Trennen	Alle	Gleiche Ebene und niedriger	Nein
Netzwerk- und globale Einstellungen konfigurieren: Sicherheitsmodus, Timeout (Zeitlimit), Simple Network Management Protocol (SNMP)	Ja	Nein	Nein
Neustart	Ja	Nein	Nein
FLASH-Aktualisierung	Ja	Nein	Nein
Benutzerkonten verwalten	Ja	Ja	Nein
Serverstatus überwachen	Ja	Ja	Nein
Auf Zielgerät zugreifen	Ja	Ja	Von Administrator zugewiesen

HINWEIS: Die in Tabelle 6-1 aufgeführten Trennungsoptionen beziehen sich nur auf Remote-Clients und gelten nicht für Benutzer mit lokalem Serverzugriff.

Benutzer können durch die Sicherheitssperre gesperrt werden, wenn sie fünfmal hintereinander ein ungültiges Kennwort eingeben. Über die Kategorie „Benutzer“ können Einstellungen für die Sicherheitssperre konfiguriert sowie gesperrte Benutzer freigegeben werden.

HINWEIS: Ein Benutzeradministrator kann kein Remote Console Switch-Administratorkonto hinzufügen oder ändern.

Abbildung 6-2. Fenster „Benutzer“



So können Sie einen Benutzer hinzufügen oder ändern:

1. Klicken Sie auf das Register **Konfigurieren** der integrierten Weboberfläche und dann auf die Kategorie **Benutzer** in der linken Spalte.
2. Klicken Sie auf der rechten Seite des Fensters auf die Schaltfläche **Benutzer hinzufügen**, um einen neuen Benutzer hinzuzufügen.
   – oder –
   Klicken Sie in der Spalte „Benutzer“ auf einen Benutzernamen, um einen bestehenden Benutzer zu ändern.

   Das Fenster **Benutzer hinzufügen/ändern** wird angezeigt.

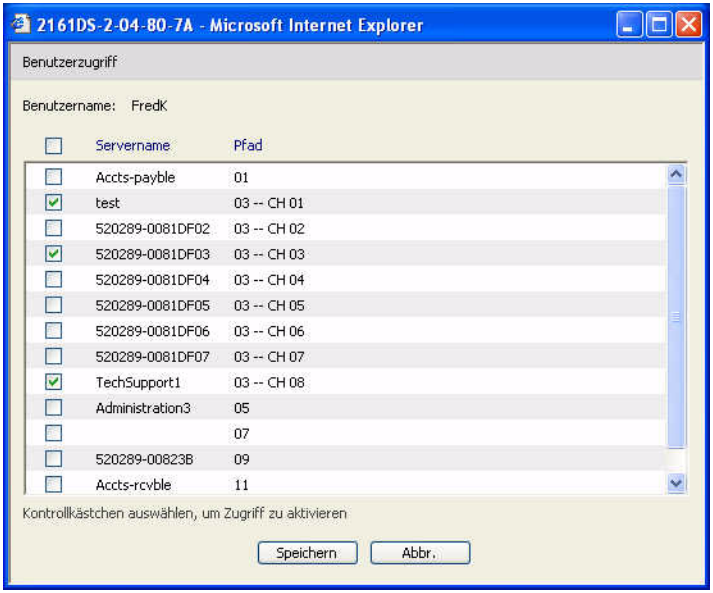
Abbildung 6-3. Fenster „Benutzer hinzufügen“

3 Geben Sie den Benutzernamen und das Kennwort ein, die dem Benutzer zugewiesen werden sollen, und bestätigen Sie das Kennwort durch die erneute Eingabe in das Feld **Kennwort bestätigen**. Das Kennwort muss zwischen 5 und 16 Zeichen lang sein und alphabetische Zeichen in Groß- und Kleinschreibung sowie mindestens eine Ziffer enthalten.

4 Wählen Sie in der Dropdown-Liste die gewünschte Zugriffsebene für diesen Benutzer aus. Wenn Sie die Option **Benutzer** auswählen, wird die Schaltfläche **Benutzer-Zugriffsrechte einrichten** verfügbar.

   a Klicken Sie auf die Schaltfläche **Benutzer-Zugriffsrechte einrichten**, um einzelne Server für diesen Benutzer auszuwählen. Das Fenster **Benutzer-Zugriffsrechte** wird angezeigt.

Abbildung 6-4. Fenster „Benutzer-Zugriffsrechte“



b Aktivieren Sie das Kontrollkästchen neben dem Servernamen, um dem Benutzer Zugriff auf diesen Server zu gewähren. Sie können auch das erste Kontrollkästchen markieren, um den Zugriff auf alle Server zu aktivieren.

c Deaktivieren Sie das Kontrollkästchen neben dem Servernamen, wenn der Benutzer keinen Zugriff auf diesen Server haben soll.

d Klicken Sie auf **Speichern**.

5 Klicken Sie auf **Speichern**, um die Einstellungen zu speichern und zum Hauptfenster der **integrierten Weboberfläche** zurückzukehren.

So ändern Sie das Benutzerkennwort:

1 Klicken Sie auf das Register **Konfigurieren** der integrierten Weboberfläche und dann auf die Kategorie **Benutzer** in der linken Spalte.

2 Klicken Sie in der Spalte „Benutzer“ auf einen Benutzernamen, um einen bestehenden Benutzer zu ändern. Das Fenster **Benutzer hinzufügen/ändern** wird angezeigt.

3 Geben Sie das Kennwort für diesen Benutzer in das Feld **Kennwort** ein und wiederholen Sie das Kennwort im Feld **Kennwort bestätigen**. Das Kennwort muss zwischen 5 und 16 Zeichen lang sein und alphabetische Zeichen in Groß- und Kleinschreibung sowie mindestens eine Ziffer enthalten.

4 Klicken Sie auf **Speichern**, um zur integrierten Weboberfläche zurückzukehren.

So löschen Sie einen Benutzer:

1 Klicken Sie auf das Register **Konfigurieren** der integrierten Weboberfläche und dann auf die Kategorie **Benutzer** in der linken Spalte.

2 Markieren Sie das Kontrollkästchen neben dem Benutzernamen, der gelöscht werden soll.

3 Klicken Sie auf die Schaltfläche **Löschen** auf der linken Seite des Fensters. Ein Bestätigungsfenster wird angezeigt.

4 Klicken Sie auf **Ja**, um den Löschvorgang zu bestätigen.
– oder –
Klicken Sie auf **Nein**, um das Fenster zu verlassen, ohne den Benutzer zu löschen.

Sperren und Freigeben von Benutzerkonten

Wenn ein Benutzer fünfmal hintereinander ein ungültiges Kennwort eingibt und die Sperrfunktion aktiviert ist, wird dieses Konto durch die **Sicherheitssperre** vorübergehend gesperrt. Wenn ein Benutzer erneut versucht sich anzumelden, wird eine entsprechende Fehlermeldung angezeigt.

HINWEIS: Diese Sperrfunktion betrifft alle Konten (Benutzer, Benutzeradministrator und Remote Console Switch-Administrator).

Die Anzahl der Stunden (1 bis 99), während denen die Konten gesperrt bleiben, kann vom Remote Console Switch-Administrator bestimmt werden. Wenn die Option **Sperren aktivieren** nicht aktiviert ist, ist die Sicherheits-Sperrfunktion deaktiviert und Benutzer werden nicht gesperrt.

Wenn ein Konto gesperrt wird, bleibt es so lange gesperrt, bis die festgelegte Zeit abgelaufen ist, der Remote Console Switch aus- und wieder eingeschaltet wurde oder ein Administrator die Sperre aufhebt. Ein Benutzeradministrator kann nur Benutzerkonten freigeben, während ein Remote Console Switch-Administrator alle Kontotypen freigeben kann.

So geben Sie ein Konto wieder frei:

1. Klicken Sie auf das Register **Konfigurieren** der integrierten Weboberfläche und dann auf die Kategorie **Benutzer** in der linken Spalte.
2. Markieren Sie das Kontrollkästchen neben dem Benutzernamen, dessen Sperre aufgehoben werden soll.
3. Klicken Sie auf die Schaltfläche **Sperre aufheben**. Das Sperrsymbol neben dem Benutzernamen wird ausgeblendet.

So legen Sie fest, wie lange ein Benutzerkonto gesperrt bleiben soll:

1. Klicken Sie auf das Register **Konfigurieren** der integrierten Weboberfläche und dann auf die Kategorie **Benutzer** in der linken Spalte.
2. Aktivieren Sie das Kontrollkästchen **Sperren aktivieren**.
3. Geben Sie ein, wie viele Stunden (1 bis 99) eine Benutzersperre bestehen bleiben soll.

HINWEIS: Nur Remote Console Switch-Administratoren können Sperrenparameter festlegen.

So deaktivieren Sie die Sicherheits-Sperrfunktion:

1. Klicken Sie auf das Register **Konfigurieren** der integrierten Weboberfläche und dann auf die Kategorie **Benutzer** in der linken Spalte.
2. Deaktivieren Sie das Kontrollkästchen **Sperren aktivieren**. Das Feld **Dauer** wird abgeblendet.

HINWEIS: Eine Deaktivierung der Sicherheits-Sperrfunktion hat keinerlei Auswirkungen auf Benutzer, die bereits gesperrt sind.

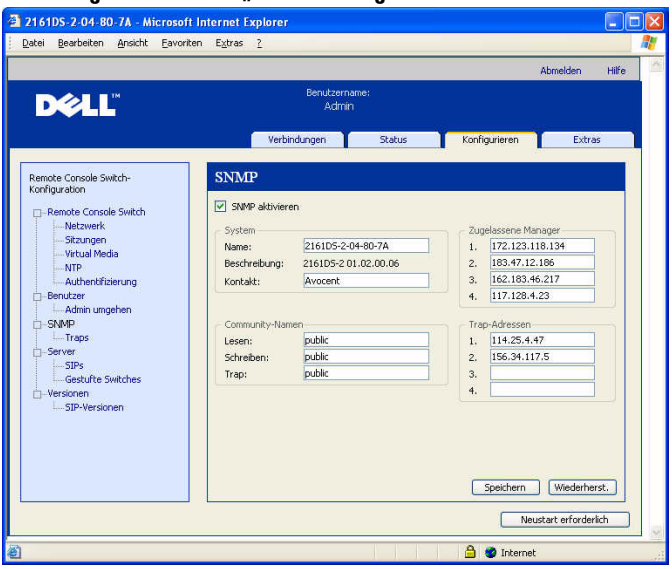
Aktivieren und Konfigurieren von SNMP

SNMP ist ein Protokoll, das verwendet wird, um Verwaltungsinformationen zwischen Netzwerk-Verwaltungsanwendungen und Remote Console Switches zu übertragen. Andere SNMP-Manager können mit Ihrem Remote Console Switch per Zugriff auf MIB-II und den öffentlichen Teil der Unternehmens-MIB kommunizieren. Wenn Sie die Kategorie **SNMP** auswählen, ruft die integrierte Weboberfläche die SNMP-Parameter von der Einheit ab.

In der Kategorie „SNMP“ können Sie die Systeminformationen und Community-Zeichenketten eingeben. Außerdem können Sie festlegen, welche Konsolen den Remote Console Switch verwalten und SNMP-Traps von dem Switch empfangen können. Weitere Informationen zu Traps finden Sie unter „Aktivieren von individuellen SNMP-Traps“ auf Seite 116 in diesem Kapitel. Wenn Sie **SNMP aktivieren** auswählen, antwortet die Einheit auf SNMP-Anforderungen über den UDP-Port 161.

HINWEIS: Die integrierte Weboberfläche verwendet zur Steuerung der Switches kein Standard-SNMP und daher auch nicht den UDP-Port 161. Die integrierte Weboberfläche verwendet zur Kommunikation mit Remote Console Switches ein sicheres, systemspezifisches Protokoll über einen anderen Netzwerk-Port.

Abbildung 6-5. Fenster „SNMP-Konfiguration“



So konfigurieren Sie allgemeine SNMP-Einstellungen:

1. Klicken Sie auf das Register **Konfigurieren** der integrierten Weboberfläche und dann auf die Kategorie **SNMP** in der linken Spalte.
2. Aktivieren Sie das Kontrollkästchen **SNMP aktivieren**, damit der Remote Console Switch auf SNMP-Anforderungen über den UDP-Port 161 reagieren kann.

3 Geben Sie den vollständigen Domänennamen des Systems in das Feld **Name** sowie einen Node-Kontakt in das Feld **System** ein.

4 Füllen Sie unter „Community-Namen“ die Felder **Lesen**, **Schreiben** und **Trap** aus. Damit werden die Community-Zeichenketten festgelegt, die für SNMP-Aktionen verwendet werden müssen. Die Zeichenketten für **Lesen** und **Schreiben** gelten nur für SNMP über UDP-Port 161 und fungieren als Kennwörter, die den Zugriff auf den Remote Console Switch schützen. Die Eingaben können eine maximale Länge von 64 Zeichen haben. Diese Felder dürfen nicht leer bleiben.

5 Geben Sie in den Feldern **Zugelassene Manager** die Adressen von bis zu vier Management-Workstations ein, die diesen Remote Console Switch verwalten dürfen. Sie können diese Felder auch leer lassen, so dass der Remote Console Switch von allen Konsolen verwaltet werden kann.

6 Sie können in den Feldern für **Trap-Adresse** die Adressen von bis zu vier Management-Workstations eingeben, an die dieser Remote Console Switch Traps senden soll.

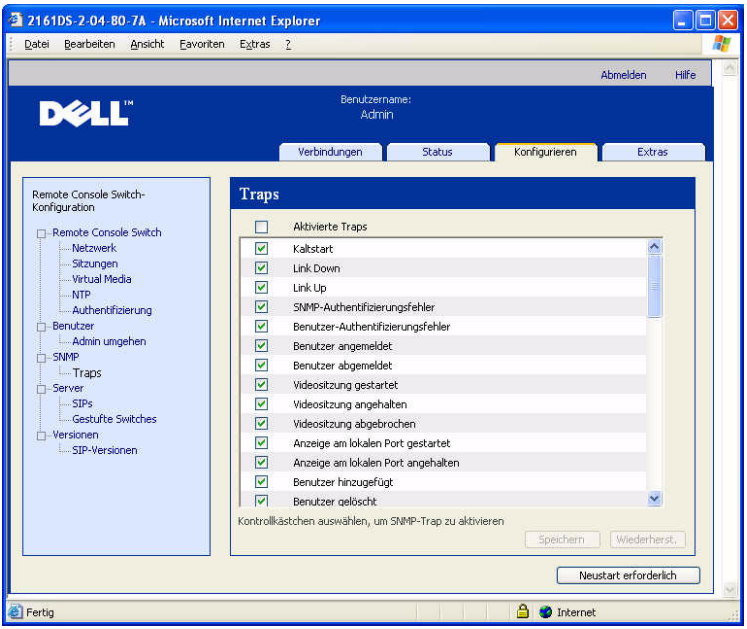
7 Klicken Sie auf **Speichern**, um die Einstellungen zu speichern und das Fenster zu schließen.
– oder –
Klicken Sie auf **Wiederherstellen**, um die Änderungen zu verwerfen und das Fenster zu verlassen. Die zuletzt gespeicherten Einstellungen werden wiederhergestellt.

HINWEIS: Nach Ändern der SNMP-Einstellungen wird die Schaltfläche „Neustart erforderlich“ auf allen Seiten angezeigt, um darauf hinzuweisen, dass der Switch neu gestartet werden muss, bevor die Änderungen in Kraft treten. Klicken Sie auf die Schaltfläche, um den Switch neu zu starten.

Aktivieren von individuellen SNMP-Traps

Ein SNMP-Trap ist eine Benachrichtigung, die vom Remote Console Switch an eine Managementkonsole gesendet wird, um darauf hinzuweisen, dass ein Ereignis im Remote Console Switch aufgetreten ist, das möglicherweise Aufmerksamkeit erfordert. Die Dell OpenManage™ IT Assistant Software ist der Ereignismanager. Sie können angeben, welche SNMP-Traps an die Managementkonsolen gesendet werden, indem Sie einfach die entsprechenden Kontrollkästchen in der Liste aktivieren. Sie können auch einfach das Kontrollkästchen neben „Aktivierte Traps“ aktivieren oder deaktivieren, um die gesamte Liste auszuwählen bzw. die gesamte Auswahl aufzuheben.

Abbildung 6-6. Fenster „SNMP-Traps“



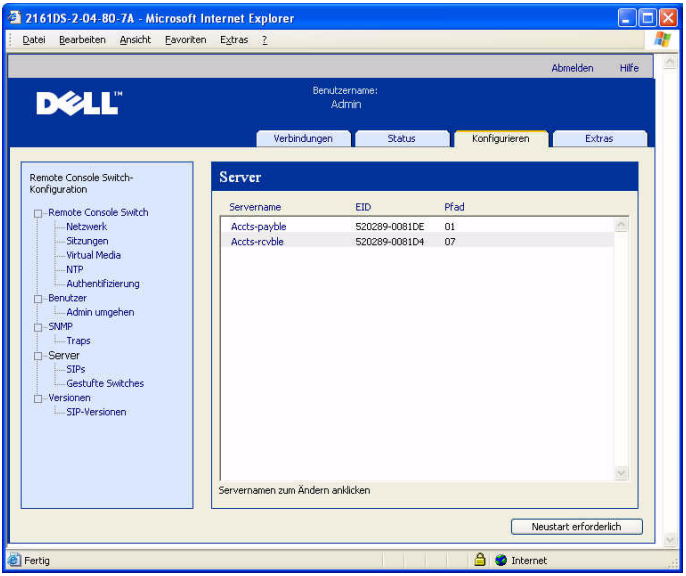
Anzeigen und Resynchronisieren von Serververbindungen

In der Kategorie **Server** werden die in der integrierten Weboberflächen-Datenbank vorhandenen Server sowie Informationen darüber, wie die Server mit dem ausgewählten Remote Console Switch verbunden sind, abgerufen und angezeigt.

Die Spalte „Pfad“ zeigt die aktuelle Serververbindung an. Es besteht entweder eine Verbindung mit einem SIP oder mit einem gestuften Switch. Wenn ein SIP angeschlossen ist, wird der ARI-Port des SIP angezeigt. Wenn ein gestufter Switch angeschlossen ist, wird auch der Switch-Kanal angezeigt. Durch Klicken auf einen Servernamen wird ein Dialogfeld aufgerufen, in dem Sie den Namen des Servers ändern können.

HINWEIS: Die Schaltfläche „Neustart erforderlich“ wird nur angezeigt, wenn ein Neustart erforderlich ist.

Abbildung 6-7. Fenster „Server“



Ändern eines Servernamens

Sie können die integrierte Weboberfläche verwenden, um einen Server von einer Remote-Workstation aus umzubenennen, anstatt den Vorgang über die OSCAR-Benutzeroberfläche des Remote Console Switches vorzunehmen.

So ändern Sie einen Gerätenamen:

1 Klicken Sie in der Kategorie **Server** auf den Namen des Servers, dessen Name geändert werden soll. Das Fenster **Servernamen ändern** wird angezeigt.

Abbildung 6-8. Fenster „Servernamen ändern“

2 Geben Sie den Namen ein, der dem Server zugewiesen werden soll. Namen müssen zwischen 1 und 15 Zeichen lang sein, alphabetische Zeichen beinhalten und dürfen keine Leerzeichen oder Sonderzeichen mit Ausnahme von Bindestrichen enthalten.

3 Klicken Sie auf **Speichern**. Der zugewiesene Name wird sowohl in der Datenbank des Remote Console Switches als auch in der lokalen Client-Datenbank aktualisiert.

Anzeigen und Konfigurieren von gestuften Switch-Verbindungen

Im Fenster „Gestufte Switches“ können Sie die gestuften Switches in Ihrem System anzeigen. Durch Klicken auf einen Switch-Namen wird ein Fenster aufgerufen, in dem Sie den Namen oder die Anzahl der Kanäle ändern können.

So konfigurieren Sie eine gestufte Switch-Verbindung:

1 Klicken Sie auf das Register **Konfigurieren** der integrierten Weboberfläche und dann auf die Unterkategorie **Gestufte Switches** in der linken Spalte.

2 Klicken Sie auf den Namen des Switches, der konfiguriert werden soll. Das Fenster „Gestuften Switch ändern“ wird geöffnet.

Abbildung 6-9. Fenster „Gestuften Switch ändern“

3 Geben Sie den neuen Namen für den Switch ein.

4 Geben Sie die Anzahl der Kanäle für den Switch ein (4 bis 24).

5 Wenn Sie die Konfiguration der Switches abgeschlossen haben, klicken Sie auf **Speichern**, um die neuen Einstellungen zu speichern.
– oder –
Klicken Sie auf **Abbrechen**, um das Dialogfeld zu verlassen, ohne die Änderungen zu speichern.

Anzeigen von SIPs und IQ-Modulen

In der Kategorie Server – SIPs können Sie die SIPs und IQ-Module in Ihrem System, ihre Port- und elektronische ID-Nummer (EID) sowie Typ und Verbindungsgerät anzeigen.

Zudem wird der SIP-Status angezeigt. Ein grünes Kreissymbol zeigt an, dass das SIP online ist. Ein gelbes Kreissymbol zeigt an, dass das SIP gerade aktualisiert wird und ein rotes X zeigt an, dass das SIP offline ist. Um Offline-SIPs zu löschen, klicken Sie auf die Schaltfläche Offline-SIPs löschen und nach entsprechender Aufforderung auf OK. Die Schaltfläche Offline-SIPs löschen steht nur Remote Console Switch-Administratoren zur Verfügung.

HINWEIS: Offline-SIPs oder IQ-Module, die an einen gestuften, analogen Console Switch angeschlossen sind, können nicht gelöscht werden.

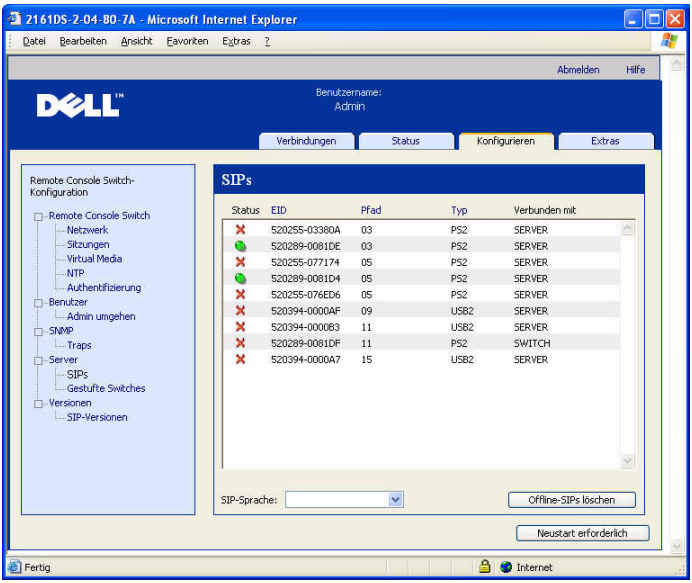
HINWEIS: Bei diesem Vorgang werden alle Offline-SIPs am Remote Console Switch gelöscht, einschließlich der SIPs von heruntergefahrenen Servern.

HINWEIS: Außerdem werden die Benutzerzugriffsrechte so aktualisiert, dass die Server der gelöschten Offline-SIPs entfernt werden.

Über das Dropdown-Menü SIP-Sprache können Sie die Sprach- und Tastaturparameter für alle Sun/USB-SIPs des gesamten Remote Console Switches bestimmen. Das Dropdown-Menü SIP-Sprache steht nur Remote Console Switch-Administratoren zur Verfügung.

HINWEIS: Die Schaltfläche „Neustart erforderlich“ wird nur angezeigt, wenn ein Neustart erforderlich ist.

Abbildung 6-10. Fenster „Server – SIPs“ – 4161DS Console Switch



HINWEIS: Der Remote Console Switch unterstützt sowohl IQ-Module als auch Dell SIPs. Dell SIPs sind für PS/2- und USB-Verbindungen verfügbar; mit den IQ-Modulen werden außerdem auch Sun- und serielle Verbindungen unterstützt.

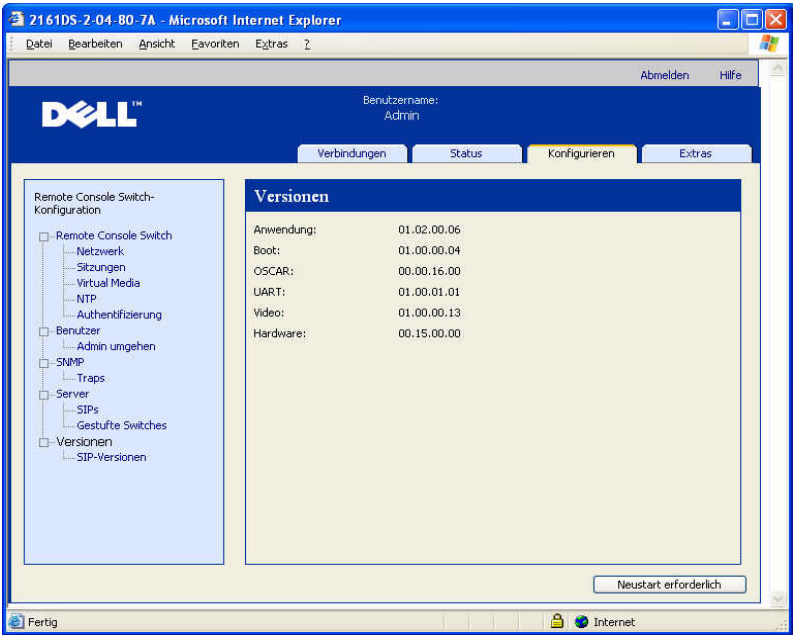
HINWEIS: Um festzustellen ob eine als PS/2 oder USB erkannte Einheit ein Dell SIP oder ein IQ-Modul ist, klicken Sie auf „Versionen – SIPs“. Weitere Informationen finden Sie unter „Unterkategorie SIPs“ auf Seite 122.

Anzeigen von Versionsinformationen für den Remote Console Switch

In der Kategorie **Versionen** werden die Versionen der Remote Console Switch-, FPGA- und ASIC-Firmware angezeigt.

HINWEIS: Die Schaltfläche „Neustart erforderlich“ wird nur angezeigt, wenn ein Neustart erforderlich ist.

Abbildung 6-11. Fenster „Firmware-Version“



Unterkategorie SIPs

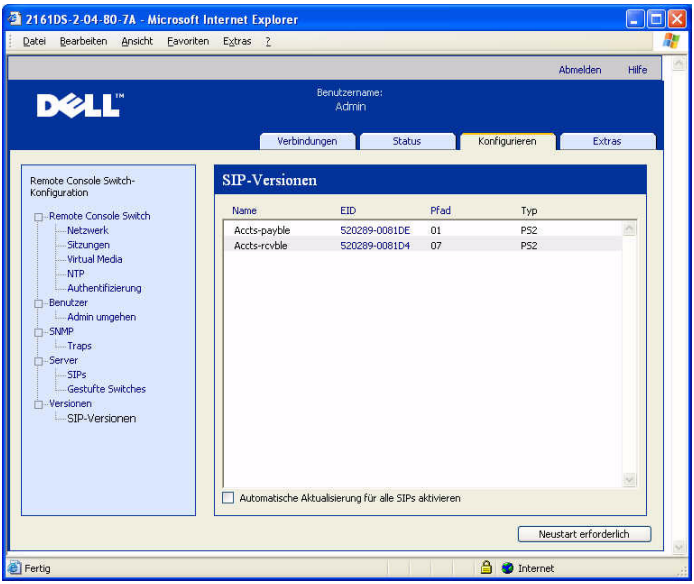
Über die Unterkategorie **SIPs** können Versionsinformationen angezeigt werden. Durch Klicken auf die EID wird ein Fenster aufgerufen, mit dem Sie die SIP-Firmware aktualisieren und die SIPs zurücksetzen können, die an einen gestuften Switch angeschlossen sind.

Durch Aktivieren des Kontrollkästchens **Auto-Aktualisierung für alle SIPs aktivieren** wird die Firmware aller nachfolgend angeschlossenen SIPs auf die Firmware-Version des Remote Console Switches aktualisiert. Dadurch wird sichergestellt, dass die SIP-Firmware mit der Remote Console Switch-Firmware kompatibel ist.

Weitere Informationen zur Aktualisierung von SIPs finden Sie unter „Aktualisieren der Firmware“ auf Seite 125.

HINWEIS: Die Schaltfläche „Neustart erforderlich“ wird nur angezeigt, wenn ein Neustart erforderlich ist.

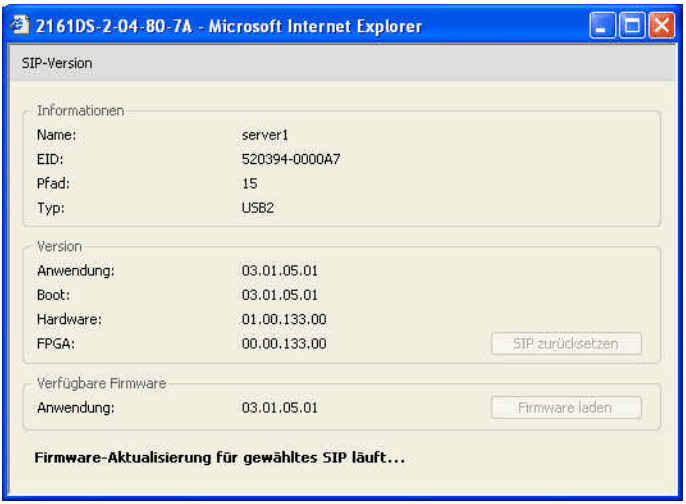
Abbildung 6-12. Fenster „SIPs – Firmware-Version“



So zeigen Sie die Versionsinformationen für ein SIP an:

1. Klicken Sie auf das Register **Konfigurieren** der integrierten Weboberfläche und dann auf die Unterkategorie **SIPs** der Kategorie **Versionen** in der linken Spalte.
2. Klicken Sie auf die EID des SIP, dessen Firmware-Version angezeigt werden soll.

Abbildung 6-13. Fenster „SIP-Version“



Falls ein gestufter Switch vom Remote Console Switch nicht erkannt wird, kann es erforderlich sein, das SIP, das den gestuften Switch mit dem Remote Console Switch verbindet, zurückzusetzen. Diese Funktion wird über die Schaltfläche **SIP zurücksetzen** in der Unterkategorie **SIPs** durchgeführt.

HINWEIS: Es stehen PS/2-, USB- und USB2-SIPs zur Verfügung. Außerdem ist der Remote Console Switch mit allen IQ-Modulen kompatibel, einschließlich Sun- und seriellen IQ-Modulen.

HINWEIS: Die Schaltfläche SIP zurücksetzen ist nur verfügbar, wenn der SIP-Typ PS/2 ist und derzeit keine Aktualisierung der Firmware durchgeführt wird.

HINWEIS: Dieser Vorgang ist nur relevant, wenn in Ihrem Remote Console Switch-System ein PS/2-SIP an einen gestuften Switch angeschlossen ist. In diesem Fall kann es erforderlich sein, das SIP zurückzusetzen, falls der gestufte Switch nicht erkannt wird.

HINWEIS: Wenn das Zurücksetzen durchgeführt wird, während ein Remote Console Switch direkt an einen Server und nicht an einen kaskadierten Switch angeschlossen ist, kann dies zu einem Ausfall von Tastatur oder Maus führen. In diesem Fall muss der Zielserver neu gestartet werden.

So setzen Sie ein SIP zurück:

1. Klicken Sie auf das Register **Konfigurieren** der integrierten Weboberfläche und dann auf die Unterkategorie **SIPs** der Kategorie **Versionen** in der linken Spalte.
2. Klicken Sie auf die EID des SIP, das zurückgesetzt werden soll.
3. Klicken Sie auf **SIP zurücksetzen**. In einer Warnmeldung werden Sie darauf hingewiesen, dass diese Funktion für gestufte Switches vorgesehen ist und dass ein Zurücksetzen des SIP möglicherweise dazu führt, dass der Server neu gestartet werden muss.
4. Klicken Sie auf **OK** um fortzufahren.
   – oder –
   Klicken Sie auf **Abbrechen**, um zur Unterkategorie „SIPs“ zurückzukehren.

Aktualisieren der Firmware

Sie können die Firmware für den Remote Console Switch oder für die SIPs aktualisieren. Die SIPs können einzeln oder gleichzeitig aktualisiert werden. Während der Aktualisierung wird eine Statusanzeige eingeblendet. Während der Aktualisierung können Sie keinen anderen Aktualisierungsvorgang starten.

Mit dem Kontrollkästchen **Auto-Aktualisierung für alle SIPs aktivieren** können Sie die automatische Aktualisierung der SIP-Firmware aktivieren. Sie können die automatische Aktualisierung jederzeit außer Kraft setzen, indem Sie die im nächsten Abschnitt beschriebene Schaltfläche **Firmware laden** verwenden.

HINWEIS: Für den 2161DS-2, 4161DS, und 2321DS können Sie neue Gerätefirmware mit dem ASMP- (falls unterstützt) oder dem TFTP-Dateiübertragungsprotokoll laden. Bei der ASMP-Dateiübertragung können Sie die Firmware aus einem lokalen Dateisystem auswählen. Bei TFTP-Dateiübertragung mit dem 2161DS können Sie die TFTP-Serveradresse und den Namen der Firmware-Datei angeben.

So aktualisieren Sie die Firmware des Remote Console Switches:

1. Klicken Sie auf das Register **Extras** der integrierten Weboberfläche. Das Fenster **Extras** wird angezeigt.
2. Klicken Sie auf die Schaltfläche **Remote Console Switch Firmware aktualisieren**.

3 Das Fenster **Remote Console Switch Firmware aktualisieren** wird angezeigt. Wählen Sie **TFTP-Server** oder „FTP-Server“ als Quelle aus, und geben Sie die IP-Adresse des TFTP-Servers bzw. FTP-Servers ein, auf dem sich die Firmware befindet, sowie den Dateinamen und Verzeichnisort.
– oder –
Klicken Sie auf **Dateisystem** und durchsuchen Sie die Verzeichnisstruktur nach dem Speicherort der FLASH-Datei. Klicken Sie auf **Öffnen**.

Abbildung 6-14. Fenster „Switch-Firmware aktualisieren“

4 Klicken Sie auf die Schaltfläche **Aktualisieren**. Die Schaltfläche **Aktualisieren** wird abgeblendet und eine Statusmeldung und eine Statusanzeige werden angezeigt.

5 Wenn die Aktualisierung abgeschlossen ist, wird der Remote Console Switch neu gestartet.

WICHTIGER HINWEIS: Fahren Sie den Remote Console Switch während der Aktualisierung nicht herunter.

Sie können die Firmware für alle SIPs eines bestimmten Typs aktualisieren.

So aktualisieren Sie mehrere SIPs gleichzeitig:

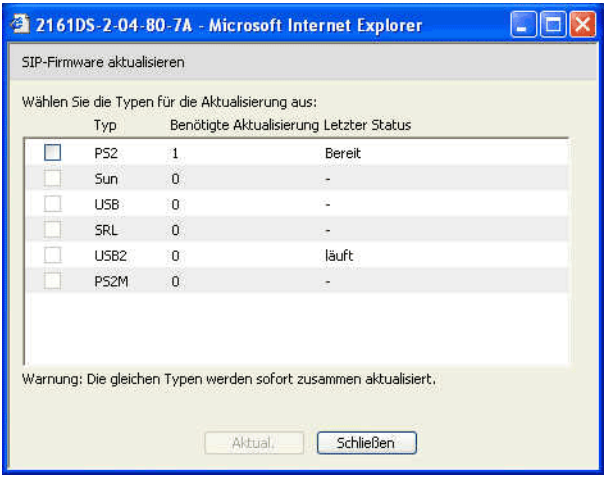
1 Klicken Sie auf das Register **Extras** der integrierten Weboberfläche. Das Fenster **Extras** wird angezeigt.

2 Klicken Sie auf die Schaltfläche **SIP-Firmware aktualisieren**. Das Fenster **SIP-Firmware aktualisieren** wird angezeigt.

3 Markieren Sie die Kontrollkästchen vor jedem SIP-Typ (PS/2, USB, USB2, Seriell oder Sun), den Sie aktualisieren möchten.

HINWEIS: Ein abgeblendetes Kontrollkästchen weist darauf hin, dass alle SIPs dieses Typs über aktuelle Firmware verfügen oder dass kein SIP dieses Typs im System vorhanden ist.

Abbildung 6-15. Fenster „SIP-Firmware aktualisieren“



4 Klicken Sie auf **Aktualisieren**. Die Schaltfläche **Aktualisieren** wird abgeblendet. Abhängig vom Status der jeweiligen SIP-Aktualisierung wird in der Spalte „Letzter Status“ entweder „In Bearbeitung“ oder „Erfolgreich beendet“ angezeigt. Die Nachricht „Firmware-Aktualisierung läuft“ wird so lange angezeigt, bis alle ausgewählten SIP-Typen aktualisiert sind.

5 Wenn die Aktualisierung abgeschlossen ist, werden Sie in einer Meldung aufgefordert, den Abschluss der Aktualisierung zu bestätigen. Sobald dies bestätigt ist, wird die Schaltfläche **Aktualisieren** wieder verfügbar.

6 Klicken Sie auf **Schließen**, um das Fenster **Firmware aktualisieren** zu beenden.

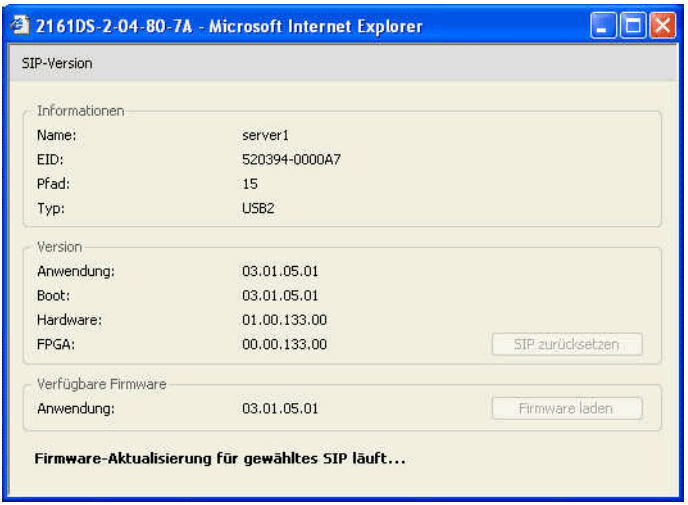
So aktualisieren Sie die Firmware für einzelne SIPs:

1 Klicken Sie auf das Register **Konfigurieren** der integrierten Weboberfläche.

2 Klicken Sie unter **Versionen** in der linken Spalte auf die Unterkategorie **SIPs**.

3 Klicken Sie auf die **EID** des SIPs, dessen Firmware-Informationen angezeigt werden sollen. Das Fenster „SIP-Version“ wird geöffnet.

Abbildung 6-16. Fenster „SIP-Version“



4 Vergleichen Sie die aktuellen Informationen mit denen im Feld **Verfügbare Firmware**, um die verfügbare Firmware-Aktualisierung für das SIP anzuzeigen. (Sie können die Firmware auch laden, wenn die aktuelle Version mit der verfügbaren Version identisch ist. In manchen Fällen kann das SIP auf eine ältere, kompatible Version heruntergestuft werden.)

5 Klicken Sie auf die Schaltfläche **Firmware laden**.

6 Die Firmware-Aktualisierung beginnt. Während der Aktualisierung wird unterhalb des Felds **Verfügbare Firmware** eine Statusmeldung angezeigt und die Schaltfläche **Firmware laden** wird abgeblendet. Wenn die Aktualisierung abgeschlossen ist, wird eine Meldung angezeigt, dass die Aktualisierung erfolgreich war.

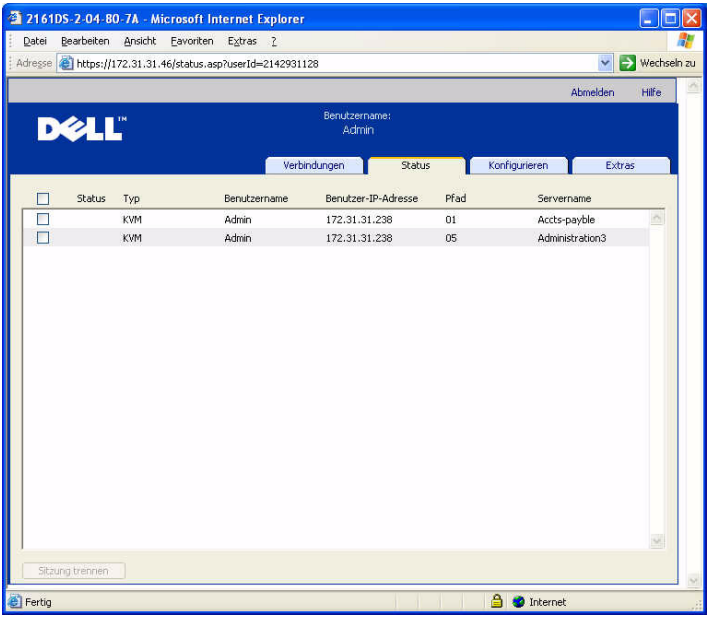
7 Wiederholen Sie die Schritte 2 - 6 für alle SIPs, die einzeln aktualisiert werden sollen.

8 Klicken Sie abschließend auf **OK**.

Steuern des Benutzerstatus

Sie können die aktuell aktiven Benutzerverbindungen über das Register **Status** der integrierten Weboberfläche anzeigen und trennen. Sie können den Sitzungstyp, den Servernamen oder das SIP, an das sie angeschlossen sind, sowie die Systemadresse anzeigen. Zusätzlich zum Trennen einer Benutzersitzung ermöglicht die integrierte Weboberfläche es einem Benutzer auch, die Steuerung eines Servers zu übernehmen, der gerade von einem anderen Benutzer verwendet wird. Weitere Informationen finden Sie unter „Trennung“ auf Seite 88.

Abbildung 6-17. Fenster „Benutzerstatus“



So trennen Sie eine Benutzersitzung:

1. Klicken Sie auf das Register **Status** der integrierten Weboberfläche. Eine Benutzerliste mit Informationen zu deren Verbindungen wird angezeigt.
2. Markieren Sie das Kontrollkästchen für einen oder mehrere Benutzer, die Sie trennen möchten.
3. Klicken Sie auf die Schaltfläche **Sitzung abbrechen**. Es wird eine Meldung mit der Aufforderung angezeigt, den Befehl zur Verbindungstrennung zu bestätigen.

4 Klicken Sie auf **OK**, um die Verbindung des Benutzers zu trennen.
– oder –
Klicken Sie auf **Abbrechen**, um das Dialogfeld zu verlassen, ohne den Befehl zur Verbindungstrennung auszuführen.

HINWEIS: Voraussetzung für eine Verbindungstrennung sind die entsprechenden Zugriffsrechte. Wenn Sie nicht über die entsprechende Berechtigung verfügen, um die Verbindung eines Benutzers zu trennen, ist das Kontrollkästchen neben diesem Benutzer nicht verfügbar.

Neustart des Systems

Sie können den Remote Console Switch über das Register **Extras** der integrierten Weboberfläche neu starten. Wenn Sie auf die Schaltfläche **Remote Console Switch neu starten** klicken, wird eine Trennungsmeldung an alle aktiven Benutzer gesendet. Dann wird der aktuelle Benutzer abgemeldet und der Remote Console Switch sofort neu gestartet.

So führen Sie einen Neustart Ihres Systems durch:

1 Klicken Sie auf das Register **Extras** der integrierten Weboberfläche. Das Fenster **Extras** wird angezeigt.

2 Klicken Sie auf die Schaltfläche **Neustart**. Es wird eine Meldung mit der Aufforderung angezeigt, den Neustart zu bestätigen.

3 Klicken Sie auf **OK**, um den Neustart durchzuführen.
– oder –
Klicken Sie auf **Abbrechen**, um den Neustart abzubrechen.

Verwalten der Konfigurationsdateien für den Remote Console Switch

Konfigurationsdateien enthalten alle Einstellungen für einen Remote Console Switch. Dazu gehören die Einstellungen der Einheit sowie SNMP-, LDAP- und NTP-Einstellungen. Sie haben die Möglichkeit, diese Konfigurationsdatei zu speichern. Sollten Sie Ihren Remote Console Switch austauschen müssen, können Sie die Konfigurationsdatei auf den neuen Switch übertragen und müssen keine manuelle Konfiguration vornehmen.

HINWEIS: Informationen zu Benutzerkonten werden in der Benutzerdatenbank und nicht in der Konfigurationsdatei gespeichert. Weitere Informationen finden Sie unter „Verwalten der Benutzerdatenbanken“ auf Seite 132.

So lesen und speichern Sie die Konfigurationsdatei eines Remote Console Switches:

1. Klicken Sie auf das Register **Extras** der integrierten Weboberfläche. Das Fenster **Extras** wird angezeigt.
2. Klicken Sie auf die Schaltfläche **Remote Console Switch-Konfiguration speichern**. Das Fenster **Remote Console Switch-Konfiguration speichern** wird angezeigt.
3. (Optional) Geben Sie ein Kennwort im Feld **Kennwort** ein und wiederholen Sie die Eingabe im Feld **Kennwort bestätigen**. Dieses Kennwort ist erforderlich, um diese Datenbank in einem Remote Console Switch wiederherzustellen. Klicken Sie auf **OK**.

HINWEIS: Sie können das Kennwortfeld leer lassen, wenn der Zugriff auf die Konfigurationsdatei ohne Kennwort erfolgen soll.

4. Klicken Sie auf **Durchsuchen** und navigieren Sie zum gewünschten Speicherort der Konfigurationsdatei. Der Speicherort wird im Feld **Speichern unter** angezeigt.
5. Klicken Sie auf **Speichern**.
6. Die Konfigurationsdatei wird vom Remote Console Switch gelesen und an dem gewünschten Ort gespeichert. Ein Statusfenster wird angezeigt.
7. Wenn dieser Vorgang abgeschlossen ist, wird eine Meldung mit der Aufforderung angezeigt, das Ende des Lesevorgangs zu bestätigen. Klicken Sie auf **OK**, um zum Hauptfenster zurückzukehren.

So stellen Sie eine Konfigurationsdatei auf einem Remote Console Switch wieder her:

1. Klicken Sie auf das Register **Extras** der integrierten Weboberfläche. Das Fenster **Extras** wird angezeigt.
2. Klicken Sie auf die Schaltfläche **Remote Console Switch-Konfiguration wiederherstellen**. Das Fenster **Remote Console Switch-Konfiguration wiederherstellen** wird angezeigt.
3. Klicken Sie auf **Durchsuchen** und navigieren Sie zu dem Speicherort der Konfigurationsdatei. Dateiname und Speicherort werden im Feld **Dateiname** angezeigt.

4 Klicken Sie auf **Wiederherstellen**. Das Fenster für die Kennworteingabe wird geöffnet.

5 (Optional) Geben Sie das Kennwort ein, das Sie beim Speichern der Konfigurationsdatenbank erstellt haben. Klicken Sie auf **OK**. Die Konfigurationsdatei wird auf dem Remote Console Switch gespeichert. Ein Statusfenster wird angezeigt.

HINWEIS: Sie können das Kennwortfeld leer lassen, wenn kein Kennwort für die Konfigurationsdatei erstellt wurde.

6 Wenn dieser Vorgang abgeschlossen ist, wird eine Meldung mit der Aufforderung angezeigt, das Ende des Schreibvorgangs zu bestätigen. Klicken Sie auf **OK**, um zum Hauptfenster zurückzukehren.

Verwalten der Benutzerdatenbanken

Benutzerdatenbankdateien enthalten alle Benutzerkonten, die einem Remote Console Switch zugeordnet sind. Sie haben die Möglichkeit, diese Benutzerdatenbankdatei zu speichern und zu verwenden, um Benutzer auf mehreren Remote Console Switches zu konfigurieren, indem die Benutzerkontendatei auf dem neuen Switch gespeichert wird.

HINWEIS: Die Benutzerkontendatei ist verschlüsselt und Sie werden aufgefordert, beim Speichern der Datei ein Kennwort zu erstellen. Sie müssen das Kennwort erneut eingeben, wenn die Datei auf einer neuen Einheit gespeichert wird.

So speichern Sie die Benutzerdatenbank eines Remote Console Switches:

1 Klicken Sie auf das Register **Extras** der integrierten Weboberfläche. Das Fenster **Extras** wird angezeigt.

2 Klicken Sie auf die Schaltfläche **Remote Console Switch-Benutzerdatenbank speichern**. Das Fenster **Remote Console Switch-Benutzerdatenbank speichern** wird angezeigt.

3 Klicken Sie auf **Durchsuchen** und navigieren Sie zu dem gewünschten Speicherort für die Benutzerdatenbankdatei. Der Speicherort wird im Feld **Speichern unter** angezeigt.

4 Klicken Sie auf **Speichern**. Das Fenster für die Kennworteingabe wird geöffnet.

5 Geben Sie ein Kennwort in das Feld Kennwort ein und wiederholen Sie das Kennwort im Feld Kennwort bestätigen. Dieses Kennwort ist erforderlich, um diese Datenbank in einem Remote Console Switch wiederherzustellen.

Klicken Sie auf **OK**. Die Benutzerdatenbankdatei wird vom Remote Console Switch gelesen und an dem gewünschten Ort gespeichert. Ein Statusfenster wird angezeigt.

6. Wenn dieser Vorgang abgeschlossen ist, wird eine Meldung mit der Aufforderung angezeigt, das Ende des Lesevorgangs zu bestätigen. Das Fenster **Remote Console Switch-Benutzerdatenbank speichern** wird nach der Bestätigung geschlossen und das Fenster **Extras** wieder angezeigt.

So stellen Sie eine Benutzerdatenbankdatei auf einem Remote Console Switch wieder her:

1. Klicken Sie auf das Register **Extras** der integrierten Weboberfläche. Das Fenster **Extras** wird angezeigt.
2. Klicken Sie auf die Schaltfläche **Remote Console Switch-Benutzerdatenbank wiederherstellen**. Das Fenster **Remote Console Switch-Benutzerdatenbank wiederherstellen** wird angezeigt.
3. Klicken Sie auf **Durchsuchen** und navigieren Sie zu dem Speicherort der Benutzerdatenbankdatei. Dateiname und Speicherort werden im Feld **Dateiname** angezeigt.
4. Klicken Sie auf **Wiederherstellen**. Das Fenster für die Kennworteingabe wird geöffnet.
5. Geben Sie das Kennwort ein, das Sie beim Speichern der Benutzerdatenbank erstellt haben. Klicken Sie auf **OK**. Die Benutzerdatenbankdatei wird auf dem Remote Console Switch gespeichert. Ein Statusfenster wird angezeigt.
6. Wenn dieser Vorgang abgeschlossen ist, wird eine Meldung mit der Aufforderung angezeigt, das Ende des Schreibvorgangs zu bestätigen. Das Fenster **Benutzerdatenbank wiederherstellen** wird nach der Bestätigung geschlossen und das Fenster **Extras** wieder angezeigt.

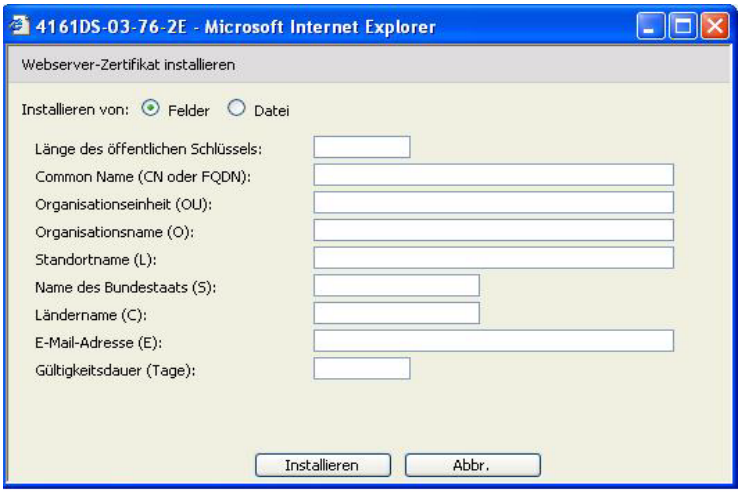
Installieren eines Webzertifikats

Ein Webzertifikat ermöglicht es Ihnen, die integrierte Weboberfläche in einen Webbrowser einzugeben, ohne den Remote Console Switch bei jedem Zugriff auf die integrierte Weboberfläche als vertrauenswürdigen Webserver anerkennen zu müssen. Mithilfe des Fensters „Webserver-Zertifikat installieren“ können Sie ein OpenSSL-Zertifikat mit eigener Signatur erstellen.

So installieren Sie ein Webzertifikat:

1. Klicken Sie auf das Register **Extras** der integrierten Weboberfläche. Das Fenster **Extras** wird angezeigt.
2. Klicken Sie auf die Schaltfläche **Webserver-Zertifikat installieren**. Das Fenster **Webserver-Zertifikat installieren** wird geöffnet.

Abbildung 6-18. Fenster „Webserver-Zertifikat installieren“



3. Wählen Sie **Felder** aus und füllen Sie die folgenden Felder aus:
   - a **Länge des öffentlichen Schlüssels**: Anzahl der für das Zertifikat gewünschten Bits.
   - b **Common Name**: Ihr Name. (Da es sich um Ihr Root-Zertifikat handelt, sollten Sie einen geeigneten Namen verwenden, z. B. „Firma_Name Zertifizierungsstelle.“)
   - c **Organisationseinheit** (optional): Name der Organisationseinheit (z. B. Marketing).
   - d **Organisationsname**: Der genaue, nicht abgekürzte Firmenname Ihrer Organisation.
   - e **Standortname**: Der Ort, in dem sich der Firmensitz befindet.
   - f **Bundesstaat**: Der nicht abgekürzte Bundesstaat, in dem sich der Firmensitz befindet.

g **Ländername**: Der aus zwei Buchstaben bestehende ISO-Code für Ihr Land.

h **E-Mail-Adresse**: Die Kontakt-E-Mail-Adresse für die Zertifizierungsstelle.

i **Gültigkeitsdauer**: Gültigkeitsdauer des Zertifikats in Tagen.

– oder –

Wählen Sie **Datei** aus und laden Sie dann eine Firmenzertifikatdatei (*.pem) herunter.

4 Wählen Sie **Installieren** aus. Schließen Sie den Webbrowser und starten Sie anschließend die integrierte Weboberfläche für dieselbe IP-Adresse erneut.

HINWEIS: Wenn eine Firmenzertifikatdatei importiert wird, kann der Neustart der integrierten Weboberfläche bis zu 30 Sekunden dauern.

5 Zeigen Sie das Zertifikat durch Anklicken an, wenn Sie dazu aufgefordert werden, und befolgen Sie die Anweisungen, um das Zertifikat in das Verzeichnis „Root Certificate Authority“ zu importieren. Wenn das Zertifikat gespeichert wurde, sollte dem Benutzer keine Warnmeldung bezüglich des Zertifikats angezeigt werden.

Verwalten von PDUs

Sie können unterstützte PDUs über die integrierte Weboberfläche steuern. Das Verketten von bis zu neun PDUs pro Remote Console Switch PDU-Port wird unterstützt. Durch die PDU-Unterstützung kann der Benutzer jeden Server bzw. jedes Gerät, der bzw. das an die PDU angeschlossen ist, einschalten, ausschalten sowie aus- und wieder einschalten.

HINWEIS: Diese Funktion ist nur für den 2321DS Remote Console Switch verfügbar.

HINWEIS: Unter dell.avocent.com finden Sie eine Auflistung der unterstützten PDUs.

So konfigurieren Sie eine PDU:

1 Klicken Sie auf das Register **Konfigurieren** der integrierten Weboberfläche und dann auf die Kategorie **PDUs** in der linken Spalte, um eine Liste der PDUs anzuzeigen.

2 Klicken Sie auf die PDU, auf die Sie zugreifen möchten. Das Fenster **PDU-Einstellungen** wird geöffnet.

3 Ändern Sie im Dialogfeld **PDU-Einstellungen** den PDU-Namen, legen Sie die Verzögerungszeit zwischen dem Aus- und Einschalten fest, aktivieren bzw. deaktivieren Sie den aktuellen Schutz, aktivieren bzw. deaktivieren Sie den hörbaren Alarm und legen Sie den minimalen Ampere-Wert und den maximalen Ampere-Wert im Feld **Eingangsparameter** fest.

So konfigurieren Sie ein Gerät, das an eine PDU angeschlossen ist:

1 Klicken Sie auf das Register **Konfigurieren** der integrierten Weboberfläche und dann auf die Kategorie **PDUs** in der linken Spalte, um eine Liste der PDUs anzuzeigen.

2 Klicken Sie auf die PDU, auf die Sie zugreifen möchten. Das Fenster **PDU-Einstellungen** wird geöffnet.

3 Klicken Sie im unteren Bereich des Fensters **PDU-Einstellungen** auf die Schaltfläche **Ausgangs-Einstellungen**, um eine Liste der Geräte anzuzeigen, die an die PDU angeschlossen sind. Das Fenster **Ausgangs-Einstellungen** wird geöffnet.

4 So ändern Sie den Namen eines Ausgangs:

   a Klicken Sie in der Spalte **Name** auf den Link für den Ausgang, den Sie ändern möchten. Das Fenster **Stromausgangsnamen ändern** wird geöffnet.

   b Wenn es sich bei dem Gerät um einen Server handelt, klicken Sie auf **Server** und wählen Sie dann den Namen aus, indem Sie auf den entsprechenden Eintrag in der Spalte **Servername** der Tabelle klicken.

   – oder –

   Wenn es sich bei dem Gerät nicht um einen Server handelt, klicken Sie auf **Anderes Gerät** und geben Sie dann den entsprechenden Text im Textfeld **Name** ein.

   c Klicken Sie auf **Speichern** und dann auf **Schließen**, um zum Fenster **Ausgangs-Einstellungen** zurückzukehren.

5 Wenn Sie das Einschaltintervall ändern möchten, geben Sie den Wert in Sekunden für den zu konfigurierenden Ausgang im Textfeld in der Spalte **Intervall Ein** ein.

6 Klicken Sie auf **Speichern** und dann auf **Schließen**, um zum Fenster **PDUs** zurückzukehren.

So nehmen Sie die Stromüberwachung für ein Gerät vor, das an eine PDU angeschlossen ist:

1. Klicken Sie auf das Register **Konfigurieren** der integrierten Weboberfläche und dann auf die Unterkategorie **Ausgänge**, die sich unter **PDUs** in der linken Spalte befindet, um eine Liste der verfügbaren Ausgänge anzuzeigen.

HINWEIS: Es werden nur Ausgänge in dieser Liste angezeigt, denen ein Name zugeordnet ist.

2. Aktivieren Sie das Kontrollkästchen neben den Ausgängen, die Sie konfigurieren möchten.
3. Klicken Sie auf die Schaltfläche **Ein**, um die ausgewählten Ausgänge zu aktivieren.

   – oder –

   Klicken Sie auf die Schaltfläche **Aus**, um die ausgewählten Ausgänge zu deaktivieren.

   – oder –

   Klicken Sie auf die Schaltfläche **Neustart**, um die ausgewählten Ausgänge neu zu starten.
4. Klicken Sie auf **Speichern**.

7

Migrieren des Remote Console Switches

Wenn Sie eine vorhandene Installation von Remote Console Switches besitzen und die Einheitenverwaltungsanzeige (EVA) der Remote Console Switch Software verwenden, befolgen Sie das in diesem Kapitel beschriebene Verfahren zur Migration der Switches von der Remote Console Switch Software auf die integrierte Weboberfläche.

HINWEIS: Die integrierte Weboberfläche wird von den 2161DS Remote Console Switches nicht unterstützt, weswegen diese Switchmodelle nicht migriert werden können. Verwenden Sie die Remote Console Software zur Verwaltung der 2161 Remote Console Switches. Informationen hierzu finden Sie in der Bedienungsanleitung der Dell Remote Console Switch-Software oder in der Softwarehilfe.

Auf die EVA zugreifen

Sie beginnen mit der Remote Console Switch-Software EVA, um den Remote Console Switch auf die integrierte Weboberfläche zu migrieren.

So greifen Sie auf die EVA zu:

1. Klicken Sie im Explorer auf das Register **Remote Console Switches**.
2. Doppelklicken Sie auf einen Remote Console Switch im **Einheitenauswahl**-Fenster.
   – oder –
   Wählen Sie einen Remote Console Switch im **Einheitenauswahl**-Fenster aus, und klicken Sie dann auf die Schaltfläche **Remote Console Switch verwalten**.
   – oder –
   Klicken Sie mit der rechten Maustaste auf einen Remote Console Switch im **Einheitenauswahl**-Fenster. Ein Popup-Menü wird angezeigt. Wählen Sie **Remote Console Switch verwalten** aus.
   – oder –
   Klicken Sie auf einen Remote Console Switch im **Einheitenauswahl**-Fenster und betätigen Sie die <Eingabetaste>. Eine Kennwort-Eingabeaufforderung wird angezeigt.

HINWEIS: Wenn die Taskschaltfläche „Remote Console Switch **konfigurieren**“ statt der Taskschaltfläche „Remote Console Switch **verwalten**“ angezeigt wird, wurde dieser Remote Console Switch bereits auf die integrierte Weboberfläche migriert.

3 Geben Sie Ihren Benutzernamen und Ihr Kennwort ein und klicken Sie auf OK. Das Dialogfeld der EVA wird angezeigt.

Aktualisieren von Firmware mithilfe der EVA

Bevor Sie mit dem Migrationsprozess beginnen (siehe „Migration von Remote Console Switches zur integrierten Weboberfläche“ auf Seite 142), verwenden Sie die EVA, um die Firmware auf eine Version zu aktualisieren, die die integrierte Weboberfläche unterstützt.

Die SIPs können einzeln oder gleichzeitig aktualisiert werden. Während der Aktualisierung wird eine Statusanzeige eingeblendet. Während der Aktualisierung können Sie keinen anderen Aktualisierungsvorgang starten.

HINWEIS: Für den 2161DS-2, 4161DS und 2321DS können Sie neue Gerätefirmware mit dem ASMP- (falls unterstützt), FTP- oder TFTP-Dateiübertragungsprotokoll laden. Bei der ASMP-Dateiübertragung können Sie die Firmware aus einem lokalen Dateisystem auswählen. Der 2161DS unterstützt die TFTP-Dateiübertragung, die es Ihnen ermöglicht, die TFTP-Serveradresse und den Namen der Firmware-Datei anzugeben.

Aktualisieren der Remote Console Switch-Firmware

So aktualisieren Sie die Remote Console Switch-Firmware:

1 Klicken Sie in der EVA auf das Register Extras. Das Dialogfeld Extras wird angezeigt.

2 Klicken Sie auf die Schaltfläche Remote Console Switch-Firmware aktualisieren.

Wenn Sie in der Kategorie „Einstellungen“ in der EVA Änderungen durchgeführt, diese aber noch nicht übernommen haben, bevor Sie die Aktualisierung starten, werden Sie in einer Warnmeldung aufgefordert, die Aktualisierung zu bestätigen, da eine Aktualisierung einen Neustart des Switches erfordert. Wenn Sie die Änderungen nicht übernehmen, werden diese vor der Aktualisierung der Firmware verworfen.

So übernehmen Sie die Änderungen vor der Aktualisierung:

a Klicken Sie auf **Nein**, um die Aktualisierung der Firmware abzubrechen.

b Klicken Sie auf **Übernehmen**.

c Klicken Sie auf die Schaltfläche **Remote Console Switch-Firmware aktualisieren**.
– oder –
Um die Änderungen vor der Aktualisierung zu verwerfen, klicken Sie auf **Ja**.

d Das Dialogfeld **Firmware aktualisieren** wird angezeigt. Wählen Sie **TFTP-Server** als Quelle aus und geben Sie die IP-Adresse des TFTP-Servers (Trivial File Transfer Protocol), auf dem sich die Firmware befindet, sowie den Dateinamen und Speicherort ein.
– oder –
Klicken Sie auf **Dateisystem** und durchsuchen Sie die Verzeichnisstruktur nach dem Speicherort der FLASH-Datei. Klicken Sie auf **Öffnen**.

3 Klicken Sie auf die Schaltfläche **Aktualisieren**. Die Schaltfläche **Aktualisieren** wird abgeblendet und eine Statusmeldung wird angezeigt.

4 Wenn die Aktualisierung abgeschlossen ist, wird eine Meldung mit der Aufforderung angezeigt, einen Neustart zu bestätigen. Die neue Firmware wird erst nach einem Neustart des Switches verwendet. Klicken Sie auf **Ja**, um den Remote Console Switch neu zu starten. Das Dialogfeld **Firmware aktualisieren** zeigt nun eine Statusmeldung an, die meldet, dass der Neustart abgeschlossen ist.
– oder –
Klicken Sie auf **Nein**, um den Neustart zu einem späteren Zeitpunkt auszuführen. Die neue Firmware kann erst nach einem Neustart verwendet werden.

HINWEIS: Wenn Sie die Remote Console Switch-Firmware auf eine Version aktualisieren, die die integrierte Weboberfläche unterstützt, sollten Sie EVA möglichst erst beenden, wenn der Neustart abgeschlossen ist. Andernfalls müssen Sie die EVA nach Abschluss des Neustarts öffnen, damit der Switch im Migrations-Assistenten verfügbar wird.

5 Klicken Sie auf **Schließen**, um das Fenster **Firmware aktualisieren** zu verlassen.

WICHTIGER HINWEIS: Fahren Sie den Remote Console Switch während der Aktualisierung nicht herunter.

Migration von Remote Console Switches zur integrierten Weboberfläche

Wenn Sie die Firmware eines Remote Console Switches auf eine Version aktualisiert haben, die die integrierte Weboberfläche unterstützt, wird der Switch im Migrations-Assistenten verfügbar. Befolgen Sie die Anweisungen des Migrations-Assistenten, um direkt über die integrierte Weboberfläche Switches verwalten und Viewer-Sitzungen starten zu können.

WICHTIGER HINWEIS: Nach der Migration eines Remote Console Switches können Sie die Remote Console Switch Software-EVA nicht mehr verwenden. Verwenden Sie stattdessen die integrierte Weboberfläche.

So führen Sie eine Migration von Remote Console Switches durch:

1. Wählen Sie im Explorer **Extras – Migration** aus. Daraufhin wird die Begrüßungsseite des Migrations-Assistenten geöffnet. Klicken Sie auf **Weiter**.
2. Alle Switches, bei denen eine Migration möglich ist, werden in der Liste **Verfügbare Remote Console Switches** angezeigt. Wählen Sie den Switch aus, der migriert werden soll, und klicken Sie auf die Schaltfläche **>**, um den Switch in die Liste der zu migrierenden **Remote Console Switches** zu verschieben.

HINWEIS: Wenn der Remote Console Switch, der migriert werden soll, nicht im Migrations-Assistenten verfügbar ist, haben Sie möglicherweise die EVA beendet, bevor die Firmware-Aktualisierung abgeschlossen war. Schließen Sie den Migrations-Assistenten und öffnen Sie die EVA, damit die aktualisierte Firmware-Version erkannt werden kann. Wenn Sie den Migrations-Assistenten wieder öffnen, sollte der Remote Console Switch verfügbar sein.

3. Klicken Sie auf **Weiter**.
4. Es wird empfohlen, bei der Migration von Switches die in der lokalen Datenbank gespeicherten Remote Console Switch-Informationen zu verwenden. Aktivieren Sie zu diesem Zweck das Kontrollkästchen im Fenster „Die Informationen der lokalen Datenbank verwenden“.
   – oder –
   Wenn Sie die Informationen der lokalen Datenbank nicht verwenden möchten, deaktivieren Sie das Kontrollkästchen.

5 Geben Sie die HTTP- und die HTTPS-Portnummer im Feld **HTTP-Port** bzw. **HTTPS-Port** ein, wenn die Portnummern für den Remote Console Switch in der seriellen Konsole geändert wurden. Weitere Informationen zum Ändern der Portnummern in der seriellen Konsole finden Sie unter „So konfigurieren Sie die HTTP- und HTTPS-Ports:“ auf Seite 20.

HINWEIS: Wenn Sie mehrere Remote Console Switches hinzugefügt haben, kann für die Remote Console Switches, die die von Ihnen angegebenen HTTP- und HTTPS-Ports nicht verwenden, keine Migration ausgeführt werden. Sie können sie migrieren, indem Sie den Migrations-Assistenten erneut ausführen und die richtigen Ports für diese Remote Console Switches angeben.

6 Klicken Sie auf **Weiter**.

7 Wenn die Migration erfolgreich durchgeführt wurde, wird das Fenster „Den Migrations-Assistenten beenden“ geöffnet.
– oder –
Wurde die Migration nicht erfolgreich durchgeführt, wird das Fenster „Der Migrations-Assistent war nicht erfolgreich“ geöffnet.

8 Klicken Sie auf **Fertig**, um den Assistenten zu beenden.

Der Remote Console Switch ist nun nicht mehr in der Remote Console Switch Software verfügbar. Sie können den Switch jetzt über die integrierte Weboberfläche verwalten; siehe „Verwalten des Remote Console Switches mithilfe der integrierten Weboberfläche“ auf Seite 105.

Verwenden des Resynchronisations-Assistenten

Befolgen Sie die Anweisungen des Resynchronisations-Assistenten, um die lokale Datenbank und die Remote Console Switch-Datenbank zu synchronisieren.

HINWEIS: Die Schaltfläche „Resynchronisieren“ ist nur für Switches verfügbar, deren Firmware die integrierte Weboberfläche unterstützt.

So starten Sie den Resynchronisations-Assistenten:

1 Klicken Sie im Explorer auf das Register **Remote Console Switches**.

2 Wählen Sie einen Remote Console Switch im **Einheitenauswahl**-Fenster aus und klicken Sie dann auf die Schaltfläche **Resynchronisieren**.
– oder –
Klicken Sie mit der rechten Maustaste auf einen Remote Console Switch im **Einheitenauswahl**-Fenster. Ein Popup-Menü wird angezeigt. Wählen Sie **Resynchronisieren** aus.

3 Der Resynchronisations-Assistent wird geöffnet.

4 Klicken Sie auf **Weiter**.

5 Aktivieren Sie das Kontrollkästchen **Offline-Server einbeziehen**, um Offline-Server in der Datenbank einzubeziehen.
– oder –
Wenn Sie Offline-Server in der Datenbank nicht einbeziehen möchten, deaktivieren Sie das Kontrollkästchen **Offline-Server einbeziehen**.

6 Aktivieren Sie das Kontrollkästchen **Namen aus der Datenbank mit Namen aus dem Remote Console Switch ersetzen**, um die Servernamen in der lokalen Datenbank zu überschreiben.
– oder –
Deaktivieren Sie das Kontrollkästchen **Namen aus der Datenbank mit Namen aus dem Remote Console Switch ersetzen**, um die Servernamen in der lokalen Datenbank beizubehalten.

7 Klicken Sie auf **Weiter**. Das Fenster „Abruf vom Remote Console Switch wird durchgeführt“ wird geöffnet.

8 Dann wird das Fenster „Erkannte Änderungen“ geöffnet, in dem die an der Datenbank vorgenommenen Änderungen angezeigt werden.

9 Klicken Sie auf „Fertig“.

8

LDAP-Funktionalität für den Remote Console Switch

Überblick

Die Dell Remote Console Switches der Produktreihen 2161DS, 2161DS-2, 4161DS und 2321DS können Benutzer über eine lokale Datenbank oder über einen externen, skalierbaren verteilten Verzeichnisdienst mithilfe der Dell Remote Console Switch Software oder der integrierten Weboberfläche mit LDAP-Unterstützung (Lightweight Directory Assistance Protocol) authentifizieren und autorisieren. LDAP ist ein Protokollstandard, der den Zugriff auf ein Verzeichnis und dessen Aktualisierung über TCP/IP ermöglicht. Die Dell Remote Console Switch Software und die integrierte Weboberfläche unterstützen sowohl das Standardschema als auch das erweiterte Dell Schema und bieten leistungsstarke Sicherheitsmerkmale einschließlich Authentifizierung, Datenschutz und Integrität.

HINWEIS: Für die Verwendung von LDAP im IPv6-Modus ist Windows 2008 Server erforderlich.

HINWEIS: Nur Microsoft Active Directory® wird von den Remote Console Switches unterstützt.

HINWEIS: Die Verwendung von Active Directory zur Erkennung von Remote Console Switch-Benutzern wird für die Betriebssysteme Microsoft Windows® 2000 und Windows Server 2003 unterstützt.

Die Struktur von Active Directory

Eine Active Directory (AD)-Implementierung besteht aus einer verteilten Datenbank, die eine hierarchische Struktur von Objekten enthält. Jedem Objekt wird eine Objektklasse zugeordnet, die bestimmt, welche Arten von Daten in diesem Objekt gespeichert werden können. An der Spitze der hierarchischen Struktur stehen Objekte, die AD-Domänen darstellen und so implementiert werden, dass eine Hierarchie von Domänennamen entsteht. Diese Hierarchie wird in einem Baumdiagramm dargestellt, das mit der herkömmlichen Darstellung von DNS-Namensräumen vergleichbar ist. Die Produktreihe der Dell Remote Console Switches ist dazu ausgelegt, eine einzige Domänenstruktur zu unterstützen, die entweder in einer flachen oder tiefen hierarchischen Namensstruktur implementiert wird.

Domänencontroller-Computer

Mit der Domänenhierarchie ist eine entsprechende Hierarchie von Domänencontroller-Computern verknüpft, auf denen AD LDAP-Dienste bereitstellt. Jede Domäne kann über mehrere Peer-Domänencontroller verfügen und über verschiedene geografische Standorte verteilt sein. Die Produktreihe der Dell Remote Console Switches ist dazu ausgelegt, diese beiden Aspekte von AD zu unterstützen. DNS wird dazu verwendet, die Netzwerkkoordinaten eines jeden Domänencontrollers zu bestimmen, so dass die Dell Remote Console Switches Situationen, in denen bestimmte Domänencontroller nicht im Netzwerk zur Verfügung stehen, problemlos bewältigen können. Zu diesem Zweck werden DNS-SRV-Einträge verwendet, damit die Dell Remote Console Switches immer zuerst versuchen, alternative Domänencontroller am „nächstgelegenen" Standort zu kontaktieren – in Abhängigkeit von in den SRV-Einträgen konfigurierten Verwaltungseinstellungen.

Objektklassen

Innerhalb jeder Domäne befindet sich eine weitere Hierarchie von Objekten, in denen Informationen über die verschiedenen Einheiten und Gruppen von Einheiten gespeichert werden. Diese Einheiten werden in AD durch Objektklassen dargestellt, mit deren Hilfe „Container" zur Organisation von Objekten in Gruppen definiert werden. Andere Objektklassen verkörpern Einheiten wie Netzwerkbenutzer, Computer, Drucker oder Netzwerkdienste. Zwei Typen von Containerklassen sind von besonderem Interesse: Gruppen und Organisationseinheiten (OU). Diese beiden Objektklassen ermöglichen es dem AD-Administrator, Gruppen von Einheiten zu definieren, um die Zuweisung von Zugriffssteuerungen und anderen Verwaltungsrichtlinien zu erleichtern. So kann eine Domäne beispielsweise dahingehend konfiguriert werden, dass ein OU-Container namens „Engineering" besteht, der verschiedene Gruppenobjekte enthält, die gemäß ihrer Funktion benannt werden, z. B. „Hardware", „Software" und „Support". Jede dieser Gruppen wird mit einer Mitgliedsliste von Benutzer- und ggf. Computerobjekten konfiguriert. Eine weitere hierarchische Ebene kann durch die „Verschachtelung" von Gruppen konfiguriert werden, wobei die Verschachtelung dadurch erreicht wird, dass der Name eines Gruppenobjekts in der Mitgliedsliste eines anderen Gruppenobjekts enthalten ist. Hierbei muss beachtet werden, dass jedem AD-Gruppenobjekt ein bestimmter „Bereich" zugeordnet ist, der für die Konfiguration von zugelassenen Verschachtelungstypen in Verbindung mit anderen Gruppen zuständig ist. Wenn der Bereich beispielsweise auf „Universal" eingestellt ist, kann die Gruppe an Verschachtelungen über Domänengrenzen hinweg beteiligt sein, wenn der Bereich aber auf „Lokal" eingestellt ist, kann die Gruppe an solchen Verschachtelungen nicht beteiligt

werden. Verschachtelungsregeln sind in der AD-Produktdokumentation dargestellt, die von Microsoft erhältlich ist. Die Produktreihe der Dell Remote Console Switches ist dazu ausgelegt, alle für AD definierten Verschachtelungsregeln zu unterstützen.

Attribute

Es wird noch eine weitere Hierarchieebene in AD verwendet. Mit den einzelnen Objektklassen ist jeweils eine Gruppe von „Attributen“ verknüpft, die dazu dienen, spezifische Informationen über die dargestellte Einheit zu speichern. So sind mit der Objektklasse „Benutzer“ beispielsweise ein Attributtyp namens SAM ACCOUNT NAME und weitere Attribute wie FIRST NAME, SURNAME, PASSWORD usw. verknüpft. Die Produktreihe der Dell Remote Console Switches verwendet die Attribute SAM ACCOUNT NAME und PASSWORD, um Benutzer zu authentifizieren (die formellen AD-Namen für diese zwei Attribute lauten „sAMAccountName“ und „unicodePWD“).

Schemata-Erweiterungen

AD ist bereits mit zahlreichen Objektklassen ausgestattet, einschließlich Standardcontainern für Computer- und Benutzerobjekte sowie Klassen für OU-Container und Klassen zur Darstellung von Computer- und Benutzereinheiten. AD kann erweitert werden, um neue Objektklassen wie die von Dell zur Verfügung gestellten einzuschließen, um so die Verwaltung von Zugriffssteuerungen zu vereinfachen. Erweiterungen dieser Art werden im Allgemeinen als „Schemata-Erweiterungen“ bezeichnet und bilden den Kern der erweiterten Dell Schema-Funktion, die in diesem Handbuch beschrieben ist. Diese Schemata-Erweiterungen bieten benutzerdefinierte Objektklassen zur Darstellung von Dell Remote Console Switches, Zugriffssteuerungsinformationen sowie einen Containertyp, der für die Zuordnung von spezifischen Zugriffssteuerungsinformationen zu bestimmten Instanzen von Dell Remote Console Switches und Benutzern verwendet wird. Hierbei ist besonders zu beachten, dass jeder Attributtyp und jede Objektklasse, die in AD verwendet werden, eine global eindeutige Kennung besitzen müssen, die als „Object Identifier“ (OID) bezeichnet wird. Diese eindeutigen Kennungen werden in erster Linie von international anerkannten Stellen verwaltet. Im Fall von AD wird das OID-Feld sekundär von Microsoft verwaltet. Dell hat OIDs für die benutzerdefinierten Objektklassen und Attributtypen erhalten, die im erweiterten Dell Schema verwendet werden. Im Folgenden sind die von Dell erhaltenen OIDs zusammenfassend dargestellt:

Dell-Erweiterung ist: dell

Dell BaseOID ist: 1.2.840.113556.1.8000.1280

RCS LinkID-Bereich ist: 12070 bis 12079

Die Produktreihe der Dell Remote Console Switches ist auch dazu ausgelegt, ausschließlich unter Verwendung der Objektklassen zu arbeiten, mit denen AD bereits ausgestattet ist. Diese Option wird als Standardschema bezeichnet. Bei dieser Option werden Dell Remote Console Switches mithilfe der Computer-Objektklasse dargestellt. Das Zuordnen spezifischer Zugriffssteuerungsinformationen zu bestimmten Instanzen von Dell Remote Console Switches und Benutzern erfolgt mithilfe der Standard-Gruppenobjekte. In diesem Fall werden Zugriffssteuerungsinformationen unter einem spezifischen Attributtyp im Gruppenobjekt gespeichert.

Die hierarchischen Strukturen in AD können Ihren Zugriff auf Informationen, die in den Verzeichnisobjekten gespeichert sind, erschweren. Um potenzielle Verzögerungen im Zusammenhang mit der Navigation der Hierarchien zu vermeiden, ist die Produktreihe der Dell Remote Console Switches darauf ausgelegt, einen Aspekt von AD zu verwenden, der als Globaler Katalog (GC) bezeichnet wird. Der GC bietet einen „Schnellsuch"-Dienst, indem Zugriff auf eine Teilmenge der in der gesamten AD-Datenbank gespeicherten Daten bereitgestellt wird und alle Hierarchien und geografischen Verteilungsstrukturen zu einer einfachen, relativ flachen Struktur „zusammengelegt" werden. Zur Abfrage des GC werden dieselben LDAP-Verzeichnisabfragen verwendet, die auch auf die vollständige AD-Datenbank Anwendung finden. Das AD-Produkt erfordert, dass mindestens einer der Domänencontroller in einem Unternehmen für die Bereitstellung von GC-Diensten konfiguriert ist. In Implementierungen von AD können ein oder mehrere bzw. alle Domänencontroller für die Bereitstellung von GC-Diensten konfiguriert sein. Die Produktreihe der Dell Remote Console Switches verwendet DNS für die Bestimmung der Netzwerkkoordinaten jedes GC-Servers, damit die Dell Remote Console Switches Situationen, in denen bestimmte GC-Server nicht im Netzwerk zur Verfügung stehen, problemlos bewältigen können. Zu diesem Zweck werden DNS-SRV-Einträge verwendet, damit die Dell Remote Console Switches immer zuerst versuchen, alternative GC-Server am „nächstgelegenen" Standort zu kontaktieren – in Abhängigkeit von in den SRV-Einträgen konfigurierten Verwaltungseinstellungen.

Standardschema im Vergleich zum erweiterten Dell Schema

Um größtmögliche Flexibilität in einer Vielzahl von Kundenumgebungen zu ermöglichen, stellt Dell eine Gruppe von Objekten zur Verfügung, die vom Benutzer in Abhängigkeit von den gewünschten Resultaten konfiguriert werden kann. Dell Schemata-Erweiterungen umfassen ein Zuordnungsobjekt, Geräteobjekt und Berechtigungsobjekt. Das Zuordnungsobjekt wird verwendet, um eine Verknüpfung zwischen Benutzern oder Gruppen mit einem bestimmten Set von Berechtigungen für ein oder mehrere SIPs herzustellen. Das Geräteobjekt definiert die einzelnen Remote Console Switches innerhalb der Active Directory-Struktur und das Berechtigungsobjekt ist über Zuordnungsobjekte mit den Geräteobjekten verbunden, um Nutzungsberechtigungen zu vergeben.

Dieses Modell bietet Administratoren größtmögliche Flexibilität bezüglich der verschiedenen Kombinationen von Benutzern, Berechtigungen und SIPs am Remote Console Switch, ohne viel zusätzliche Komplexität zu verursachen.

Vor Installation der Dell Schemata-Erweiterungen sollten Administratoren die Beschreibungen und Anweisungen in diesem Kapitel gründlich lesen, um herauszufinden, welches Schema am besten für ihre jeweilige Installation geeignet ist. Die Veränderung eines Schemaobjekts bringt seine entsprechende Verbreitung im Active Directory mit sich, d. h., das Objekt kann nach seiner Erstellung nicht mehr gelöscht, sondern lediglich deaktiviert werden. Aus diesem Grund müssen die Vorteile von Änderungen am Schema sorgfältig abgewogen werden, bevor Änderungen vorgenommen werden.

Der wichtigste Vorteil einer Installation der Dell Schemata-Erweiterungen ist die Vereinfachung des Systems: Bei Verwendung des Active Directory-Standardschemas entspricht ein Remote Console Switch am ehesten einem Computer-Geräteobjekt und wird daher als solches konfiguriert. Der Remote Console Switch ist jedoch kein Computer. Aus diesem Grund können nicht alle Schemafunktionen angewendet werden. Bei der Konfiguration eines Remote Console Switches, der auf diese Weise zugewiesen wurde, muss daher mit besonderer Sorgfalt vorgegangen werden.

Darüber hinaus erleichtert die Verwendung der Dell Schemata-Erweiterungen die Suche nach und die Identifizierung von Geräten am Switch. Bei der Suche nach einem Switch, der mithilfe eines Computer-Geräteobjekts konfiguriert wurde, schließt die Suche alle Computergeräte innerhalb der Active Directory-Struktur ein.

Der Remote Console Switch kann die Authentifizierung gleichermaßen gut unter Verwendung beider Schemata durchführen. Bei beiden Methoden stehen sämtliche Funktionen zur Verfügung. Die Entscheidung, welche Methode innerhalb der jeweiligen Installation zu bevorzugen ist, bleibt dem Administrator überlassen. Im Folgenden werden Anweisungen für Installationen mit und ohne Dell Schemata-Erweiterungen gegeben. Abschnitte und Anweisungen, die sich nur auf ein bestimmtes Schema beziehen, sind entsprechend gekennzeichnet und können bei Installationen, auf die sie nicht zutreffen, übergangen werden.

Standardinstallation

Folgende Schritte müssen durchgeführt werden, damit ein Dell Remote Console Switch zur Authentifizierung Active Directory verwenden kann:

1. Konto für „Admin umgehen“ konfigurieren
2. DNS-Einstellungen konfigurieren
3. Network Time Protocol (NTP) einstellen
4. Authentifizierungsparameter konfigurieren
5. Gruppenobjekte konfigurieren
6. CA-Root-Zertifikat erstellen und herunterladen
7. Login-Timeout einstellen

Konto für „Admin umgehen“ konfigurieren

Falls ein Netzwerkfehler auftritt, wird ein Konto zur Verfügung gestellt, das unabhängig davon verwendet werden kann, ob die Einheit die Authentifizierung anhand eines LDAP-Servers durchführen kann. Dieses Konto sollte vor der Konfiguration aller anderen Einstellungen konfiguriert werden.

HINWEIS: Sie müssen als Benutzer „Admin“ (kein Kennwort) angemeldet sein, um diesen Vorgang durchzuführen.

So konfigurieren Sie das Konto für „Admin umgehen“ über die integrierte Weboberfläche:

1. Klicken Sie auf das Register **Konfigurieren** und dann auf **Benutzer – Admin umgehen**.
2. Geben Sie den Benutzernamen und das Kennwort ein, die Sie dem Benutzer zuweisen möchten, und bestätigen Sie das Kennwort durch die erneute Eingabe im Feld **Kennwort bestätigen**.
3. Klicken Sie auf **Speichern**.

Konfigurieren von DNS-Einstellungen

Bevor der LDAP-Client Namen auflösen kann, muss mindestens ein DNS-Server angegeben werden.

Die Unterkategorie **Netzwerk** zeigt den Namen des Remote Console Switches an und ermöglicht die Änderung von Netzwerkeinstellungen wie **IP-Adresse**, **Subnetzmaske**, **Gateway**, **LAN-Geschwindigkeit** und **DHCP/BootP**-Einstellung. Der für den Remote Console Switch angezeigte Name entspricht dem Namen, der im Feld **Systemname** der **SNMP**-Kategorie vergeben wurde.

Die Unterkategorie **Netzwerk** ermöglicht die Eingabe und die Wartung von bis zu drei DNS-Servern. Diese DNS-Server werden für die Auflösung von DNS-Namen verwendet, die in der Anzeige für die LDAP-Authentifizierung bereitgestellt werden.

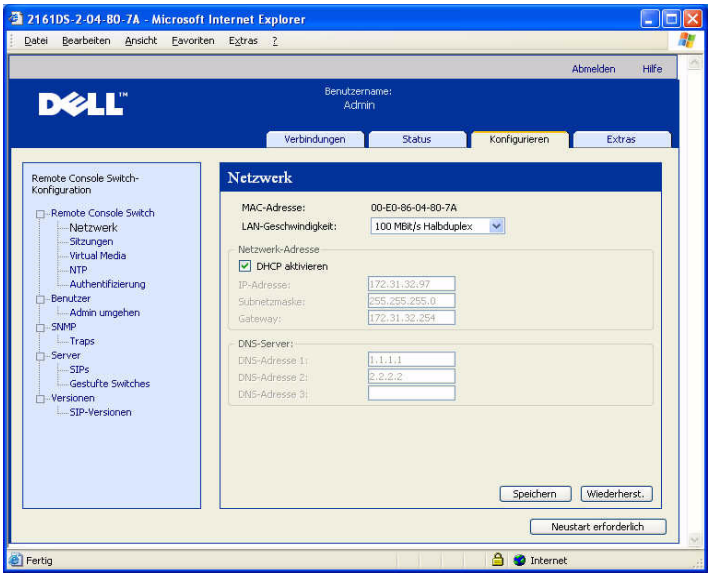
HINWEIS: Mindestens ein DNS-Server muss konfiguriert sein, um die LDAP-Funktion anwenden zu können.

HINWEIS: Sie können die DNS-Serveradressen auch über die serielle Verwaltungsoberfläche der Einheit einrichten. Weitere Informationen zur Verwendung der seriellen Verwaltungsoberfläche finden Sie in der Produktdokumentation zu Ihrer Einheit.

So konfigurieren Sie die DNS-Einstellungen über die integrierte Weboberfläche:

1. Klicken Sie auf das Register **Konfigurieren** und dann auf **Remote Console Switch – Netzwerk**.
2. Legen Sie die DNS-Einstellungen fest und klicken Sie auf **Speichern**.

Abbildung 8-1. Integrierte Weboberfläche – Unterkategorie „Netzwerk“



Konfigurieren der NTP-Einstellungen (Network Time Protocol)

Der Switch muss Zugang zur aktuellen Uhrzeit haben, um die Gültigkeit von Zertifikaten überprüfen zu können. Sie können den Switch so konfigurieren, dass die aktualisierte Zeit vom Netzwerkzeitserver (NTP) abgefragt wird.

So konfigurieren Sie die NTP-Einstellungen über die integrierte Weboberfläche:

1. Klicken Sie auf das Register **Konfigurieren** und dann auf **Remote Console Switch – NTP**.
2. Klicken Sie auf das Kontrollkästchen **NTP aktivieren**.
3. Geben Sie den Namen Ihrer Netzwerkzeitquelle in die entsprechenden Felder ein. Sie müssen außerdem ein Stundenintervall angeben, das festlegt, wie oft die aktuelle Zeit abgefragt wird. Wenn das Intervall auf „0“ eingestellt ist, wird die Abfrage nur beim Hochfahren der Einheit oder bei Änderungen am Menü **Global – NTP** durchgeführt.
4. Klicken Sie auf **Speichern**.

Konfigurieren der LDAP-Authentifizierungsparameter

In der Anzeige für die **Authentifizierung** können Sie die Konfigurationsparameter für Authentifizierung und Autorisierung konfigurieren. Sie können den Benutzernamen, das Kennwort und andere Informationen an den Remote Console Switch senden, der dann mithilfe von LDAP-Daten aus dem Verzeichnisdienst abruft, um die Berechtigungen des jeweiligen Benutzers zu bestimmen.

LDAP-Authentifizierung aktivieren

Im Feld **Authentifizierungseinstellungen** können Sie zwischen lokaler und LDAP-Authentifizierung wählen. Markieren Sie das Kontrollkästchen **LDAP-Authentifizierung verwenden**, damit die Authentifizierung anhand des für LDAP aktivierten Verzeichnisdiensts durchgeführt wird.

Sobald LDAP aktiviert ist, sollten RCS- und Root-Domänen in den vorgesehenen Feldern zugewiesen werden.

Authentifizierungsparameter eingeben

Wenn Sie vorhaben, das erweiterte Dell Schema zu installieren, geben Sie nur die RCS- und Root-Domänen ein, die verwendet werden sollen.

Wenn Sie das erweiterte Dell Schema nicht verwenden, werden die RCS-Switches und zugriffsgesteuerten SIPs Ihrer Installation in Active Directory als Computerobjekte konfiguriert. Zu diesem Zweck müssen Sie zunächst eine Organisationseinheit (OU) konfigurieren, die Gruppenobjekte beinhaltet, welche die Verbindung zwischen Benutzern und zugriffsgesteuerten Remote Console Switches und ihren angeschlossenen SIPs herstellen. Diese Funktion kann von einer bereits vorhandenen oder einer speziell zu diesem Zweck erstellten OU übernommen werden. Sie muss jedoch innerhalb der OU-Objekte in der Gruppen-Container-Domäne einzigartig sein.

Wählen Sie nun ein Attribut innerhalb des LDAP-Verzeichnisses, das freigegebene Zugriffssteuerungsinformationen enthalten soll. Dieses Attribut sollte noch nicht benutzt worden sein und Zeichenkettenwerte speichern können. (Standardmäßig ist dafür das Attribut „Info“ des Gruppenobjekts vorgesehen.)

Abschließend müssen Sie den Speicherort für den **Gruppen-Container**, die **Gruppen-Container-Domäne** und das **Attribut für Zugriffskontrolle** in die entsprechenden Felder im Fenster **Global – Authentifizierung** eingeben.

Detaillierte Beschreibungen der Felder in der Authentifizierungsanzeige finden Sie unter Tabelle 8-1.

So greifen Sie auf die Anzeige für die **Authentifizierung** über die integrierte Weboberfläche zu:

Klicken Sie auf das Register **Konfigurieren** und dann auf **Remote Console Switch – Authentifizierung**.

Abbildung 8-2. Integrierte Weboberfläche – Anzeige für lokale/LDAP-Authentifizierung und Parameter

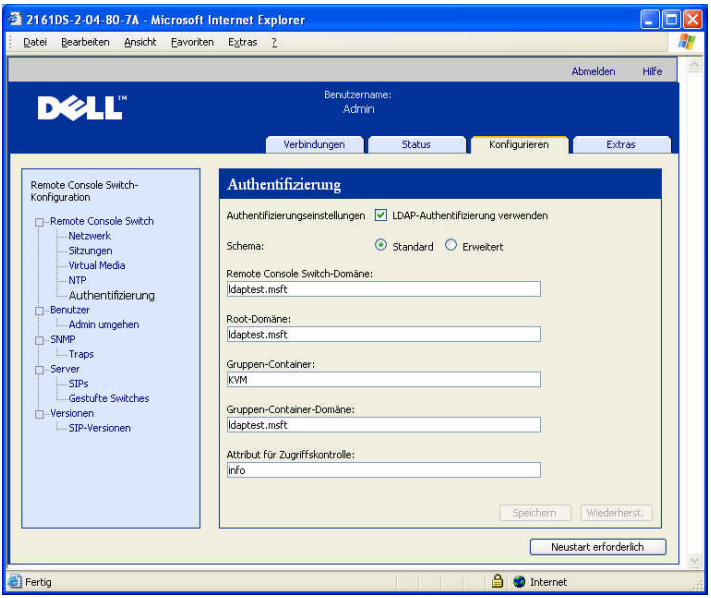


Tabelle 8-1. Beschreibung der Felder in der Authentifizierungsanzeige

Feld	Beschreibung
Authentifizierungseinstellungen	Benutzer können bestimmen, dass die Authentifizierung über LDAP erfolgen soll, indem dieses Kontrollkästchen markiert wird. Der Benutzer kann sich weiterhin über das Konto „Admin umgehen“ anmelden, falls die LDAP-Server nicht zur Verfügung stehen.
Schema	Optionsfeld, das anzeigt, welche Active Directory (AD)-Objektklassen für die Speicherung von Autorisierungsinformationen verwendet werden. Im vorgegebenen Standardschema werden Microsoft Active Directory-Objekte verwendet. Bei Verwendung des erweiterten Schemas werden zusätzliche Dell Objektklassen hinzugefügt.
RCS-Domäne	Das Feld „RCS-Domäne“ enthält den Namen der Active Directory-Domäne, die dazu bestimmt wurde, alle Objekte zu umfassen, die Remote Console Switches und SIPs darstellen.
Root-Domäne	Die oberste Domäne innerhalb der Active Directory – Gesamtstruktur.
Gruppen-Container (nur Standard-schema-Set)	Dieses Feld ist verfügbar, wenn das Standardschema ausgewählt wurde. Es enthält einen Teil des „Distinguished Name“ (DN) eines Organisationseinheiten (OU)-Objekts in Active Directory. In der OU werden Gruppenobjekte zusammengefasst, die einen Bezug zwischen Benutzern und zugriffsgesteuerten Remote Console Switches sowie ihren angeschlossenen SIPs herstellen. Wenn der Distinguished Name der ausgewählten OU beispielsweise folgendermaßen lautet: ou=KVM-AccessControls,dc=MyCom,dc=com, sollte das Gruppen-Container-Feld auf „KVM-Zugriffssteuerungen” eingestellt werden. Der im Gruppen-Container-Feld eingegebene Name muss innerhalb der OU-Objekte in der Gruppen-Container-Domäne eindeutig sein. Sie können eine bereits vorhandene OU für den Gruppen-Container verwenden oder eine neue OU speziell zu diesem Zweck erstellen. Der standardmäßige Gruppen-Container ist KVM.
Gruppen-Container-Domäne (nur Standard-schema-Set)	Dieses Feld ist verfügbar, wenn das Standardschema ausgewählt wurde, und enthält den DNS-Namen der Active Directory-Domäne, in der sich der Gruppen-Container befindet.

Attribut für Zugriffskontrolle (nur Standard-schema-Set)	Der Wert in diesem Feld gibt an, welches Attribut im LDAP-Verzeichnis freigegebene Zugriffssteuerungsinformationen enthalten soll. Das Feld ist nur verfügbar, wenn das Standardschema ausgewählt wurde. Das **Attribut für Zugriffskontrolle** wird aus den Attributen in dem LDAP-Verzeichnisobjekt ausgewählt, das die Gruppe darstellt, deren Mitgliedsliste sowohl den Benutzer als auch die Einheit bzw. den angeschlossenen Computer enthält, auf die/den Sie zugreifen wollen. Bei Verwendung des Standardschemas ist es erforderlich, dass Gruppenobjekte im Gruppen-Container über ein Attribut verfügen, das die der Gruppe zugeordnete Berechtigungsstufe enthalten soll. Das Feld „Attribut für Zugriffskontrolle“ ist verfügbar, wenn das Standardschema ausgewählt wurde, und enthält den Namen des gewählten Attributs. Das gewählte Attribut muss einen Zeichenkettenwert speichern können. Das Standardattribut ist beispielsweise „Info“, ein Attribut, auf das über das Snap-In „Active Directory-Benutzer und -Computer“ (ADUC) zugegriffen werden kann. Unter Verwendung von ADUC wird der Wert des Info-Attributs eingestellt, indem auf die Eigenschaft „Anmerkungen“ des Gruppenobjekts zugegriffen wird.

LDAP-SSL-Zertifikate

Sämtlicher LDAP-Protokollaustausch (zwischen einem Remote Console Switch und Active Directory-Servern) ist durch SSL gesichert. Das durch SSL gesicherte LDAP-Protokoll wird als LDAPS (Lightweight Directory Access Protocol over SSL) bezeichnet. Jede LDAPS-Verbindung beginnt mit einem Protokoll-Handshake, der die Übertragung des Sicherheitszertifikats vom entsprechenden Active Directory-Server zum Remote Console Switch veranlasst. Nach Empfang des Zertifikats ist es die Aufgabe des Remote Console Switches, dessen Gültigkeit zu überprüfen. Um das Zertifikat überprüfen zu können, muss die Einheit mit einer Kopie des Root-Zertifikats der Zertifizierungsstelle (CA) konfiguriert werden. Zu diesem Zweck muss das Zertifikat zunächst erstellt werden.

SSL auf einem Domänencontroller aktivieren

Wenn Sie die Microsoft Enterprise Root CA verwenden wollen, um automatisch sämtlichen Domänencontrollern SSL-Zertifikate zuzuweisen, müssen Sie die folgenden Schritte ausführen, um SSL auf allen Domänencontrollern zu aktivieren (falls noch nicht geschehen).

1. Installieren Sie eine Microsoft Enterprise Root CA auf einem Domänencontroller.
   a. Wählen Sie **Start – Systemsteuerung – Software**.
   b. Wählen Sie **Windows-Komponenten hinzufügen/entfernen** aus.
   c. Markieren Sie im Assistenten für Windows-Komponenten das Kontrollkästchen **Zertifikatdienste**.
   d. Wählen Sie **Enterprise Root CA** als CA-Typ und klicken Sie auf **Weiter**.
   e. Geben Sie den allgemeinen Namen für diese CA ein, klicken Sie auf **Weiter** und dann auf **Fertigstellen**.
2. Aktivieren Sie SSL auf sämtlichen Domänencontrollern, indem Sie ein SSL-Zertifikat für jeden Controller installieren.
   a. Klicken Sie auf **Start – Verwaltung – Sicherheitsrichtlinie für Domänen**.
   b. Erweitern Sie den Ordner „Richtlinien öffentlicher Schlüssel“, klicken Sie mit der rechten Maustaste auf **Einstellungen der automatischen Zertifikatanforderung** und klicken Sie auf **Automatische Zertifikatanforderung**.
   c. Klicken Sie im Assistenten für automatische Zertifikatsanforderung auf **Weiter** und wählen Sie **Domänencontroller** aus.
3. Klicken Sie auf **Weiter** und dann auf **Fertigstellen**.

Eine Datei mit einem Zertifikat/einem privaten Schlüssel kann mithilfe von openssl und Linux erstellt werden. Openssl kann von **openssl.org** heruntergeladen werden. Wenn in den nachstehenden Anweisungen Text in <> angegeben ist, bedeutet dies, dass der Benutzer anhand der Kriterien am Ende dieser Zeile einen Wert festlegen muss.

So erstellen Sie ein zu importierendes Zertifikat:

1. Geben Sie an der Linux-Eingabeaufforderung „openssl“ ein und betätigen Sie die Eingabetaste. Der Benutzer befindet sich nun in der OpenSSL-Eingabeaufforderung.

   OpenSSL> genrsa -out privatekey.pem <512>

   Generating RSA private key, 512 bit long modulus

   .....++++++++++++

   .....++++++++++++

   e is 65537 (0x10001)

   OpenSSL> req -new -key privatekey.pem -x509 -out certificate.pem-batch -days <365>

2. Geben Sie die Informationen ein, die in Ihre Zertifikatanfrage im Distinguished Name oder DN aufgenommen werden. Für einige Felder ist möglicherweise ein Standardwert vorhanden. Wenn Sie möchten, können Sie '.' eingeben, um ein Feld leer zu lassen.

   Country Name (2 letter code) [GB]:<US>

   State or Province Name (full name) [Berkshire]:<Texas>

   Locality Name (eg, city) [Newbury]:<Austin>

   Organization Name (eg, company) [My Company Ltd]:<Dell, Inc.>

   Organizational Unit Name (eg, section) []:<Round Rock>

   Common Name (eg, your name or your servershostname)[]:<Appliance DNSNameorIP>

   Email Address []:<support@dell.com>

   OpenSSL> quit

3. Geben Sie an der Linux-Eingabeaufforderung catcertificate.pemprivatekey.pem > webserver.pem'einundkonvertierenSiedieDateidannvomUNIX-ZeilenvorschubindenDOS-Zeilenumbruch/-Zeilenvorschub,indemSie'unix2doswebserver.pem'eingeben.'

So exportieren Sie das CA-Zertifikat:

1. Öffnen Sie das Verwaltungstool für Zertifizierungsstellen (CA) im Windows-Betriebssystem:
   Start – Alle Programme – Verwaltung – Zertifizierungsstelle.
2. Sie können die Eigenschaften der Zertifizierungsstelle anzeigen, indem Sie mit der rechten Maustaste auf die entsprechende Zertifizierungsstelle im Baumdiagramm klicken und **Eigenschaften** auswählen. Das Dialogfeld „Eigenschaften der Zertifizierungsstelle“ wird angezeigt.
3. Klicken Sie auf das Register **Allgemein** und die Schaltfläche **Zertifikat anzeigen**, um das Dialogfeld „Zertifikat“ zu öffnen.
4. Klicken Sie auf das Register **Details** und dann auf die Schaltfläche **In Datei kopieren**. Der Zertifikatexport-Assistent wird gestartet.
5. Klicken Sie auf **Weiter**, um den Assistenten zu verwenden.
6. Wählen Sie auf der Seite „Exportdateiformat“ das Optionsfeld **Base-64-codiertes X.509-Zertifikat (.CER)** aus und klicken Sie auf **Weiter**.
7. Geben Sie einen Dateinamen und Pfad für das exportierte Zertifikat ein bzw. durchsuchen Sie die Verzeichnisstruktur nach einem entsprechenden Dateinamen und Pfad. Klicken Sie auf die Schaltfläche **Weiter**.
8. Klicken Sie auf die Schaltfläche **Fertigstellen**.

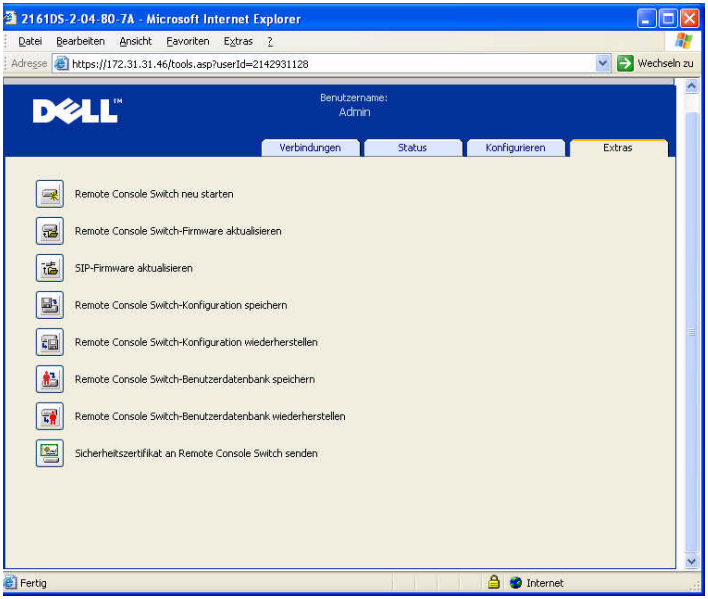
Die aus diesem Vorgang resultierende Zertifikatsdatei ist ordnungsgemäß formatiert und kann von OpenSSL gelesen werden.

Im Allgemeinen ist es ausreichend, das CA-Zertifikat einmal zu laden; es muss allerdings erneut geladen werden, wenn das Zertifikat gesperrt wird, abläuft oder die Option **Werkseitige Standardeinstellungen wiederherstellen** im Menü der seriellen Konsole ausgewählt wird.

HINWEIS: Die Anweisungen oben gelten für Microsoft Root-CA-Zertifikate. Informationen bezüglich anderer CAs erhalten Sie vom entsprechenden Anbieter.

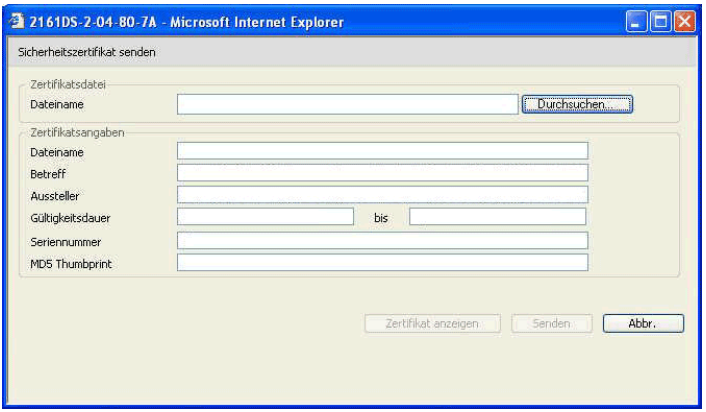
HINWEIS: Das Network Time Protocol (NTP) muss aktiviert sein, damit LDAPS funktionieren kann.

Abbildung 8-3. Integrierte Weboberfläche – Sicherheitszertifikat senden



Nach dem Senden des Sicherheitszertifikats wird das folgende Fenster angezeigt.

Abbildung 8-4. Integrierte Weboberfläche – Zertifikat senden



Schaltfläche	Beschreibung
Durchsuchen	Ermöglicht das Navigieren zu einer Zertifikatsdatei, indem ein Dialogfeld zur Dateiauswahl geöffnet wird und der Benutzer eine Zertifikatsdatei auswählen kann.
Zertifikat anzeigen	Zeigt das aktuelle Zertifikat des Remote Console Switches an.
Senden	Sendet das Zertifikat an den Remote Console Switch.
Abbrechen	Schließt das Dialogfeld.

Sie können die Verzeichnisstruktur nach einem Zertifikat durchsuchen und das Zertifikat öffnen. Wenn das Zertifikat geöffnet ist und sein Inhalt angezeigt wird, kann der Benutzer das Zertifikat an die Einheit senden.

Feld	Beschreibung
Datei	Pfad und Name der Zertifikatsdatei, die mit der Schaltfläche „Durchsuchen“ (Dateiauswahl) geöffnet wurde.
Betreff	Betreff des geöffneten Zertifikats.
Aussteller	Person oder Instanz, die das Zertifikat ausgestellt hat.
Gültigkeitsdauer	Zeitraum, für den das Zertifikat gültig ist.
Seriennummer	Seriennummer des Zertifikats.
SHA-1 Thumbprint	Vom Zertifikat abgeleiteter SHA-1 Thumbprint.
MD5 Thumbprint	Vom Zertifikat abgeleiteter MD5 Thumbprint.

Login Timeout

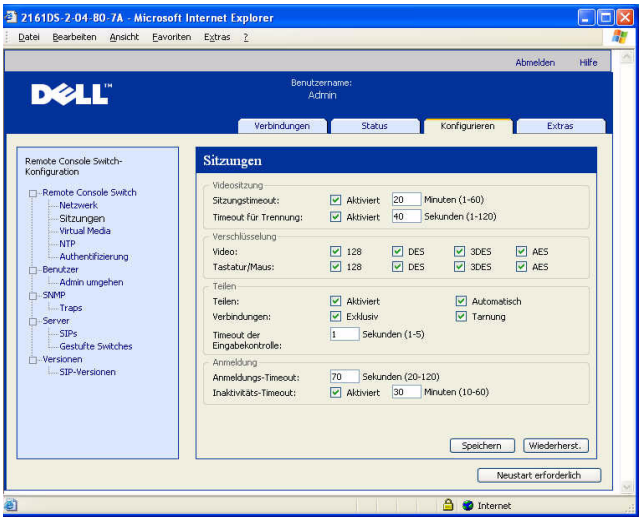
Falls eine derart umfangreiche Verzeichnisstruktur vorhanden ist, dass die LDAP-Authentifizierung nur langsam durchgeführt werden kann, stellt das Fenster „Sitzungen“ eine Login-Timeout-Funktion mit einem Standard-Timeout von 30 Sekunden zur Verfügung. Das Login-Timeout ist der Zeitraum zwischen dem Betätigen des Schaltfläche **OK** im Anmeldedialogfenster durch den Benutzer und dem Zeitpunkt, bis zu dem die Einheit reagiert haben muss. Die Einheit verwendet diesen Wert außerdem dazu, das Timeout für eine LDAP-Authentifizierungsanforderung zu bestimmen.

So legen Sie das Login-Timeout über die integrierte Weboberfläche fest:

1. Klicken Sie auf das Register **Konfigurieren** und dann auf **Remote Console Switch – Sitzungen**.
2. Geben Sie die Anzahl von Sekunden im Menü **Login-Timeout** ein.

3 Klicken Sie auf **Speichern**.

Abbildung 8-5. Integrierte Weboberfläche – Login-Timeout



Anzeigen von CA-Zertifikatsinformationen

Der Remote Console Switch kann in diesem Fenster nur dann vollständige CA-Zertifikatsinformationen anzeigen, wenn der öffentliche Schlüssel kleiner oder gleich 2048 Bit ist. Wenn der Schlüssel mehr als 2048 Bit umfasst, werden die Daten zu Betreff, Aussteller und Gültigkeitsdauer unvollständig dargestellt.

Die folgende Anzeige ist ein Beispiel für CA-Zertifikatsinformationen:

1 Laden Sie das CA-Zertifikat vom Client auf die Einheit.

2 Geben Sie im Hauptmenü der seriellen Konsole Option 8 ein, um das LDAP CA-Zertifikat anzuzeigen.

Die Einheit zeigt die folgenden Informationen an:

```
Begin CA certificate information display
subject= /DC=msft/DC=ldaptest/CN=MyCertificate
issuer= /DC=msft/DC=ldaptest/CN=MyCertificate
notBefore=Dec 7 20:09:56 2005 GMT
notAfter=Dec 7 20:18:34 2010 GMT
serial=7BA146C0221A08B447B989292074329F
```

```
MD5 Fingerprint=
CB:6D:70:30:31:E5:1B:C0:90:BB:DB:32:B2:C9:D1:5A
End CA certificate information display
```

Führen Sie die Schritte der folgenden Anweisungen durch, um die Installation der RCS Software auf Microsoft Windows Server 2003 Plattformen zu ermöglichen:

1. Öffnen Sie das **Start**-Menü.
2. Klicken Sie mit der rechten Maustaste auf **Arbeitsplatz** und wählen Sie **Eigenschaften** aus.
3. Klicken Sie auf das Register **Erweitert**.
4. Klicken Sie auf die Schaltfläche **Leistungseinstellungen**.
5. Wählen Sie das Register **Datenausführungsverhinderung** aus.
6. Wählen Sie die Schaltfläche **Datenausführungsverhinderung nur für erforderliche Windows-Programme und -Dienste aktivieren** aus.
7. Klicken Sie auf **OK**.
8. Klicken Sie im Dialogfeld „Systemeigenschaften“ erneut auf **OK**.

Konfigurieren von Gruppenobjekten

Die Zugriffssteuerung wird auf ein bestimmtes Active Directory-Benutzerkonto angewendet, indem dieser Benutzer in die Mitgliedsliste einer Gruppe im Gruppen-Container aufgenommen wird. Die Mitgliedsliste der Gruppe muss außerdem die Objekte enthalten, die den/die Remote Console Switch(es) und SIP(s) darstellen, für die der Benutzer Zugriffsberechtigungen besitzt. Die gewährte Zugriffsebene wird durch den Wert eines spezifischen Attributs im Gruppenobjekt (Standardschema) bzw. im Zuordnungsobjekt (erweitertes Schema) bestimmt. Es stehen drei Berechtigungsstufen mit zunehmenden Zugriffsrechten zur Verfügung: „KVM-Benutzer“, „KVM-Benutzeradministrator“ und „KVM-Einheitenadministrator“, wobei letzterer über die höchsten Zugriffsrechte verfügt.

HINWEIS: Wenn die Zugriffsebene „KVM-Benutzer“ nicht verwendet wird, müssen SIP-Objekte nicht konfiguriert werden, da beide Administratortypen standardmäßig Zugriffsrechte für alle SIPs haben.

Tabelle 8-2. LDAP (Gruppenattribut-Autorisierung)

Vorgang	KVM-Einheitenadministrator	KVM-Benutzeradministrator	KVM-Benutzer
Trennen	Darf einen anderen Einheitenadministrator oder einen Benutzer-administrator trennen. Die Berechtigung muss für jedes Zielgerät (Target Device, TD) konfiguriert werden, indem das TD in das entsprechende Gruppenobjekt im Verzeichnis aufgenommen wird.	Darf einen anderen Benutzeradministrator trennen. Die Berechtigung muss für jedes Zielgerät konfiguriert werden, indem das Zielgerät in das entsprechende Gruppenobjekt im Verzeichnis aufgenommen wird.	Nein
Netzwerk-parameter und globale Einstellungen konfigurieren	Ja. – Die Berechtigung muss für jede Einheit konfiguriert werden, indem die Einheit in das entsprechende Gruppenobjekt im Verzeichnis aufgenommen wird.	Nein	Nein
Neustart durchführen	Ja. – Die Berechtigung muss für jede Einheit konfiguriert werden, indem die Einheit in das entsprechende Gruppenobjekt im Verzeichnis aufgenommen wird.	Nein	Nein
FLASH-Aktualisierung	Ja. – Die Berechtigung muss für jede Einheit konfiguriert werden, indem die Einheit in das entsprechende Gruppenobjekt im Verzeichnis aufgenom-men wird.	Nein	Nein

Benutzer-konten verwalten	Ja. – Die Berechtigung muss für jede Einheit konfiguriert werden, indem die Einheit in das entsprechende Gruppenobjekt im Verzeichnis aufgenom-men wird.	Ja. – Die Berechtigung muss für jede Einheit konfiguriert werden, indem die Einheit in das entsprechende Gruppenobjekt im Verzeichnis aufgenommen wird.	Nein
Port-Einstell-ungen konfigurieren	Ja. – Die Berechtigung muss für jede Einheit konfiguriert werden, indem die Einheit in das entsprechende Gruppenobjekt im Verzeichnis aufgenom-men wird.	Ja. – Die Berechtigung muss für jede Einheit konfiguriert werden, indem die Einheit in das entsprechende Gruppenobjekt im Verzeichnis aufgenommen wird.	Nein
Auf Zielgerät zugreifen	Ja. – Die Berechtigung muss für jede Einheit konfiguriert werden, indem die Einheit in das entsprechende Gruppenobjekt im Verzeichnis aufgenom-men wird.	Ja. – Die Berechtigung muss für jede Einheit konfiguriert werden, indem die Einheit in das entsprechende Gruppenobjekt im Verzeichnis aufgenommen wird.	Ja, wenn entsprechend vom Administrator konfiguriert. Die Berechti-gung muss für jedes Zielgerät (Target Device, TD) konfiguriert werden, indem das TD in das entsprechende Gruppenob-jekt im Verzeichnis aufgenommen wird.

Ein AD-Benutzerkonto muss entsprechend konfiguriert werden, um die Berechtigung vom Einheitenadministrator zu erhalten, Felder in der Authentifizierungsanzeige zu ändern. Insbesondere die Authentifizierungseinstellungen dürfen nur von einem Einheitenadministrator verändert werden.

Überblick über Active Directory-Objekte für das Standardschema

Für jeden der physischen Remote Console Switches im Netzwerk, der zum Zweck der Authentifizierung und Autorisierung in Active Directory eingebunden werden soll, muss mindestens ein Computerobjekt erstellt werden, durch das der Switch darstellt wird. Darüber hinaus müssen Sie ein Computerobjekt für jedes SIP erstellen, das an den RCS angeschlossen ist und über die Berechtigungsstufe „KVM-Benutzer“ gesteuert werden soll. Für die beiden Administratorebenen sind Computerobjekte zur Darstellung von SIPs nicht erforderlich. Benutzer in der KVM-Benutzergruppe haben nur Zugriff auf SIPs, die sich ebenfalls in der KVM-Benutzergruppe befinden. Benutzer mit Administratorrechten haben standardmäßig Zugriff auf alle SIPs.

So richten Sie Gruppenobjekte für einen Remote Console Switch ein:

1. Falls noch nicht geschehen, erstellen Sie die Organisationseinheit, in der die Gruppenobjekte in Verbindung mit Ihrer Switch-Installation enthalten sein sollen.
2. Innerhalb dieser Organisationseinheit erstellen Sie drei Gruppenobjekte, die die Berechtigungsstufen für Benutzer darstellen sollen: jeweils ein Gruppenobjekt für KVM-Einheitenadministratoren, KVM-Benutzeradministratoren und KVM-Benutzer.
3. Unter Verwendung des MSADUC-Tool öffnen Sie das Gruppenobjekt für KVM-Einheitenadministratoren und wählen die Eigenschaft „Anmerkungen“. Geben Sie die Zugriffsebene („KVM-Einheitenadministrator“) für diese Gruppe im Feld „Anmerkungen“ ein und speichern Sie die Einstellung. Wiederholen Sie diesen Schritt für die anderen beiden Gruppenobjekte unter Verwendung der entsprechenden Namen.

HINWEIS: Die einfache Syntax für alle Attributwerte für Zugriffssteuerung ist:

„[<beliebige Textzeichenkette> <Begrenzungszeichen>] < Berechtigungsstufe> [<Begrenzungszeichen> <beliebige Textzeichenkette>]“

Dabei gilt: <Berechtigungsstufe>: = „KVM-Benutzer“ oder „KVM-Benutzeradministrator“ oder „KVM-Einheitenadministrator“

<Begrenzungszeichen>: = ein oder mehr der folgenden Zeichen: <Zeilenvorschub> oder <c/r> oder <Komma> oder <Semikolon> oder <Tabulator>

<beliebige Textzeichenkette> ist eine Kette von alphanumerischen Zeichen und kann eine Nullkette (d. h. leere Zeichenkette) sein.

Eckige Klammern weisen auf optionale Elemente hin; die folgende Vorlage zeigt beispielsweise an, dass die Angabe einer Berechtigungsstufe im Anschluss an eine optionalen Zeichenkette und ein optionales Begrenzungszeichen erforderlich ist: „[<beliebige Textzeichenkette> <Begrenzungszeichen>] < Berechtigungsstufe1>".

4 Erstellen Sie ein Computerobjekt, das den Remote Console Switch darstellt.

5 Erstellen Sie ein Computerobjekt für jedes SIP, das an einen Server angeschlossen ist und dessen Zugriff auf die Berechtigungsstufe „KVM-Benutzer" beschränkt werden soll.

6 Fügen Sie den entsprechenden Gruppenobjekten das Computerobjekt hinzu, das den Switch darstellt.

7 Fügen Sie dem entsprechenden Gruppenobjekt Benutzerobjekte hinzu, um ihre Zugriffsebene festzulegen.

8 Fügen Sie der KVM-Benutzergruppe die Computerobjekte für die zugriffsgesteuerten SIPs hinzu.

Überblick über Active Directory-Objekte für das erweiterte Dell Schema

Für jeden der physischen Remote Console Switches im Netzwerk, der zum Zweck der Authentifizierung und Autorisierung in Active Directory eingebunden werden soll, muss mindestens ein RCS-Geräteobjekt erstellt werden, durch das der physische Switch dargestellt wird, sowie ein Zuordnungsobjekt. Das Zuordnungsobjekt wird verwendet, um eine Verknüpfung zwischen Benutzern oder Gruppen mit einem bestimmten Set von Berechtigungen für ein oder mehrere SIPs herzustellen. Dieses Modell bietet Administratoren größtmögliche Flexibilität bezüglich der verschiedenen Kombinationen von Benutzern, RCS-Berechtigungen und SIPs am Remote Console Switch, ohne viel zusätzliche Komplexität zu verursachen.

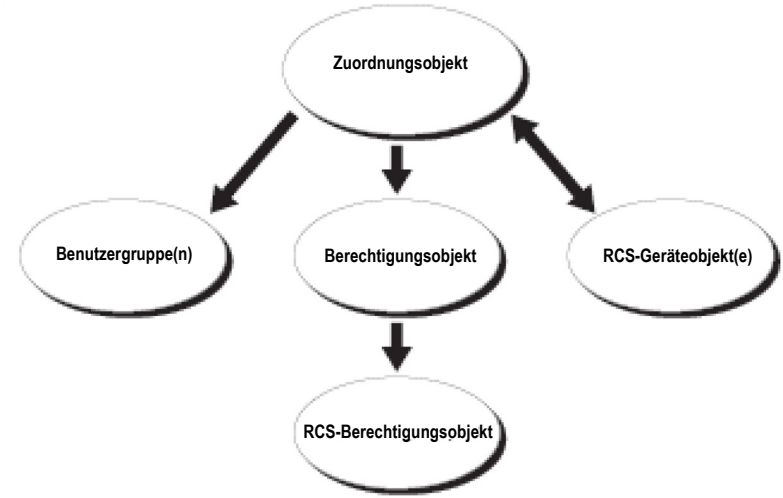
Das RCS-Geräteobjekt stellt die Verknüpfung zum Remote Console Switch für die Abfrage des Active Directory zum Zweck der Authentifizierung und Autorisierung dar. Wenn ein Remote Console Switch zum Netzwerk hinzugefügt wird, muss der Administrator den Remote Console Switch und sein Geräteobjekt mit dem entsprechenden Active Directory-Namen konfigurieren, damit Benutzer die Authentifizierung und Autorisierung über Active Directory durchführen können. Der Administrator muss den Remote Console Switch zudem mindestens einem Zuordnungsobjekt hinzufügen, damit die Benutzerauthentifizierung durchgeführt werden kann.

Sie können beliebig viele Zuordnungsobjekte erstellen und jedes Zuordnungsobjekt kann mit beliebig vielen Benutzern, Benutzergruppen und RCS-Geräteobjekten verknüpft werden. Die Benutzer und RCS-Geräteobjekte können Mitglieder einer beliebigen Domäne im Unternehmen sein.

Allerdings kann jedes Zuordnungsobjekt nur mit einem Berechtigungsobjekt verknüpft sein (bzw. Verknüpfungen von Benutzern, Benutzergruppen oder RCS-Geräteobjekten mit einem Berechtigungsobjekt herstellen). Ein Berechtigungsobjekt gibt einem Administrator die Kontrolle darüber, welche Benutzer über welche Berechtigungen im Hinblick auf bestimmte SIPs verfügen.

In Abbildung 8-6 wird veranschaulicht, dass das Zuordnungsobjekt die Verbindung bereitstellt, die für sämtliche Authentifizierungs- und Autorisierungsvorgänge erforderlich ist.

Abbildung 8-6. Typisches Setup für Active Directory-Objekte

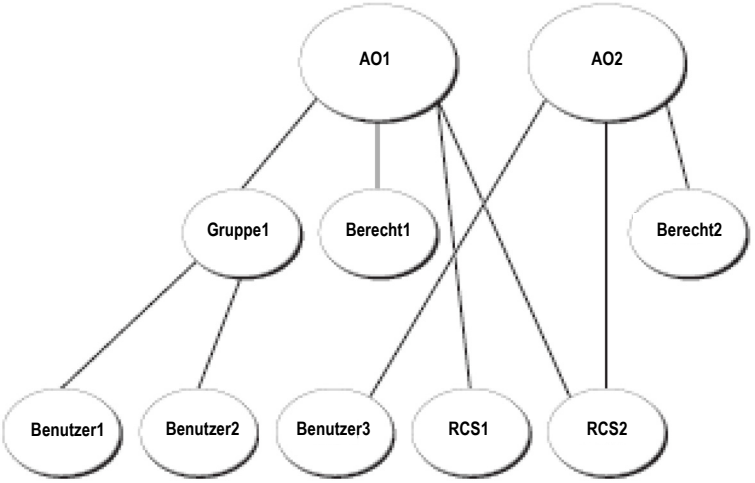


Sie können beliebig viele Zuordnungsobjekte erstellen. Es muss allerdings mindestens ein Zuordnungsobjekt erstellt werden und für jeden Remote Console Switch im Netzwerk, der zum Zweck der Authentifizierung und Autorisierung in Active Directory eingebunden werden soll, muss mindestens ein RCS-Geräteobjekt vorhanden sein. Das Zuordnungsobjekt kann beliebig viele Benutzer und/oder Gruppen sowie RCS-Geräteobjekte enthalten. Das Zuordnungsobjekt verfügt allerdings nur über ein Berechtigungsobjekt pro Zuordnungsobjekt. Das Zuordnungsobjekt verbindet die „Benutzer", die über „Berechtigungen" für die jeweiligen RCSs verfügen.

Darüber hinaus können Sie Active Directory-Objekte in einer Domäne oder in mehreren Domänen einrichten. Beispiel: Sie haben zwei Remote Console Switches (RCS1 und RCS2) und drei bestehende Active Directory-Benutzer (Benutzer1, Benutzer2 und Benutzer3). Sie möchten Benutzer1 und Benutzer2 Administratorrechte für beide Remote Console Switches und Benutzer3 Anmeldeberechtigung für den RCS2 erteilen.

Abbildung 8-7 zeigt, wie die Active Directory-Objekte in diesem Beispiel eingerichtet werden.

Abbildung 8-7. Active Directory-Objekte in einer einzigen Domäne einrichten



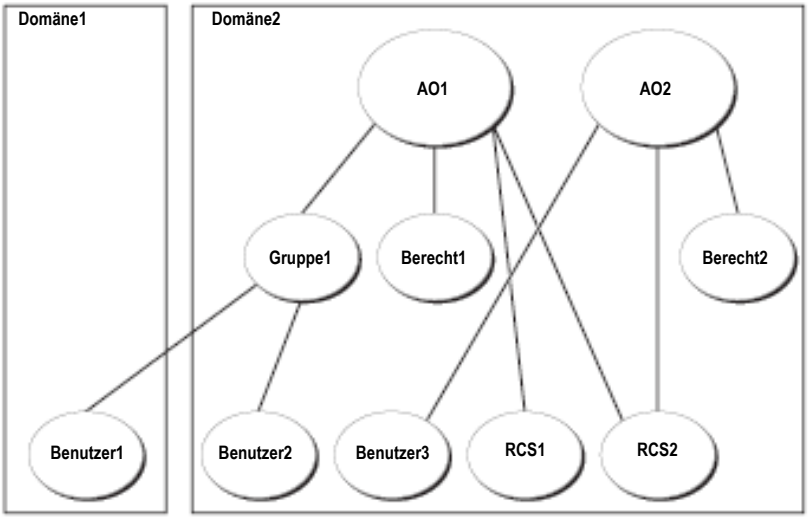
Führen Sie die folgenden Schritte durch, um die Objekte in einer einzigen Domäne einzurichten:

1. Erstellen Sie zwei Zuordnungsobjekte.
2. Erstellen Sie zwei RCS-Geräteobjekte, RCS1 und RCS2, um die beiden Remote Console Switches darzustellen.
3. Erstellen Sie zwei Berechtigungsobjekte, Berecht1 und Berecht2, wobei Berecht1 über alle Berechtigungen (Administrator) und Berecht2 über eine Anmeldeberechtigung verfügt.
4. Fassen Sie Benutzer1 und Benutzer2 in Gruppe1 zusammen.
5. Fügen Sie Gruppe1 als Mitglieder im Zuordnungsobjekt 1 (AO1), Berecht1 als Berechtigungsobjekte in AO1 und RCS1 und RCS2 als RCS-Geräte in AO1 hinzu.
6. Fügen Sie Benutzer3 als Mitglied im Zuordnungsobjekt 2 (AO2), Berecht2 als Berechtigungsobjekt in AO2 und RCS2 als RCS-Gerät in AO2 hinzu.

Detaillierte Anweisungen finden Sie im Abschnitt „Hinzufügen von Remote Console Switch-Benutzern und -Berechtigungen zu Active Directory mithilfe von Dell Schemata-Erweiterungen“.

Abbildung 8-8 zeigt, wie die Active Directory-Objekte in mehreren Domänen eingerichtet werden. In diesem Beispiel haben Sie zwei Remote Console Switches (RCS1 und RCS2) und drei bestehende Active Directory-Benutzer (Benutzer1, Benutzer2 und Benutzer3). Benutzer1 ist in Domäne1; und Benutzer2 und Benutzer3 sind in Domäne2. Sie möchten Benutzer1 und Benutzer2 Administratorrechte für beide Remote Console Switches und Benutzer3 Anmeldeberechtigung für den RCS2 erteilen.

Abbildung 8-8. Active Directory-Objekte in mehreren Domänen einrichten



Führen Sie die folgenden Schritte durch, um die Objekte in mehreren Domänen einzurichten:

1. Stellen Sie sicher, dass die Funktion für die Domänengesamtstruktur sich im einheitlichen Modus oder im Windows 2003-Modus befindet.
2. Erstellen Sie zwei Zuordnungsobjekte, AO1 (mit Bereich „Universal“) und AO2, in einer der Domänen. In der Abbildung sind die Objekte in Domäne2 dargestellt.
3. Erstellen Sie zwei RCS-Geräteobjekte, RCS1 und RCS2, um die beiden Remote Console Switches darzustellen.

4 Erstellen Sie zwei Berechtigungsobjekte, Berecht1 und Berecht2, wobei Berecht1 über alle Berechtigungen (Administrator) und Berecht2 über eine Anmeldeberechtigung verfügt.

5 Fassen Sie Benutzer1 und Benutzer2 in Gruppe1 zusammen. Der Gruppenbereich der Gruppe1 muss auf „Universal“ eingestellt sein.

6 Fügen Sie Gruppe1 als Mitglieder im Zuordnungsobjekt 1 (AO1), Berecht1 als Berechtigungsobjekte in AO1 und RCS1 und RCS2 als RCS-Geräte in AO1 hinzu.

7 Fügen Sie Benutzer3 als Mitglied im Zuordnungsobjekt 2 (AO2), Berecht2 als Berechtigungsobjekt in AO2 und RCS2 als RCS-Gerät in AO2 hinzu.

Konfigurieren von Active Directory mit Dell Schemata-Erweiterungen für den Zugriff auf RCS

Bevor Sie Active Directory für den Zugriff auf Ihren Remote Console Switch verwenden können, müssen Sie die Active Directory-Software und den Remote Console Switch entsprechend konfigurieren, indem Sie die folgenden Schritte in der angegebenen Reihenfolge ausführen:

1 Erweitern Sie das Active Directory-Schema.

2 Erweitern Sie das Snap-In „Active Directory-Benutzer und -Computer“.

3 Fügen Sie Active Directory die RCS-Benutzer und ihre jeweiligen Berechtigungen hinzu.

Active Directory-Schema erweitern (optional)

Durch die Erweiterung des Active Directory-Schemas werden eine Dell Organisationseinheit, Dell Schema-Klassen und -Attribute sowie Beispielberechtigungen und Zuordnungsobjekte hinzugefügt.

HINWEIS: Bevor Sie das Schema erweitern, müssen Sie über Schema-Administratorberechtigungen als Schemamaster im Rahmen der FSMO-Rollen (Flexible Single Master Operation) für die Domänengesamtstruktur verfügen.

Sie können Ihr Schema mithilfe von zwei verschiedenen Methoden erweitern: mithilfe des Dell Schema Extender-Dienstprogramms oder der LDIF-Skriptdatei.

HINWEIS: Bei Verwendung der LDIF-Skriptdatei wird die Dell Organisationseinheit nicht hinzugefügt.

Die LDIF-Dateien und den Dell Schema Extender erhalten Sie unter www.dell.com/support.

Anweisungen zur Verwendung der LDIF-Dateien finden Sie in der Readme-Datei, die sich im LDIF-Dateiverzeichnis befindet. Wenn Sie den Dell Schema Extender zur Erweiterung des Active Directory-Schemas verwenden, führen Sie die Schritte im Abschnitt „Dell Schema Extender verwenden“ durch.

Sie können den Schema Extender oder die LDIF-Dateien von einem beliebigen Speicherort kopieren und ausführen.

Dell Schema Extender verwenden

HINWEIS: Der Dell Schema Extender verwendet die SchemaExtenderOem.ini-Datei. Ändern Sie den Namen dieser Datei nicht, damit sichergestellt ist, dass das Dell Schema Extender-Dienstprogramm ordnungsgemäß funktioniert.

1. Klicken Sie auf dem Willkommen-Bildschirm auf Weiter.
2. Lesen Sie den Warnhinweis und klicken Sie erneut auf Weiter.
3. Wählen Sie entweder die Option Aktuelle Anmeldeberechtigungen verwenden aus oder geben Sie einen Benutzernamen und ein Kennwort mit Schema-Administratorrechten ein.
4. Klicken Sie auf Weiter, um den Dell Schema Extender auszuführen.
5. Klicken Sie auf Fertigstellen.

Dell-Erweiterung für das Snap-In „Active Directory-Benutzer und -Computer“ installieren (optional)

Wenn Sie das Schema in Active Directory erweitern, müssen Sie auch das Snap-In „Active Directory-Benutzer und -Computer“ erweitern, damit der Administrator die Remote Console Switch Geräte, Benutzer und Benutzergruppen, Remote Console Switch-Zuordnungen und SIP-Berechtigungen verwalten kann. Die Dell Erweiterung für das Snap-In „Active Directory-Benutzer und -Computer“ ist eine Option bei der Installation Ihrer Systemmanagementsoftware unter Verwendung der Dell Systems Management Consoles-CD. Weitere Anweisungen für die Installation von Systemmanagementsoftware finden Sie in der Schnellinstallationsanleitung für die Dell OpenManage Software.

HINWEIS: Sie müssen den Administrator Pack auf jedem System installieren, auf dem die Active Directory Remote Console Switch-Objekte verwaltet werden. Die Installation wird im folgenden Abschnitt „Snap-In Active Directory-Benutzer und -Computer öffnen“ beschrieben. Wenn Sie den Administrator Pack nicht installieren, kann das Dell SIP-Objekt im Container nicht angezeigt werden.

HINWEIS: Weitere Informationen über das Snap-In „Active Directory-Benutzer und -Computer“ finden Sie in der entsprechenden Produktdokumentation von Microsoft.

Snap-In Active Directory-Benutzer und -Computer öffnen

Führen Sie die folgenden Schritte durch, um das Snap-In „Active Directory-Benutzer und -Computer“ zu öffnen:

Wenn Sie sich am Domänencontroller befinden, klicken Sie auf **Start – Verwaltung – Active Directory-Benutzer und -Computer**. Wenn Sie sich nicht am Domänencontroller befinden, muss das entsprechende Microsoft Administrator Pack auf Ihrem lokalen System installiert sein. Um dieses Administrator Pack zu installieren, klicken Sie auf **Start – Ausführen**, geben Sie `MMC` ein und betätigen Sie die **Eingabetaste**. Dadurch wird die Microsoft Management Console (MMC) geöffnet.

1. Klicken Sie im Fenster „Konsole 1“ auf **Datei** (bzw. „Konsole“ bei Systemen unter Windows 2000).
2. Klicken Sie auf **Snap-In hinzufügen/entfernen**.
3. Wählen Sie das Snap-In „Active Directory-Benutzer und -Computer“ aus und klicken Sie auf **Hinzufügen**.
4. Klicken Sie auf **Schließen** und auf **OK**.

Hinzufügen von Benutzern und Berechtigungen zu Active Directory mithilfe von Dell Schemata-Erweiterungen

Mit dem von Dell erweiterten Snap-In „Active Directory-Benutzer und -Computer“ können Sie Remote Console Switch-Benutzer und -Berechtigungen durch Erstellen von SIP-Objekten, Zuordnungsobjekten und Berechtigungsobjekten hinzuzufügen. Führen Sie die Schritte im entsprechenden Abschnitt durch, um den jeweiligen Objekttyp hinzuzufügen.

SIP-Objekt erstellen

1. Klicken Sie im MMC-Fenster „Konsolenstamm“ mit der rechten Maustaste auf einen Container.
2. Wählen Sie **Neu – Dell SIP-Objekt**. Das Fenster „Neues Objekt“ wird geöffnet.
3. Geben Sie einen Namen für das neue Objekt ein. Dieser Name muss dem Namen des Remote Console Switches entsprechen, den Sie in Schritt 4 des Abschnitts „Remote Console Switch konfigurieren“ eingeben.
4. Wählen Sie **SIP-Geräteobjekt** aus.
5. Klicken Sie auf **OK**.

Berechtigungsobjekt erstellen

Berechtigungsobjekte müssen in derselben Domäne erstellt werden wie das Zuordnungsobjekt, dem sie zugeordnet sind.

1. Klicken Sie im MMC-Fenster „Konsolenstamm“ mit der rechten Maustaste auf einen Container.
2. Wählen Sie **Neu – Dell SIP-Objekt** aus, um das Fenster „Neues Objekt“ zu öffnen.
3. Geben Sie einen Namen für das neue Objekt ein.
4. Wählen Sie **Berechtigungsobjekt** aus.
5. Klicken Sie auf **OK**.
6. Klicken Sie mit der rechten Maustaste auf das neu erstellte Berechtigungsobjekt und wählen Sie **Eigenschaften** aus.
7. Klicken Sie auf das Register **RCS-Berechtigungen** und wählen Sie die Remote Console Switch-Berechtigungen aus, über die der Benutzer verfügen soll.

Verwendung der Dell Zuordnungsobjekt-Syntax

Bei Verwendung der Syntax für Dell Zuordnungsobjekte werden Objekttypen im Dell LDAP-Schema standardmäßig als Benutzer und Gruppe zugeordnet. Im erweiterten Dell Schema hat Dell eindeutige Objekt-IDs für vier neue Objektklassen hinzugefügt:

- KVM-Einheitenobjekte
- KVM-SIP-Objekte
- Berechtigungsobjekte
- Zuordnungsobjekte

Jede dieser neuen Objektklassen wird aus verschiedenen Kombinationen (Hierarchien) von Active Directory-Standardklassen und eindeutigen Dell Attributtypen definiert. Jeder eindeutige Dell Attributtyp wird mit einer Standardattributsyntax von Active Directory definiert.

Die von Microsoft verwendeten Standardobjektklassen für Active Directory enthalten Benutzer und Gruppe. Die Benutzerklasse bezeichnet im Allgemeinen Active Directory-Objekte, die Informationen zu Einzelobjekten enthalten. Die Gruppenklasse enthält Container zum Verschachteln und Speichern von Informationen, die mehrere Objekte betreffen.

Jedes KVM-Einheitenobjekt stellt einen einzelnen Remote Console Switch innerhalb von Active Directory dar. Da es sich hierbei um Einzelobjekte handelt, werden sie im LDAP standardmäßig als Benutzer und nicht als Gruppen-Objekte eingestuft.

Jedes Berechtigungsobjekt verfügt über eine bestimmte Kombination von Berechtigungen. Jede Kombination wird als separate Einheit betrachtet und ist daher ein Benutzerobjekt und kein Gruppenobjekt.

Ein Zuordnungsobjekt enthält gesammelte Informationen über Berechtigungen von spezifischen Benutzerkonten in Bezug auf eine spezifische Einheit (bzw. mehrere Einheiten) und/oder einen spezifischen SIP (bzw. mehrere SIPs). Benutzerkonten in einem Einheitenobjekt können eine beliebige Kombination der folgenden Eigenschaften enthalten:

- Einzelkonto
- Active Directory-Sicherheitsgruppe für Benutzerkonten
- Mehrere Active Directory-Sicherheitsgruppen für Benutzerkonten

Ähnliches gilt für Einheiten und/oder SIPs innerhalb eines Zuordnungsobjekts. Da Zuordnungsobjekte Sicherheitsgruppen in der gleichen Weise verwenden können, werden sie als Gruppenobjekte definiert.

Zuordnungsobjekt erstellen

Das Zuordnungsobjekt ist von einer Gruppe abgeleitet und muss einen Gruppentyp enthalten. Der Zuordnungsbereich gibt den Sicherheitsgruppentyp für das Zuordnungsobjekt an. Wenn Sie ein Zuordnungsobjekt erstellen, müssen Sie den Zuordnungsbereich wählen, der dem hinzuzufügenden Objekttyp entspricht. Wählen Sie beispielsweise „Universal“ aus, sind die Zuordnungsobjekte nur dann verfügbar, wenn die Active Directory-Domäne mindestens im einheitlichen Modus betrieben wird.

So erstellen Sie ein Zuordnungsobjekt:

1. Klicken Sie im MMC-Fenster „Konsolenstamm“ mit der rechten Maustaste auf einen Container.
2. Wählen Sie **Neu – Dell SIP-Objekt** aus, um das Fenster „Neues Objekt“ zu öffnen.
3. Geben Sie einen Namen für das neue Objekt ein.
4. Wählen Sie **Zuordnungsobjekt** aus.
5. Wählen Sie den Bereich für das Zuordnungsobjekt aus.
6. Klicken Sie auf **OK**.

Objekte zu einem Zuordnungsobjekt hinzufügen

Unter Verwendung des Fensters „Eigenschaften“ für das Zuordnungsobjekt können Sie Benutzer oder Benutzergruppen, Berechtigungsobjekte sowie SIP-Geräte oder SIP-Geräteobjekte zuordnen.

HINWEIS: Im Windows 2000-Modus oder einem höheren Modus müssen Sie Universalgruppen verwenden, um Ihre Benutzer oder SIP-Objekte über Domänen zu erstrecken.

Sie können Gruppen von Benutzern und SIP-Geräten hinzufügen.
Die Erstellung Dell-bezogener Gruppen erfolgt auf die gleiche Art und Weise wie die Erstellung anderer Gruppen.

So fügen Sie Benutzer oder Benutzergruppen hinzu:

1. Klicken Sie mit der rechten Maustaste auf das Zuordnungsobjekt und wählen Sie **Eigenschaften** aus.
2. Wählen Sie das Register **Benutzer** und klicken Sie auf **Hinzufügen**.
3. Geben Sie den Namen des Benutzers oder der Benutzergruppe ein und klicken Sie auf **OK**.

Klicken Sie auf das Register **Berechtigungsobjekt**, um dem Zuordnungsobjekt das Berechtigungsobjekt hinzuzufügen, das die Berechtigungen des Benutzers bzw. der Benutzergruppe bei der Authentifizierung an einem SIP-Gerät definiert.

HINWEIS: Sie können jedem Zuordnungsobjekt nur ein Berechtigungsobjekt hinzufügen.

So fügen Sie ein Berechtigungsobjekt hinzu:

1. Wählen Sie das Register **Berechtigungsobjekte** und klicken Sie auf **Hinzufügen**.
2. Geben Sie den Namen des Berechtigungsobjekts ein und klicken Sie auf **OK**.

Klicken Sie auf das Register **Produkte**, um dem Zuordnungsobjekt ein oder mehrere SIP-Geräte hinzuzufügen. Die zugeordneten Geräte bestimmen die an das Netzwerk angeschlossenen SIP-Geräte, die für die definierten Benutzer oder Benutzergruppen zur Verfügung stehen.

HINWEIS: Sie können einem Zuordnungsobjekt mehrere SIP-Geräte hinzufügen.

So fügen Sie SIP-Geräte oder SIP-Gerätegruppen hinzu:

1. Wählen Sie das Register **Produkte** und klicken Sie auf **Hinzufügen**.
2. Geben Sie den Namen des SIP-Geräts oder der SIP-Gerätegruppe ein und klicken Sie auf **OK**.
3. Klicken Sie im Fenster „Eigenschaften“ auf **Übernehmen** und dann auf **OK**.

Zugriffssicherheit bei Konsolenumleitung

Bei jeder Installation des Remote Console Switches hat der Benutzer die Berechtigung, die integrierte Weboberfläche aufzurufen. Die Funktionalität der integrierten Weboberfläche für einen Benutzer wird durch die Benutzer-Berechtigungsstufe eingeschränkt, die im Remote Console Switch festgelegt ist. LDAP mit Dell Schemata-Erweiterung sorgt für eine zusätzliche Sicherheitsebene bei der Einheitenverwaltung, indem Administratoren die Möglichkeit gegeben wird, den Zugriff von Benutzern auf die integrierte Weboberfläche einzuschränken.

Der Zugriff auf die integrierte Weboberfläche wird nur dann gewährt, wenn diese Berechtigungsstufe für den Benutzer im Register„KVM-Einheitenberechtigungen“ des Dell Berechtigungsobjekts konfiguriert wurde. Mithilfe des Kontrollkästchens zur Konsolenumleitung im Register „KVM-SIP-Berechtigungen“ des Dell Berechtigungsobjekts kann ein Benutzer, der nicht berechtigt ist, die integrierte Weboberfläche zum Starten einer Video Viewer-Sitzung mit einer untergeordneten Gruppe von SIPs aufzurufen, dies über den RCS Client tun. Diese Berechtigungen werden über eine Kombination der Konfigurationsparameter im Dell Berechtigungsobjekt und in den SIP-Objekten festgelegt, die im Dell Zuordnungsobjekt enthalten sind.

Wenn ein Benutzer keinen Zugriff auf die integrierte Weboberfläche haben, jedoch Viewer-Sitzung vom RCS Client starten können soll, führen Sie die folgenden Schritte aus:

1. Erstellen Sie ein Dell SIP-Objekt für jedes SIP, auf das der/die Benutzer zugreifen darf/dürfen.
2. Erstellen Sie ein Active Directory-Benutzerkonto für jeden Benutzer, dessen Zugriff kontrolliert werden soll.
3. Erstellen Sie ein Dell Berechtigungsobjekt. Aktivieren Sie keines der drei Kontrollkästchen im Register „KVM-Einheitenberechtigungen“. Aktivieren Sie das Kontrollkästchen für den Zugriff über die Konsolenumleitung im Register „KVM-SIP-Berechtigungen“.

HINWEIS: Wenn Sie eines der Kontrollkästchen für die KVM-Einheitenberechtigungen *und* das Kontrollkästchen für den Zugriff über die Konsolenumleitung aktivieren, erhalten die in den KVM-Einheitenberechtigungen festgelegten Benutzerberechtigungen Vorrang vor dem Kontrollkästchen für den Zugriff über die Konsolenumleitung und der Benutzer hat weiterhin Zugriff auf die EVA.

4. Erstellen Sie ein Dell Zuordnungsobjekt.
5. Öffnen Sie das Dialogfeld „Eigenschaften“ für das in Schritt 4 erstellte Dell Zuordnungsobjekt.
   a. Fügen Sie alle in Schritt 2 erstellen Benutzerkonten hinzu.
   b. Fügen Sie das in Schritt 3 erstellte Berechtigungsobjekt hinzu.
   c. Fügen Sie das in Schritt 1 erstellte SIP-Objekt hinzu.

Verwenden von Active Directory zur Anmeldung am Remote Console Switch

Sie können Active Directory verwenden, um sich über die Remote Console Switch Software oder die integrierte Weboberfläche am Remote Console Switch anzumelden.

Die Anmeldesyntax ist für alle drei Methoden die gleiche:

<benutzername@domäne> oder <domäne>\x3c benutzername> oder <domäne>/<benutzername> (wobei benutzername eine ASCII-Zeichenkette von 1-256 Byte ist). Weder im Benutzernamen noch im Domänennamen ist die Verwendung von Leerzeichen oder Sonderzeichen (z. B. , / oder @) zulässig.

HINWEIS: Sie können keine NetBIOS-Domänennamen wie „Americas“ angeben, da solche Namen nicht aufgelöst werden können.

HINWEIS: Wenn kein Domänenname enthalten ist, wird die lokale Datenbank im Remote Console Switch für die Authentifizierung des Benutzers verwendet.

Anforderung zur Benennung von Zielgeräten für die LDAP-Implementierung

Sollten Sie die folgende Fehlermeldung erhalten:

```
Fehler bei der Anmeldung. Grund: Zugriff nicht
gestattet aufgrund von Fehlern im Authentifizierungs-
Server.
```

Überprüfen Sie, dass das SIP-Objekt in Active Directory erstellt wurde und sein Name genau mit dem über die OSCAR-Benutzeroberfläche am Console Switch zugewiesenen SIP-Namen übereinstimmt.

Das Dell Standardschema und das erweiterte Dell Schema verwenden in Microsoft Windows Active Directory spezifische Objektklassen, um SIPs darzustellen. Unter den Standardbenennungskonventionen von Microsoft für diese Objektklassen ist die Verwendung von Sonder- oder Leerzeichen nicht möglich. Soll LDAP in einer bestehenden Umgebung eingesetzt werden, in der Zielgerätenamen in SIPs derzeit Leer- oder Sonderzeichen enthalten, müssen diese entsprechend umbenannt werden.

Die Umbenennung eines SIP sollte über die integrierte Weboberfläche oder über die OSCAR-Benutzeroberfläche am Console Switch erfolgen. Danach muss über die Remote Console Switch Software eine Resynchronisation durchgeführt werden. Anweisungen für die Umbenennung eines Zielgerätes in einem SIP finden Sie unter „Zuweisen von Gerätenamen“ auf Seite 51. Hierbei ist zu beachten, dass SIP-Namen in der OSCAR-Benutzeroberfläche mit Leerzeichen versehen werden können, dies jedoch in Active Directory nicht zulässig ist. Benennen Sie SIP-Objekte gemäß den Active Directory-Regeln von Microsoft.

Häufig gestellte Fragen

In Tabelle 8-3 werden häufig gestellte Fragen und Antworten aufgeführt.

Tabelle 8-3. Verwenden des RCS mit Active Directory: FAQ

Kann ich mich unter Verwendung von Active Directory über mehrere Gesamtstrukturen hinweg beim Remote Console Switch anmelden?	Der RCS Active Directory-Abfragealgorithmus unterstützt nur eine Struktur in einer Gesamtstruktur.
Funktioniert die Anmeldung am Remote Console Switch unter Verwendung von Active Directory im gemischten Modus (d. h. auf den Domänencontrollern in der Gesamtstruktur werden unterschiedliche Betriebssysteme ausgeführt, z. B. Microsoft Windows NT® 4.0, Windows 2000 oder Windows Server 2003)?	Ja. Im gemischten Modus müssen sich alle Objekte, die für den Abfrageprozess des Remote Console Switches verwendet werden (unter Benutzern, SIP-Geräteobjekten und Zuordnungsobjekten) in derselben Domäne befinden. Das von Dell erweiterte Snap-In „Active Directory-Benutzer und -Computer“ überprüft den Modus und erteilt Benutzerbeschränkungen, um Objekte im gemischten Modus über mehrere Domänen hinweg erstellen zu können.

Unterstützt die Verwendung des Remote Console Switches mit Active Directory Umgebungen mit mehreren Domänen?	Ja. Die Funktionsebene für die Domänengesamtstruktur muss sich im einheitlichen Modus oder im Windows 2003-Modus befinden. Zusätzlich müssen die Gruppen unter Zuordnungsobjekt, Remote Console Switch-Benutzerobjekten und SIP-Geräteobjekten (einschließlich Zuordnungsobjekt) Universalgruppen sein.
Können sich diese von Dell erweiterten Objekte (Dell Zuordnungsobjekt, Dell Remote Console Switch-Gerät und Dell Berechtigungsobjekt) in unterschiedlichen Domänen befinden?	Das Zuordnungsobjekt und das Berechtigungsobjekt müssen sich in derselben Domäne befinden. Das von Dell erweiterte Snap-In „Active Directory-Benutzer und -Computer“ veranlasst Sie dazu, diese beiden Objekte in derselben Domäne zu erstellen. Andere Objekte können sich in unterschiedlichen Domänen befinden.
Gibt es Beschränkungen für eine SSL-Konfiguration des Domänencontrollers?	Ja. Alle SSL-Zertifikate der Active Directory-Server in der Gesamtstruktur müssen von derselben Root-CA signiert sein, da der Remote Console Switch nur das Laden eines zuverlässigen CA-SSL-Zertifikats erlaubt.

Was kann ich tun, wenn ich mich nicht über die Active Directory-Authentifizierung am Remote Console Switch anmelden kann? Wie ist dieses Problem zu lösen?	Dieses Problem kann wie folgt behoben werden: • Wenn kein Domänenname festgelegt wurde, wird die lokale Datenbank verwendet. Verwenden Sie das Standardkonto für den lokalen Administrator, um sich anzumelden, wenn die AD-Authentifizierung nicht funktioniert. • Vergewissern Sie sich, dass das Kontrollkästchen „Active Directory aktivieren“ (Remote Console Switch Software) bzw. das Kontrollkästchen „LDAP-Authentifizierung verwenden“ (integrierte Weboberfläche) auf der Active Directory-Konfigurationsseite für den Remote Console Switch markiert ist. • Überprüfen Sie, dass die DNS-Einstellung auf der Netzwerk-Konfigurationsseite für den Remote Console Switch korrekt ist. • Überprüfen Sie, dass das Network Time Protocol (NTP) bei mindestens einem der Server aktiviert ist, die auf der NTP-Anzeige angegeben sind. • Überprüfen Sie, dass Sie das Active Directory-Zertifikat von Ihrer Active Directory-Root-CA auf den Remote Console Switch geladen haben. • Überprüfen Sie die Domänencontroller-SSL-Zertifikate, um sicherzustellen, dass sie nicht abgelaufen sind. • Überprüfen Sie, dass Ihre Angaben für „Remote Console Switch-Name“, „Root-Domänenname“ und „Remote Console Switch-Domänenname“ mit der Konfiguration für Ihre Active Directory-Umgebung übereinstimmen. • Stellen Sie sicher, dass Sie bei der Anmeldung den korrekten Benutzer-domänennamen und nicht den NetBIOS-Namen verwenden.

A

Anhang A: Remote Console Switch Software – Tastatur- und Maus-Tastenkombinationen

Tabelle A-1. Tastatur- und Maus-Tastenkombinationen im Unterteilungsfenster

Operation	Beschreibung
F6	Navigiert zwischen den geteilten Bildschirmen und markiert das letzte Element, auf dem sich der Eingabefokus befand.
F8	Markiert die Unterteilung.
Pfeil-nach-links- oder Pfeil-nach-oben-Taste	Verschiebt die Unterteilung nach links, sofern diese markiert ist.
Pfeil-nach-rechts- oder Pfeil-nach-unten-Taste	Bewegt die Unterteilung nach rechts, sofern diese markiert ist.
Pos1	Maximiert das rechte Fenster des geteilten Bildschirms (das linke Fenster wird ausgeblendet), sofern die Unterteilung markiert ist.
Ende	Maximiert das linke Fenster des geteilten Bildschirms (das rechte Fenster wird ausgeblendet), sofern die Unterteilung markiert ist.
Mausklick + Mausziehen	Bewegt die Unterteilung nach links oder rechts.

Tabelle A-2. Tastatur- und Maus-Tastenkombinationen zur Steuerung in der Baumstrukturansicht

Operation	Beschreibung
Einfacher Mausklick	Hebt die bestehende Auswahl auf und wählt den Knoten aus, über dem sich der Mauszeiger befindet.
Doppelter Mausklick	Blendet einen erweiterbaren Knoten ein/aus (ein Knoten, der untergeordnete Objekte hat). Keine Aktivität bei einem untergeordneten Knoten (ein Knoten, der keine untergeordneten Objekte hat).
Pfeil-nach-oben-Taste	Hebt die bestehende Auswahl auf und wählt den nächsten Knoten aus, der über der aktuellen Markierung liegt.
Pfeil-nach-unten-Taste	Hebt die bestehende Auswahl auf und wählt den nächsten Knoten aus, der unter der aktuellen Markierung liegt.
Leertaste	Markiert den Knoten, auf dem sich momentan der Eingabefokus befindet, oder hebt seine Markierung auf.
Eingabetaste	Blendet abwechselnd den Knoten ein oder aus, auf dem sich der Eingabefokus befindet. Gilt nur für Knoten mit untergeordneten Objekten. Keine Aktivität, wenn der Knoten keine untergeordneten Objekte hat.
Pos1	Hebt die bestehende Auswahl auf und wählt den Stammknoten aus.
Ende	Hebt die bestehende Auswahl auf und wählt den letzten Knoten aus, der in der Baumstruktur angezeigt wird.

Tabelle A-3. Tastatur- und Maus-Tastenkombinationen für die Einheitenliste

Operation	Beschreibung
Eingabe- oder Returntaste	Startet die Standardaktion für die ausgewählte Einheit.
Pfeil-nach-oben-Taste	Hebt die bestehende Auswahl auf und bewegt die Auswahl um eine Zeile nach oben.
Pfeil-nach-unten-Taste	Hebt die bestehende Auswahl auf und bewegt die Auswahl um eine Zeile nach unten.

Tabelle A-3. Tastatur- und Maus-Tastenkombinationen für die Einheitenliste (Fortsetzung)

Operation	Beschreibung
Bild auf	Hebt die bestehende Auswahl auf, blättert eine Seite nach oben und wählt die erste Position auf der Seite aus.
Bild ab	Hebt die bestehende Auswahl auf, blättert eine Seite nach unten und wählt die letzte Position auf der Seite aus.
Entf	Führt die Löschfunktion durch. Hat dieselbe Funktion wie die Menüfunktion „Bearbeiten ->Löschen“. Weitere Informationen im entsprechenden Abschnitt.
Strg + Pos1	Bewegt die Markierung und die Auswahl auf die erste Zeile in der Tabelle.
Strg + Ende	Bewegt die Markierung und die Auswahl auf die letzte Zeile in der Tabelle.
Umschalttaste + Pfeil-nach-oben-Taste	Erweitert die Auswahl um eine Zeile nach oben.
Umschalttaste + Pfeil-nach-unten-Taste	Erweitert die Auswahl um eine Zeile nach unten.
Umschalttaste + Bild auf	Erweitert die Auswahl um eine Seite nach oben.
Umschalttaste + Bild ab	Erweitert die Auswahl um eine Seite nach unten.
Umschalttaste + Mausklick	Hebt eine bestehende Auswahl auf und wählt die Zeilen zwischen der aktuellen Markierung und der Zeile aus, in der sich der Mauszeiger befindet, wenn ein Mausklick durchgeführt wird.
Strg + Mausklick	Kehrt den Auswahlstatus der Zeile um, in der sich der Mauszeiger befindet, ohne dass der Auswahlstatus einer anderen Zeile beeinflusst wird.
Doppelter Mausklick	Startet die Standardaktion für die ausgewählte Einheit.

B

Anhang B: TCP-Ports

Die nachfolgende Tabelle zeigt die Funktionen des Remote Console Switch und der verwendeten Ports.

Tabelle B-1. Verwendete Ports

Port	Funktion
TCP 80/443	Standard-HTTP/HTTPS
TCP 2068/8192	Video Viewer-Video, Tastatur, Maus, Benutzerauthentifizierung und Virtual Media.
TCP/UDP 3211	Erkennung, EVA-Benutzerauthentifizierung.
TCP 3871	Plug-In-Unterstützung

HINWEIS: Die meisten Daten auf den Ports 2068 und 3211 wurden mit dem Secure Socket Layer (SSL)-Protokoll verschlüsselt.

Abbildung B-1. TCP-Port-Kommunikation

HINWEIS: Die TCP/IP-Ports sind statisch und können nicht verändert werden.

C

Anhang C: MIBs und SNMP-Traps

Dieser Anhang bietet Informationen aus den MIBs (Management Information Bases), die für die Dell 2161DS-2/4161DS/2321DS Remote Console Switches verfasst wurden. Abschnitte in diesem Handbuch folgen den MIB-Gruppen und bieten Erklärungen und Definitionen für die Terminologie, die zur Festlegung von MIB-Objekten verwendet wird. Sie können auf MIB-11- und MIB-Datenbanken zugreifen, während Sie IPv4 oder IPv6 verwenden, und IPv4- bzw. IPv6-spezifische Traps hinzufügen.

MIB ist eine virtuelle Datenbank für verwaltete Objekte im SNMP-Agent. Sie ist eine Sammlung von Objekten, welche die Eigenschaften der verwalteten Geräte definiert.

Die Remote Console Switch MIB-Definitionen verwenden die in den folgenden Kommentaranforderungen (RFC, Request For Comments) beschriebene Struktur.

- RFC-1155-SMI

  Beschreibt die gemeinsamen Strukturen und das Identifikationsschema für die Festlegung der Verwaltungsinformationen, die mit TCP/IP-basiertem Internet verwendet werden.

- RFC-1212

  Beschreibt das Format, das für die Erstellung präziser und beschreibender MIB-Module verwendet wird.

- RFC-1213-MIB

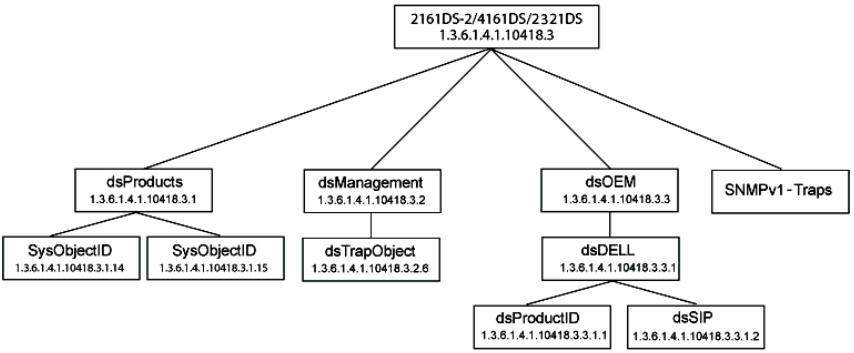
  Beschreibt den Internetstandard MIB-II für die Verwendung mit Netzwerk-Managementprotokollen in TCP/IP-basierten Internetanwendungen.

- RFC-1215

  Beschreibt die standardisierten SNMP-Traps und bietet die Möglichkeit zum Definieren unternehmensspezifischer Traps.

Die private Remote Console Switch MIB wird mit der Objektkennzeichnung 1.3.6.1.4.1.10418.3 dargestellt, die die Unterkategorien dsProducts (1), dsManagement (2), dsOEM (3) und SNMP-Traps umfasst (siehe Abbildung C-1).

Abbildung C-1. Dell Remote Console Switch MIB-Struktur



MIB-Gruppen

Produkt-ID-Gruppe (dsProductID) 1.3.6.1.4.1.10418.3.3.1.1

Produkt-ID-Objekte sind in Tabelle C-1 aufgeführt. Die Produkt-ID-Gruppe dient in erster Linie dazu, dass die Managementkonsole Hersteller, Modell, Produktversion und Firmwareversion des Remote Console Switches eindeutig feststellen kann. Produkt-ID-Gruppen-Objekttypen können bei Bestandsaufnahmen oder der automatischen Erkennung von Inkompatibilität oder nicht übereinstimmenden Versionen verschiedener Hardware- und Softwarekomponenten eines Systems nützlich sein.

Tabelle C-1. Produkt-IP-Gruppenobjekte

Objekttyp	Beschreibung	OID
dsProductIDDisplayName	Produktname in UTF8.	1.3.6.1.4.1.10418.3.3.1.1.1
dsProductIDVendor	Lieferant des Produkts in UTF8.	1.3.6.1.4.1.10418.3.3.1.1.3
ProductIDProductVersion	Globale Produktversion in UTF8.	1.3.6.1.4.1.10418.3.3.1.1.4
dsProductIDDModuleFWVersion	Die Zeichenkette für die Firmwareversion des D-Moduls in UTF8.	1.3.6.1.4.1.10418.3.3.1.1.5
dsProductIDMainboardFWVersion	Die Zeichenkette für die Firmwareversion des Main Boards in UTF8.	1.3.6.1.4.1.10418.3.3.1.1.6

Objekttyp	Beschreibung	OID
dsProductIDStatus	Meldet den Betriebsstatus des Produkts basierend auf einer Zuordnung der privaten MIB-Variablen dsServerStatus wie folgt:	1.3.6.1.4.1.10418.3.3.1.1.7 dsProductIDStatus
	dsServerStatus	OK (3) – Das Produkt ist betriebsbereit.
	ready (1)	Unbekannt (2) – Das Produkt wird hochgefahren und ist nicht betriebsbereit.
	startupInProgress (2)	
	subsystemUpgrading (3)	Nicht-kritisch (4) – Das Produkt führt eine Flash-Aktualisierung durch und ist nicht betriebsbereit.
	kdbMseSubsystemFailure (4)	
	videoSubsystemFailure (5)	Nicht behebbar (6) – Es ist ein Fehler im Subsystem aufgetreten. Das Produkt ist nicht vollständig betriebsbereit.
		Nicht behebbar (6) – Es ist ein Fehler im Subsystem aufgetreten. Das Produkt ist nicht vollständig betriebsbereit.
dsProductIDDescription	Produktbeschreibung in UTF8.	1.3.6.1.4.1.10418.3.3.1.1.2
dsProductIDVendor	Lieferant des Produkts in UTF8.	1.3.6.1.4.1.10418.3.3.1.1.3
ProductIDProductVersion	Globale Produktversion in UTF8.	1.3.6.1.4.1.10418.3.3.1.1.4
dsProductIDDModuleFWVersion	Die Zeichenkette für die Firmwareversion des D-Moduls in UTF8.	1.3.6.1.4.1.10418.3.3.1.1.5

Objekttyp	Beschreibung	OID
dsProductIDMainboardFWVersion	Die Zeichenkette für die Firmwareversion des Main Boards in UTF8.	1.3.6.1.4.1.10418.3.3.1.1.6
dsProductIDStatus	Meldet den Betriebsstatus des Produkts basierend auf einer Zuordnung der privaten MIB-Variablen dsServerStatus wie folgt:	1.3.6.1.4.1.10418.3.3.1.1.7
		dsProductIDStatus
	dsServerStatus ready (1)	OK (3) – Das Produkt ist betriebsbereit.
	startupInProgress (2) subsystemUpgrading (3)	Unbekannt (2) – Das Produkt wird hochgefahren und ist nicht betriebsbereit.
	kdbMseSubsystemFailure (4) videoSubsystemFailure (5)	Nicht-kritisch (4) – Das Produkt führt eine Flash-Aktualisierung durch und ist nicht betriebsbereit.
		Nicht behebbar (6) – Es ist ein Fehler im Subsystem aufgetreten. Das Produkt ist nicht vollständig betriebsbereit.
		Nicht behebbar (6) – Es ist ein Fehler im Subsystem aufgetreten. Das Produkt ist nicht vollständig betriebsbereit.

SIP-Gruppe (dsSIP) 1.3.6.1.4.1.10418.3.3.1.2

SIP-Gruppenobjekte sind in Tabelle C-2 aufgeführt. Die SIP-Gruppenobjekte sind in Tabellenform strukturiert und enthalten Informationen über die an den Remote Console Switch angeschlossenen SIPs wie Boot-, Anwendungs- und Hardwareversion des SIPs.

Tabelle C-2. SIP-Gruppenobjekte

Objekttyp	Beschreibung	OID
dsSipTable	Tabelle mit SIP-Informationen.	1.3.6.1.4.1.10418.3.3.1.2.1
dsSipTableEntry	Ein Eintrag in der SIP-Tabelle.	1.3.6.1.4.1.10418.3.3.1.2.1.1
dsSipTableIndex	Ein eindeutiger Index, der für einen Eintrag in der SIP-Tabelle steht.	1.3.6.1.4.1.10418.3.3.1.2.1.1.1
dsSipTableInputPort	Eine Eingangsportnummer. Beschreibt den Port, an den das SIP angeschlossen ist.	1.3.6.1.4.1.10418.3.3.1.2.1.1.2
dsSipTableEID	Die EID des SIPs.	1.3.6.1.4.1.10418.3.3.1.2.1.1.3
dsSipTableBootImageVersion	Die Boot-Image-Version des SIPs in UTF8.	1.3.6.1.4.1.10418.3.3.1.2.1.1.4
dsSipTableAppImageVersion	Die Anwendungs-Image-Version des SIPs in UTF8.	1.3.6.1.4.1.10418.3.3.1.2.1.1.5
dsSipTableHardwareVersion	Die Hardware-Version des SIPs in UTF8.	1.3.6.1.4.1.10418.3.3.1.2.1.1.6
dsSipTableStatus	Der Status des SIPs.	1.3.6.1.4.1.10418.3.3.1.2.1.1.7

SNMP-Trap-Objektgruppe

Dieser Abschnitt beschreibt die Variablen, die an Dell 2161DS-2/4161DS Remote Console Switches gesendet werden. Hier finden Sie zusätzliche Informationen über Traps oder Alarme, die von einem Ereignis am RCS ausgelöst werden. Die folgenden Objekte dienen zum Erstellen von Traps. Die Objekte werden als Traps gesendet. Auf sie kann nicht auf andere Weise zugegriffen werden.

Benutzername	
Variablenname	dsTrapObjectUserName
OID	1.3.6.1.4.1.10418.3.2.6.1
Beschreibung	Dieses Objekt wird als Trap gesendet, um den Namen des Benutzers zu identifizieren, bei dem der Trap-Fehler aufgetreten ist. Wenn die Trap-Bedingung durch Aktivitäten am lokalen Port (OSD) aufgetreten ist, so ist der Wert dieses Objektes die folgende Zeichenkette: local port.
Syntax	UTF8String (SIZE (3.16))

Benutzername am Zielgerät	
Variablenname	dsTrapObjectTargetUserName
OID	1.3.6.1.4.1.10418.3.2.6.2
Beschreibung	Dieses Objekt wird als Trap gesendet, um den Namen des Zielgerätbenutzers zu identifizieren, bei dem die Trap-Bedingung aufgetreten ist.
Syntax	UTF8String (SIZE (3.16))

Image-Typ	
Variablenname	dsTrapObjectImageType
OID	1.3.6.1.4.1.10418.3.2.6.3
Beschreibung	Dieses Objekt wird als Trap gesendet, um den Namen des Software-Images zu identifizieren, bei dem die Trap-Bedingung aufgetreten ist.
Syntax	UTF8String (SIZE (0.64))

Neue Image-Version	
Variablenname	dsTrapObjectImageNewVersion
OID	1.3.6.1.4.1.10418.3.2.6.4
Beschreibung	UTF8String (SIZE (0.32))
Syntax	Dieses Objekt wird als Trap gesendet, um die Version des neuen Software-Images zu identifizieren, mit dem die Remote Console Switch aktualisiert wird.

Aktuelle Image-Version	
Variablenname	dsTrapObjectImageCurrentVersion
OID	1.3.6.1.4.1.10418.3.2.6.5
Beschreibung	Dieses Objekt wird als Trap gesendet, um die Version des Software-Images zu identifizieren, die momentan auf dem Remote Console Switch vorhanden ist.
Syntax	UTF8String (SIZE (0.32))

Image-Aktualisierungs-ergebnisse	
Variablenname	dsTrapObjectImageUpgradeResults
OID	1.3.6.1.4.1.10418.3.2.6.6
Beschreibung	Dieses Objekt wird als Trap gesendet, um die Ergebnisse einer FTP-, TFTP- oder ASMP-Image-Aktualisierung zu melden.
Syntax	UTF8String (SIZE (0.64))

Sitzungskennung	
Variablenname	dsTrapObjectSessionIdentifier
OID	1.3.6.1.4.1.10418.3.2.6.7
Beschreibung	Dieses Objekt wird als Trap gesendet, um die Sitzung zu identifizieren, bei der die Trap-Bedingung aufgetreten ist. Der Wert ist, sofern bekannt, der Servername. Ansonsten ist der Wert der Verbindungspfad zum Server. Wenn der Wert der Verbindungspfad ist, wird er im folgenden Format dargestellt: SIP s:Channel c Dabei ist s die ID des SIPs und c ist die Kanalnummer für den gestuften Switch (0, wenn kein Switch unter dem Pfad vorhanden ist).
Syntax	UTF8String (SIZE (0.32))

SIP-Kennung	
Variablenname	dsTrapObjectSipId
OID	1.3.6.1.4.1.10418.3.2.6.8
Beschreibung	Dieses Objekt wird als Trap gesendet, um das SIP zu identifizieren, bei dem die Trap-Bedingung aufgetreten ist.
Syntax	UTF8String (SIZE (0.32))

Kennung des gestuften Switches	
Variablenname	dsTrapObjectTieredSwitchName
OID	1.3.6.1.4.1.10418.3.2.6.9
Beschreibung	Dieses Objekt wird als Trap gesendet, um den gestuften Switch zu identifizieren, bei dem die Trap-Bedingung aufgetreten ist.
Syntax	Syntax UTF8String (SIZE (0.15))

Alte Kennung des gestuften Switches	
Variablenname	dsTrapObjectOldTieredSwitchName
OID	1.3.6.1.4.1.10418.3.2.6.10
Beschreibung	Dieses Objekt wird als Trap gesendet, um den alten Namen eines gestuften Switches zu identifizieren, dessen Name geändert wurde.
Syntax	UTF8String (SIZE (0.15))

Server-Kennung	
Variablenname	dsTrapObjectServerName
OID	1.3.6.1.4.1.10418.3.2.6.11
Beschreibung	Dieses Objekt wird als Trap gesendet, um den Server zu identifizieren, bei dem die Trap-Bedingung aufgetreten ist.
Syntax	UTF8String (SIZE (0.15))

Alte Kennung des Servers	
Variablenname	dsTrapObjectOldServerName
OID	1.3.6.1.4.1.10418.3.2.6.12
Beschreibung	Dieses Objekt wird als Trap gesendet, um den alten Namen eines Servers herauszufinden, dessen Name geändert wurde.
Syntax	UTF8String (SIZE (0.15))

Dateinamen-Kennung	
Variablenname	dsTrapObjectFileName
OID	1.3.6.1.4.1.10418.3.2.6.13
Beschreibung	Dieses Objekt wird als Trap gesendet, um den Namen einer Datei zu identifizieren, bei der die Trap-Bedingung aufgetreten ist.
Syntax	DisplayString (SIZE (0.12))

Firmware-Zustand	
Variablenname	dsTrapObjectFirmwareCondition
OID	1.3.6.1.4.1.10418.3.2.6.14
Beschreibung	Diese Trap-Nachricht enthält Daten für anwendungsspezifische Diagnosetests. Sie dient zur diagnostischen Hilfe bei Problemen, die bei der Installation auftreten. Hierzu muss der Benutzer die bereitgestellte Firmware installieren, um die jeweiligen Probleme zu isolieren, und in den Trap-Einstellungen Fehlermeldungen aktivieren. Der Inhalt besteht aus einem Dell Application Message Packet ohne Adresse, Größe und Befehlsheader. Die Parameter der Nachricht sind abhängig vom jeweiligen Problem, das die Firmware entdecken und melden soll.
Syntax	OCTET STRING (SIZE (0.64))

Gerätekennung	
Variablenname	dsTrapObjectDeviceId
OID	1.3.6.1.4.1.10418.3.2.6.15
Beschreibung	Dieses Objekt wird als Trap gesendet, um das Gerät zu identifizieren, bei dem die Trap-Bedingung aufgetreten ist.
Syntax	UTF8String (SIZE (0.32))

Warnung/ Alarmzustand	
Variablenname	dsTrapObjectAlarmCondition
OID	1.3.6.1.4.1.10418.3.2.6.16
Beschreibung	Dieses Objekt wird als Trap gesendet, um die Warn- oder Alarmaktivität zu identifizieren, bei dem die Trap-Bedingung aufgetreten ist. „Alarm“ stellt den Alarm ein, „OK“ gibt an, dass der Fehler nicht mehr vorhanden ist.
Syntax	SyntaxINTEGER {alarm(1),ok(2)}

Erklärung der Warnung/des Alarms	
Variablenname	dsTrapObjectAlarmDescription
OID	1.3.6.1.4.1.10418.3.2.6.17
Beschreibung	Dieses Objekt wird als Trap gesendet, um die Warnung oder den Alarmzustand zu erklären, aufgrund dessen die Trap-Bedingung aufgetreten ist. Dies dient zur Anzeige oder zur Protokollierung.
Syntax	UTF8String (SIZE (0.64))

Grund der Benutzerkontensperre	
Variablenname	dsTrapObjectLockReason
OID	1.3.6.1.4.1.10418.3.2.6.18
Beschreibung	Dieses Objekt wird als Trap gesendet, um den Grund dafür ausfindig zu machen, warum ein Benutzerkonto gesperrt wurde.
Syntax	UTF8String (SIZE (0.64))

Grund für die Aufhebung der Benutzerkontensperre	
Variablenname	dsTrapObjectUnlockReason
OID	1.3.6.1.4.1.10418.3.2.6.19
Beschreibung	Dieses Objekt wird als Trap gesendet, um den Grund dafür ausfindig zu machen, warum die Sperrung eines Benutzerkontos aufgehoben wurde.
Syntax	UTF8String (SIZE (0.64))

IP-Adresse	
Variablenname	dsTrapObjectIPAddress
OID	1.3.6.1.4.1.10418.3.2.6.20
Beschreibung	Dieses Objekt wird als Trap gesendet, um die IP-Adresse zu identifizieren, bei der eine Trap-Bedingung aufgetreten ist.
Syntax	UTF8String (SIZE (0.256))

SIP-Image-Aktualisierungsergebnisse	
Variablenname	dsTrapObjectSipImageUpgradeResult
OID	1.3.6.1.4.1.10418.3.2.6.21
Beschreibung	Dieses Objekt wird als Trap gesendet, um das Ergebnis einer SIP-Image-Aktualisierung zu melden.

Syntax	SyntaxINTEGER {
	sipUpgradeNoFirmwareImage(1), -- Es ist kein Firmware-Image vorhanden
	sipUpgradeLostContact(2), -- Kommunikation zum SIP wurde abgebrochen
	sipUpgradeFailedRestart(3), -- Der SIP startete nach der Aktualisierung nicht neu
	sipUpgradeFailedVerify(4), -- Fehler beim Aktualisieren des SIP auf die richtige Version
	sipUpgradeSuccess(9999) -- Erfolgreich
	}

SIP-Image-Typ	
Variablenname	dsTrapTrapObjectTypeOfImage
OID	1.3.6.1.4.1.10418.3.2.6.22
Beschreibung	Dieses Objekt wird als Trap gesendet, um den Software-Image-Typ zu melden, bei dem die Trap-Bedingung aufgetreten ist.
Syntax	SyntaxINTEGER {boot(1),app(2)}

Zugriffsmodus des Virtual Media-Laufwerks	
Variablenname	dsTrapObjectVirtualMediaDriveAccessMode
OID	1.3.6.1.4.1.10418.3.2.6.23
Beschreibung	Dieses Objekt wird als Trap gesendet, um den Zugriffsmodus für ein virtuelles Remote-Laufwerk zu melden, bei dem die Trap-Bedingung aufgetreten ist.
Syntax	SyntaxINTEGER {readonly(1),readwrite(2)}

Virtual Media-Laufwerkstyp	
Variablenname	dsTrapObjectVirtualMediaDriveType
OID	1.3.6.1.4.1.10418.3.2.6.24
Beschreibung	Dieses Objekt wird als Trap gesendet, um den Typ eines virtuellen Remote-Laufwerks zu melden, bei dem die Trap-Bedingung aufgetreten ist.
Syntax	SyntaxINTEGER {floppy_memorykey(1),cd_dvd_rom(2),generic(3)}

Code der Image-Aktualisierungsergebnisse	
Variablenname	dsTrapObjectImageUpgradeResultsCode
OID	1.3.6.1.4.1.10418.3.2.6.25
Beschreibung	Dieses Objekt wird als Trap gesendet, um die Ergebnisse einer FTP-, TFTP- oder ASMP-Image-Aktualisierung zu melden.

Code der Image-Aktualisierungsergebnisse (Fortsetzung)	
Syntax	SyntaxINTEGER { imageUpgradeTftpNoSocket(1), -- TFTP ohne Socket imageUpgradeTftpConnectFailure(2), -- Fehler bei der TFTP-Verbindung des TFTP-Servers imageUpgradeTftpRequestDenied(3), -- TFTP-Serveranfrage verweigert imageUpgradeTftpBadPacket(4), -- TFTP-Fehler – Nicht-Daten-Paket empfangen imageUpgradeTftpOOS(5), -- TFTP-Fehler – Zu viele Pakete in falscher Reihenfolge imageUpgradeTftpTooBig(6), -- TFTP-Fehler – Übertragene Datenmenge übersteigt Dateigröße imageUpgradeTftpTimeout(7), -- TFTP-Fehler – Timeout wurde während der Übertragung überschritten, zu viele Versuche imageUpgradeAlreadyInProgress(8), -- Aktualisierung wird bereits durchgeführt imageUpgradeCannotStart(9), -- Aktualisierungs-Thread wurde nicht gestartet imageUpgradeMemoryError(10), -- Fehler bei der Speicherzuordnung imageUpgradeTftpProtocolError(11), -- TFTP-Protokollfehler. Übertragung konnte nicht beendet werden imageUpgradeBadType(12), -- Bildtyp entspricht nicht dem Bereich (Boot/App) für Aktualisierung imageUpgradeInvalidAppDowngrade(13), -- Ungültige Downgradeversion imageUpgradeChecksumError(14), -- Prüfsummenfehler imageUpgradeFlashError(15), -- Flash-Fehler imageUpgradeInternalError(16), -- Interner Fehler imageUpgradeFileNotFound(17), -- Datei nicht gefunden

Code der Image-Aktualisierungsergebnisse (Fortsetzung)	
Syntax (Fortsetzung)	imageUpgradeBadHeader(18), -- Ungültiger Image-Header imageUpgradeIncompatibleHeader(19), -- Header ist nicht kompatibel imageUpgradeTftpXferFail(20), -- TFTP-Übertragung fehlgeschlagen imageUpgradeTftpSvrNoResponse(21), -- Keine Reaktion vom TFTP-Server imageUpgradeNetworkUnreachable(22), -- Keine Verbindung zum Netzwerk imageUpgradeSuccess(9999) -- Erfolgreich }

Unternehmens-Traps

SNMP-Traps ermöglichen es einem Agenten, die Managementkonsole über wichtige Systemereignisse zu informieren. Damit eine SNMP-Managementanwendung Systemereignisse über SNMP-Traps interpretieren kann, muss die Anwendung Zugriff auf die Namen und Objekttypen im Remote Console Switch haben. Dies wird durch die MIB-Module ermöglicht, die Variablen enthalten, die so eingestellt und gelesen werden können, dass sie den RCS mit Informationen versorgen.

Dieser Abschnitt beschreibt die Traps, die vom Dell 2161DS-2/4161DS SNMP-Agenten erstellt werden. Die in Tabelle C-3 beschriebenen unternehmensspezifischen Traps gehören zu dem MIB-Unternehmen mit der OID 1.3.6.1.4.1.10418.3.2.6 und werden mit den unter „SNMP-Trap-Objektgruppe“ auf Seite 196 beschriebenen Trap-Variablen gesendet.

Tabelle C-3. Unternehmensspezifische Traps

Trap-ID	Trap-Nachricht	Schweregrad	Beschreibung
1	Der Remote Console Switch führt einen Neustart durch. Befehl erteilt von Benutzer: %s.	Information	Der Remote Console Switch führt einen Neustart durch. Der Name des Benutzers, der den Neustart initiiert hat, ist in „dsTrapObjectUserName“ enthalten.
2	Am Remote Console Switch angemeldeter Benutzer. Benutzer: %s.	Information	Ein Benutzer hat sich am Remote Console Switch angemeldet. Der Name des Benutzers, der am Remote Console Switch angemeldet ist, ist in „dsTrapObjectUserName“ enthalten.
3	Vom Remote Console Switch abgemeldeter Benutzer. Benutzer: %s.	Information	Ein Benutzer hat sich am Remote Console Switch abgemeldet. Der Name des Benutzers, der sich vom Remote Console Switch abgemeldet hat, ist in „dsTrapObjectUserName“ enthalten.
4	Videositzung gestartet. Benutzer: %s. Server: %s.	Information	Eine Videositzung wurde gestartet. Der Name des Benutzers, der mit der Sitzung verbunden ist, ist in „dsTrapObjectUserName“ enthalten. Die Sitzungskennung ist in „dsTrapObjectSessionIdentifier“ enthalten.
5	Videositzung angehalten. Benutzer: %s. Server: %s.	Information	Eine Videositzung wurde angehalten. Der Name des Benutzers, der mit der Sitzung verbunden war, ist in „dsTrapObjectUserName“ enthalten. Die Sitzungskennung ist in „dsTrapObjectSessionIdentifier“ enthalten.

Trap-ID	Trap-Nachricht	Schweregrad	Beschreibung
6	Videositzung abgebrochen. Befehl erteilt von Benutzer: %s. Getrennter Benutzer: %s. Server: %s.	Information	Eine Videositzung wurde von einem anderen Benutzer abgebrochen. Der Name des Benutzers, der die Sitzung abgebrochen hat, ist in „dsTrapObjectUserName“ enthalten. Der Name des Benutzers, dessen Sitzung abgebrochen wurde, ist in „dsTrapObjectTargetUserName“ enthalten. Die Sitzungskennung ist in „dsTrapObjectSessionIdentifier“ enthalten.
7	Anzeige am lokalen Port gestartet. Server: %s.	Information	Ein Benutzer am lokalen Port zeigt einen Server an. Die Sitzungskennung ist in „dsTrapObjectSessionIdentifier“ enthalten.
8	Anzeige am lokalen Port angehalten. Server: %s.	Information	Ein Benutzer am lokalen Port hat die Anzeige des Servers beendet. Die Sitzungskennung ist in „dsTrapObjectSessionIdentifier“ enthalten.
9	FTP-, TFTP- oder ASMP-Imageaktu-alisierung gestartet. Befehl erteilt von Benutzer: %s. Image-Typ: %s. Neue Version: %s. Aktuelle Version: %s.	Information	Der Remote Console Switch hat eine FTP-, TFTP- oder ASMP-Aktualisierung eines Images gestartet. Der Name des Benutzers, der die FTP-, TFTP- oder ASMP-Image-Aktualisierung initiiert hat, ist in „dsTrapObjectUserName“ enthalten. Der Image-Typ, der aktualisiert wird, ist in „dsTrapObjectImageType“ enthalten. Die Version des Images, mit dem der Remote Console Switch aktualisiert wird, ist in „dsTrapObjectImageNewVersion“ enthalten. Die Version des Images, die momentan vom Remote Console Switch ausgeführt wird, ist in „dsTrapObjectImageCurrentVersion“ enthalten.

Trap-ID	Trap-Nachricht	Schweregrad	Beschreibung
10	Ergebnis Text: %s. Ergebnisse Code: %d.	Information	Das Ergebnis einer FTP-, TFTP- oder ASMP-Image-Aktualisierung.
11	Neuer Benutzer zur lokalen Benutzerdatenbank hinzugefügt. Befehl erteilt von Benutzer: %s. Neuer Benutzer: %s.	Information	Der lokalen Benutzerdatenbank wurde ein neuer Benutzer hinzugefügt. Der Name des Benutzers, der den neuen Benutzer hinzugefügt hat, ist in „dsTrapObjectUserName“ enthalten. Der Name des neuen Benutzers ist in „dsTrapObjectTargetUserName“ enthalten.
12	Benutzer aus lokaler Benutzerdatenbank gelöscht. Befehl erteilt von Benutzer: %s. Gelöschter Benutzer: %s.	Information	Aus der lokalen Benutzerdatenbank wurde ein Benutzer gelöscht. Der Name des Benutzers, der den Benutzer gelöscht hat, ist in „dsTrapObjectUserName“ enthalten. Der Name des gelöschten Benutzers ist in „dsTrapObjectTargetUserName“ enthalten.
13	Benutzer in lokaler Benutzerdatenbank geändert. Befehl erteilt von Benutzer: %s. Geänderter Benutzer: %s.	Information	Ein Benutzer wurde geändert. Der Name des Benutzers, der den Benutzer geändert hat, ist in „dsTrapObjectUserName“ enthalten. Der Name des geänderten Benutzers ist in „dsTrapObjectTargetUserName“ enthalten.
14	Benutzer-authentifizierung am Remote Console Switch fehlgeschlagen. Benutzer: %s.	Information	Ein Benutzer konnte am Remote Console Switch nicht authentifiziert werden. Der Name des Benutzers, der nicht authentifiziert werden konnte, ist in „dsTrapObjectUserName“ enthalten.

Trap-ID	Trap-Nachricht	Schweregrad	Beschreibung
15	SIP hinzugefügt. SIP-ID: %s.	Information	Ein SIP wurde hinzugefügt. Die ID des hinzugefügten SIPs ist in „dsTrapObjectSipId“ enthalten.
16	SIP entfernt. SIP-ID: %s.	Information	Ein SIP wurde entfernt. Die ID des entfernten SIPs ist in „dsTrapObjectSipId“ enthalten.
17	Servername geändert. Alter Name: %s. Neuer Name: %s. Angeschlossen an SIP: %s.	Information	Der Name eines Servers wurde geändert. Der vorherige Name des Servers ist in „dsTrapObjectOldServerName“ enthalten. Der neue Name des Servers ist in „dsTrapObjectServerName“ enthalten. Die ID des SIPs, an das der Server angeschlossen ist, ist in „dsTrapObjectSipId“ enthalten.
18	Gestufter Switch hinzugefügt. Gestufter Switch Name: %s. Angeschlossen an SIP: %s.	Information	Ein gestufter Switch wurde hinzugefügt. Der Name des hinzugefügten Switches ist in „dsTrapObjectTieredSwitchName“ enthalten. Die ID des SIPs, an den der Switch angeschlossen wurde, ist in „dsTrapObjectSipId“ enthalten.
19	Gestufter Switch entfernt. Gestufter Switch Name: %s. War Angeschlossen an SIP: %s.	Information	Ein gestufter Switch wurde entfernt. Der Name des entfernten Switches ist in „dsTrapObjectTieredSwitchName“ enthalten. Die ID des SIPs, an den der Switch angeschlossen war, ist in „dsTrapObjectSipId“ enthalten.

Trap-ID	Trap-Nachricht	Schweregrad	Beschreibung
20	Gestufter Switch Name geändert: Alter Name: %s. Neuer Name: %s. Angeschlossen an SIP: %s.	Information	Der Name eines gestuften Switches wurde geändert. Der vorherige Name des gestuften Switches ist in „dsTrapObjectOldTieredSwitchName“ enthalten. Der neue Name des gestuften Switches ist in „dsTrapObjectTieredSwitchName“ enthalten. Die ID des SIPs, an den der Switch angeschlossen ist, ist in „dsTrapObjectSipId“ enthalten.
21	Konfigurations-datei in den Remote Console Switch geladen. Befehl erteilt von Benutzer: %s. Name Der Geladenen Datei: %s.	Information	Der Remote Console Switch hat eine Konfigurationsdatei geladen. Der Name des Benutzers, der dem Remote Console Switch den Befehl zum Laden der Konfigurationsdatei erteilt hat, ist in „dsTrapObjectUserName“ enthalten. Der Name der geladenen Datei ist in „dsTrapObjectFileName“ enthalten.
22	Benutzerdaten-bank-Datei in den Remote Console Switch geladen. Befehl erteilt von Benutzer: %s. Name der geladenen Datei: %s.	Information	Der Remote Console Switch hat eine Benutzerdatenbank-Datei geladen. Der Name des Benutzers, der dem Remote Console Switch den Befehl zum Laden der Benutzerdatenbank-Datei erteilt hat, ist in „dsTrapObjectUserName“ enthalten. Der Name der geladenen Datei ist in „dsTrapObjectFileName“ enthalten.

Trap-ID	Trap-Nachricht	Schweregrad	Beschreibung
23	Ungültige Verbindung erkannt. Geräte-ID: %s.	Information	Der Remote Console Switch hat eine ungültige Verbindung erkannt. Dies können z. B. zwei SIP-Geräte an einem Port sein, an dem ein oder mehrere Legacy-KVM-Switches angeschlossen sind, oder andere unzulässige Konfigurationen. Informationen über die Art des Fehlers sind im Objekt „dsTrapObjectFirmwareCondition“ gespeichert. **HINWEIS:** Dieses Trap wird abgelehnt und wird nicht mehr gesendet.
24	Subsystem-aktualisierung wurde gestartet. Geräte-ID: %s.	Information	Der Remote Console Switch hat eine Subsystem-Aktualisierung gestartet. Dies kann ein Download vom D-Modul auf das Main Board sein oder ein SIP- oder anderer Subsystem-Download vom Main Board. Informationen über das Subsystem, das aktualisiert wird, sind im Objekt „dsTrapObjectFirmwareCondition“ gespeichert. **HINWEIS:** Dieses Trap wird abgelehnt und wird nicht mehr gesendet.
25	Subsystem-neustart. Geräte-ID: %s.	Information	Der Remote Console Switch hat einen Download beendet und startet das im Objekt „dsTrapObjectFirmwareCondition“ angegebene Subsystem neu. **HINWEIS:** Dieses Trap wird abgelehnt und wird nicht mehr gesendet.
26	Kommuni-kationspro-bleme in der Systemkonfi-guration. Geräte-ID: %s.	Schwer-wiegend	Der Remote Console Switch hat Kommunikationsprobleme innerhalb der Systemkonfiguration festgestellt. Dies kann auf Installationsprobleme hinweisen, die zu deutlichen Problemen mit dem Switch führen können.

Trap-ID	Trap-Nachricht	Schweregrad	Beschreibung
27	Speicherproblem. Geräte-ID: %s.	Kritisch	Der Remote Console Switch hat ein Speicherproblem festgestellt. Die Art dieses Problems wird im Objekt „dsTrapObjectFirmwareCondition“ beschrieben.
28	Watchdog zurücksetzen. Geräte-ID: %s.	Kritisch	Der Remote Console Switch hat festgestellt, dass der Watchdog zurückgesetzt wurde. Dies deutet auf einen äußerst schwerwiegenden Fehler in der Firmware/Hardware hin, der den normalen Betrieb des Remote Console Switches unmöglich macht.
29	Trap für besonderen Zustand ausgelöst. Geräte-ID: %s.	Information	Der Remote Console Switch hat einen besonderen Zustand festgestellt. Zu Diagnosezwecken wird ein Trap gesendet. Der Zustand wurde aufgezeichnet und ist im Objekt „dsTrapObjectFirmwareCondition“ gespeichert.
30	Subsystem-aktualisierung fehlgeschlagen. Geräte-ID: %s.	Information	Der Remote Console Switch hat einen besonderen Zustand festgestellt, der aus einer fehlgeschlagenen Subsystem-Aktualisierung entstanden ist. Der Zustand wurde aufgezeichnet und ist im Objekt „dsTrapObjectFirmwareCondition“ gespeichert.
31	Warnzustand. Geräte-ID: %s. Alarmzustand: %d. Alarmbeschreibung: %s.	Geringfügig	Der Remote Console Switch hat einen besonderen Zustand festgestellt. Ein Trap wird gesendet, um den Benutzer zu warnen. Ein Parameter befindet sich außerhalb des normalen Bereichs, z. B. der Temperaturbereich. Dies führt wahrscheinlich nicht zu einem ungewöhnlichen Verhalten des Remote Console Switches, kann jedoch einem schwereren Fehler vorausgehen.

Trap-ID	Trap-Nachricht	Schweregrad	Beschreibung
32	Kritischer Zustand. Geräte-ID: %s. Alarmzustand: %d. Alarmbeschreibung: %s.	Kritisch	Der Remote Console Switch hat einen besonderen Zustand festgestellt. Ein Trap wird gesendet, um den Benutzer zu warnen. Einige Parameter befindet sich außerhalb ihres normalen Bereiches. Unvorhersehbares Systemverhalten ist zu erwarten.
33	Benutzerkonto gesperrt. Client-IP-Adresse: %s. Gesperrter Benutzer: %s. Grund: %s.	Geringfügig	Ein Benutzerkonto wurde gesperrt. Die IP-Adresse des Client ist in „dsTrapObjectIPAddress“ enthalten. Der Name des gesperrten Benutzers ist in „dsTrapObjectTargetUserName“ enthalten. Der Grund für das Sperren des Benutzerkontos ist in „dsTrapObjectLockReason“ enthalten.

Trap-ID	Trap-Nachricht	Schweregrad	Beschreibung
34	Benutzerkonto Freigegeben. Client-IP-Adresse: %s. Befehl erteilt von Benutzer: %s. Freigegebener Benutzer: %s. Grund: %s.	Geringfügig	Ein Benutzerkonto wurde wieder freigegeben. Die IP-Adresse des Client, der die Freigabe des Benutzerkontos angefordert hat, ist in „dsTrapObjectIPAddress“ enthalten. Wenn das Benutzerkonto durch einen Neustart der Einheit oder durch Ablaufen des Sperrzeitraums (wie im Objekt „dsTrapObjectUnlockReason“ festgelegt) wieder freigegeben wurde, ist das Feld für die IP-Adresse leer. Der Name des Benutzers, der den Benutzer freigegeben hat, ist in „dsTrapObjectUserName“ enthalten. Wenn das Benutzerkonto durch einen Neustart der Einheit oder durch Ablaufen des Sperrzeitraums (wie im Objekt „dsTrapObjectUnlockReason“ festgelegt) wieder freigegeben wurde, ist das Feld für den Namen des Benutzers leer. Der Name des freigegebenen Benutzers ist in „dsTrapObjectTargetUserName“ enthalten. Der Grund für die Freigabe des Benutzerkontos ist in „dsTrapObjectUnlockReason“ enthalten.

Trap-ID	Trap-Nachricht	Schweregrad	Beschreibung
35	SIP-Image-Aktualisierung gestartet. Befehl erteilt von Benutzer: %s. Image-Typ: %s. Neue Version: %s. Aktuelle Version: %s. Server: %s. SIP-ID: %s.	Information	Eine Software-Image-Aktualisierung wurde an einem SIP gestartet. Der Name des Benutzers, der die SIP-Aktualisierung initiiert hat, ist in „dsTrapObjectUserName“ enthalten. Der Typ des Software-Images, das aktualisiert wird, ist in „dsTrapObjectSipTypeOfImage“ enthalten. Die Software-Image-Version, auf die das SIP aktualisiert wird, ist in „dsTrapObjectImageNewVersion“ enthalten. Die Software-Image-Version, die sich aktuell auf dem SIP befindet, ist in „dsTrapObjectImageCurrentVersion“ enthalten. Der Name des Servers, der an das zu aktualisierende SIP angeschlossen ist, ist in „dsTrapObjectServerName“ enthalten. Die ID des zu aktualisierenden SIPs ist in „dsTrapObjectSipId“ enthalten.

Trap-ID	Trap-Nachricht	Schweregrad	Beschreibung
36	Ergebnis der SIP-Image-Aktualisierung. Ergebnis: %d. Aktualisierung gestartet von Benutzer: %s. Aktualisierungs-Image-Typ: %d. Aktualisierungs-version: %s. Aktuelle Version: %s. Server: %s. SIP-ID: %s.	Information	Das Ergebnis einer SIP-Software-Image-Aktualisierung. Das Ergebnis der Image-Aktualisierung ist in „dsTrapObjectSipImageUpgradeResult“ enthalten. Der Name des Benutzers, der die SIP-Aktualisierung initiiert hat, ist in „dsTrapObjectUserName“ enthalten. Der Software-Image-Typ, für den das Aktualisierungsergebnis bestimmt ist, ist in „dsTrapObjectTypeOfImage“ enthalten. Die Software-Image-Version, mit der das SIP aktualisiert werden soll, ist in „dsTrapObjectImageNewVersion“ enthalten. Die Software-Image-Version, die sich auf dem SIP befindet, ist in „dsTrapObjectImageCurrentVersion“ enthalten. Wenn die Software-Image-Aktualisierung erfolgreich war, stimmt diese Version mit der in „dsTrapObjectImageNewVersion“ angegebenen Version überein. Der Name des Servers, der an das SIP angeschlossen ist, ist in „dsTrapObjectServerName“ enthalten. Die ID des SIPs, für das das Ergebnis bestimmt ist, ist in „dsTrapObjectSipId“ enthalten.
37	SIP neu gestartet. Server: %s. SIP-ID: %s.	Information	Ein SIP wurde neu gestartet. Ein SIP startet nach Abschluss einer SIP-Image-Aktualisierung neu. Der Name des Servers, der an das SIP angeschlossen ist, ist in „dsTrapObjectServerName“ enthalten. Die ID des SIPs, das neu gestartet wird, ist in „dsTrapObjectSipId“ enthalten.

Trap-ID	Trap-Nachricht	Schweregrad	Beschreibung
38	Virtual Media-Remote-Sitzung gestartet. Benutzer: %s. Server: %s. SIP: %s.	Information	Eine Virtual Media-Remote-Sitzung zu einem Server wurde gestartet. Derselbe Benutzer, der die VM-Sitzung gestartet hat, muss vorher eine Videositzung mit dem Server aufgebaut haben. Der Name des Benutzers, der mit der VM-Sitzung verbunden ist, ist in „dsTrapObjectUserName“ enthalten. Der Name des Servers, mit dem der Benutzer verbunden ist, ist in „dsTrapObjectServerName“ enthalten. Die ID des SIPs, das von der Videositzung verwendet wird, ist in „dsTrapObjectSipId“ enthalten.
39	Virtual Media-Remote-Sitzung angehalten. Benutzer: %s. Server: %s.	Information	Eine Virtual Media-Remote-Sitzung zu einem Server wurde angehalten. Der Name des Benutzers, der mit der VM-Sitzung verbunden war, ist in „dsTrapObjectUserName“ enthalten. Der Name des Servers, mit dem der Benutzer verbunden war, ist in „dsAvrTrapObjectServerName“ enthalten.

Trap-ID	Trap-Nachricht	Schweregrad	Beschreibung
40	Remote-Videositzung abgebrochen. Befehl erteilt von Benutzer: %s. Getrennter Benutzer: %s. Server: %s.	Information	Eine Virtual Media-Remote-Sitzung wurde von einem anderen Benutzer abgebrochen oder getrennt. Der Name des Benutzers, der die VM-Sitzung abgebrochen oder getrennt hat, ist in „dsTrapObjectUserName“ enthalten (falls verfügbar). Ist der Benutzername nicht verfügbar, wird eine leere Zeichenfolge gemeldet. Es ist kein Benutzername verfügbar, wenn die Remote-Sitzung über die OSCAR-Benutzeroberfläche abgebrochen oder getrennt wurde und die OSCAR-Benutzeroberflächen-Authentifizierung deaktiviert ist. Der Name des Benutzers, dessen VM-Sitzung abgebrochen oder getrennt wurde, ist in „dsTrapObjectTargetUserName“ enthalten. Der Name des Servers, mit dem der Benutzer verbunden war, ist in „dsTrapObjectServerName“ enthalten.
41	Virtual Media-Remote-Sitzung reserviert. Benutzer: %s. Server: %s.	Information	Ein Benutzer hat eine reservierte Virtual Media-Remote-Sitzung aufgebaut. Der Name des Benutzers, der eine reservierte Virtual Media-Sitzung aufgebaut hat, ist in „dsTrapObjectUserName“ enthalten. Der Name des Servers, mit dem der Benutzer verbunden war, ist in „dsTrapObjectServerName“ enthalten.

Trap-ID	Trap-Nachricht	Schweregrad	Beschreibung
42	Nicht-reservierte Virtual Media-Sitzung zu Server von Benutzer aufgebaut. Benutzer: %s. Server: %s.	Information	Eine nicht-reservierte Virtual Media-Remote-Sitzung wurde von einem Benutzer aufgebaut. Der Name des Benutzers, der eine nicht-reservierte Virtual Media-Sitzung aufgebaut hat, ist in „dsTrapObjectUserName“ enthalten. Der Name des Servers, mit dem der Benutzer verbunden war, ist in „dsTrapObjectServerName“ enthalten.
43	Virtual Media-Remote-Laufwerk zugewiesen. Benutzer: %s. Server: %s. Laufwerk-Typ: %s. Laufwerk-Zugriffsmodus: %s.	Information	Ein Virtual Media-Remote-Laufwerk wurde zugeordnet. Der Name des Benutzers, der die Virtual Media-Sitzung aufgebaut hat, ist in „dsTrapObjectUserName“ enthalten. Der Name des Servers, mit dem der Benutzer verbunden war, ist in „dsTrapObjectServerName“ enthalten. Der Typ des Laufwerks, das zugeordnet wurde, ist in „dsTrapObjectVirtualMediaDriveType“ enthalten. Der Zugriffsmodus für das zugeordnete Laufwerk ist in „dsTrapObjectVirtualMediaDriveAccessMode“ enthalten.

Trap-ID	Trap-Nachricht	Schweregrad	Beschreibung
44	Zuordnung von Remote-Virtual Media-Laufwerk aufgehoben. Benutzer: %s. Server: %s. Laufwerk-Typ: %s. Laufwerk-Zugriffsmodus: %s.	Information	Die Zuordnung eines Virtual Media-Remote Laufwerks wurde aufgehoben. Der Name des Benutzers, der die Virtual Media-Sitzung aufgebaut hat, ist in „dsTrapObjectUserName“ enthalten. Der Name des Servers, mit dem der Benutzer verbunden war, ist in „dsTrapObjectServerName“ enthalten. Der Typ des Laufwerks, dessen Zuordnung aufgehoben wurde, ist in „dsTrapObjectVirtualMediaDriveType“ enthalten. Der Zugriffsmodus für das Laufwerk, dessen Zuordnung aufgehoben wurde, ist in „dsTrapObjectVirtualMediaDriveAccessMode“ enthalten.
45	Virtual Media-Laufwerk am lokalen Port zugeordnet. Server: %s.	Information	Ein Virtual Media-Laufwerk wurde dem Server von einem Benutzer am lokalen Port zugeordnet. Die Sitzungskennung ist in „dsKvmTrapObjectSessionIdentifier“ enthalten. Der Typ des Laufwerks, dessen Zuordnung aufgehoben wurde, ist in „dsTrapObjectVirtualMediaDriveType“ enthalten. Der Zugriffsmodus für das Laufwerk, dessen Zuordnung aufgehoben wurde, ist in „dsTrapObjectVirtualMediaDriveAccessMode“ enthalten.

Trap-ID	Trap-Nachricht	Schweregrad	Beschreibung
46	Zuordnung von Virtual Media-Laufwerk am lokalen Port aufgehoben. Server: %s.	Information	Die Zuordnung eines Virtual Media-Laufwerks zum Server wurde von einem Benutzer am lokalen Port aufgehoben. Die Sitzungskennung ist in „dsTrapObjectSessionIdentifier“ enthalten. Der Typ des Laufwerks, dessen Zuordnung aufgehoben wurde, ist in „dsTrapObjectVirtualMediaDriveType“ enthalten. Der Zugriffsmodus für das Laufwerk, dessen Zuordnung aufgehoben wurde, ist in „dsTrapObjectVirtualMediaDriveAccessMode“ enthalten.
47	Lokale Videositzung abgebrochen. Befehl erteilt von Benutzer: %s. Server: %s.	Information	Eine lokale Virtual Media-Sitzung wurde von einem anderen Benutzer abgebrochen oder getrennt. Der Name des Benutzers, der die VM-Sitzung abgebrochen oder getrennt hat, ist in „dsTrapObjectUserName“ enthalten (falls verfügbar). Ist der Benutzername nicht verfügbar, wird eine leere Zeichenfolge gemeldet. Es ist kein Benutzername verfügbar, wenn die Remote-Sitzung über die OSCAR-Benutzeroberfläche abgebrochen oder getrennt wurde und die OSCAR-Authentifizierung deaktiviert ist. Der Name des Servers, mit dem der Benutzer verbunden war, ist in „dsTrapObjectServerName“ enthalten.
48	Lokale Virtual Media-Sitzung reserviert. Server: %s.	Information	Eine Virtual Media-Sitzung wurde von einem lokalen Benutzer reserviert. Der Name des Servers, mit dem der Benutzer verbunden war, ist in „dsTrapObjectServerName“ enthalten.

Trap-ID	Trap-Nachricht	Schweregrad	Beschreibung
49	Virtual Media-Sitzung am lokalen Port nicht reserviert. Server: %s.	Information	Die Reservierung einer lokalen Virtual Media-Sitzung wurde von einem Benutzer aufgehoben. Der Name des Servers, mit dem der Benutzer verbunden war, ist in „dsTrapObjectServerName“ enthalten.
50	Videositzung Am lokalen Port abgebrochen. Befehl erteilt von Benutzer: %s. Server: %s.	Information	Eine Videositzung am lokalen Port wurde von einem anderen Benutzer abgebrochen. Der Name des Benutzers, der die Sitzung abgebrochen hat, ist in „dsTrapObjectUserName“ enthalten. Die Sitzungskennung ist in „dsTrapObjectSessionIdentifier“ enthalten.
51	CA-Zertifikats-datei in den Remote Console Switch geladen. Befehl erteilt von Benutzer: %s.	Information	Der Remote Console Switch hat eine CA-Zertifikatsdatei geladen. Der Name des Benutzers, der dem Remote Console Switch den Befehl zum Laden der CA-Zertifikatsdatei erteilt hat, ist in „dsTrapObjectUserName“ enthalten.

D

Anhang D: FLASH-Aktualisierungen

Aktualisieren des Remote Console Switches

Die FLASH-Aktualisierungsfunktion des Remote Console Switches dient zur Aktualisierung Ihres Remote Console Switches mit der neuesten Firmware.

Sie können die Switch-Firmware entweder über eine serielle Konsole oder direkt über die OSCAR-Benutzeroberfläche oder über die integrierte Weboberfläche aktualisieren.

HINWEIS: Wenn die Option „Autom. SIP-Update aktivieren“ ausgewählt ist, werden alle angeschlossenen SIPs automatisch aktualisiert, wenn die Firmware aktualisiert wird. Weitere Informationen über das Aktivieren/Deaktivieren der Option „Autom. SIP-Update aktivieren“ finden Sie unter „Aktualisieren der Firmware des SIP-Moduls“ auf Seite 229.

Aktualisieren der Firmware über die integrierte Weboberfläche

Siehe „Aktualisieren der Firmware“ auf Seite 125.

Aktualisieren der Firmware mithilfe einer seriellen Konsole

Sie benötigen Folgendes für die Aktualisierung:

- Server, auf dem ein serielles Terminal-Programm ausgeführt wird
- Freier serieller Port (COM-Port) am Server
- Serielles Kabel
- Firmware-Update

So laden Sie eine neue FLASH-Datei hoch:

VORSICHT: Der Remote Console Switch startet den FLASH-Aktualisierungsprozess. Eine Anzeige auf dem Bildschirm gibt den Fortschritt der Aktualisierung an. Wenn der Upload beendet ist, setzt der Switch die internen Subsysteme zurück und führt die Aktualisierung durch.

1. Schließen Sie ein Terminal oder einen PC mit Terminal-Emulationssoftware an den Konfigurationsport auf der Geräterückseite des Remote Console Switches an. Das Terminal muss wie folgt eingestellt werden: 9600 bps, 8 bits, 1 stop bit, no parity und no flow control.

2. Schließen Sie den LAN-Port des Remote Console Switch an einen Ethernet-Hub an, der gleichzeitig mit dem PC verbunden ist, der als TFTP- oder FTP-Server verwendet wird.
3. Starten Sie sowohl die Server-TFTP- bzw. FTP-Software als auch die Terminal-Emulationssoftware.
4. Stellen Sie sicher, dass der Remote Console Switch eingeschaltet ist. Nach circa 40 Sekunden gibt der Remote Console Switch eine Meldung aus: **Dell Remote Console Switch bereit ... Drücken Sie eine beliebige Taste, um fortzufahren**. Drücken Sie eine beliebige Taste, um das Hauptmenü aufzurufen. Das Hauptmenü des Remote Console Switches wird angezeigt.
5. Sie benötigen nun die IP-Adresse des TFTP- bzw. FTP-Servers.
6. Weisen Sie die IP-Adresse im Remote Console Switch zu, falls erforderlich:
   a. Geben Sie im **HyperTerminal**-Fenster `1` ein, um die Netzwerkkonfiguration auszuwählen.
   b. Achten Sie auf die IP-Adresse des Remote Console Switches. Die ersten drei Ziffern müssen mit denen der IP-Adresse des Servers (Schritt 5) übereinstimmen. Die letzte Ziffer muss unterschiedlich sein. Ist die IP-Adresse des Remote Console Switches nicht korrekt, ändern Sie sie folgendermaßen: Geben Sie `3` ein, um die IP-Adresse auszuwählen, und geben Sie dann die richtige Adresse ein.
   c. Geben Sie `0` ein, um das Menü für die **Netzwerkkonfiguration** zu verlassen. Befolgen Sie die Anweisungen auf dem Bildschirm, wenn die IP-Adresse geändert wurde.
7. Geben Sie im Hauptmenü „2“ ein, um „Firmware-Management“ auszuwählen. Die aktuelle Version Ihrer Firmware wird im Bildschirm „Firmware-Management“ angezeigt.
8. Geben Sie im Menü **Firmware-Management** den Wert `1` ein, um **FLASH Download (TFTP)** auszuwählen, oder geben Sie „2“ ein, um **FLASH Download (FTP)** auszuwählen.
9. Geben Sie die IP-Adresse des TFTP- bzw. FTP-Servers ein und drücken Sie die <Eingabetaste>.
10. Geben Sie den Namen der FLASH-Datei ein und betätigen Sie die <Eingabetaste>.

11 Wenn Sie einen FTP-Server verwenden, geben Sie den Benutzernamen und das Kennwort für den FTP-Server ein und betätigen Sie die <Eingabetaste>.

12 Bestätigen Sie den TFTP- bzw. FTP-Download, indem Sie `y` oder `yes` eingeben und die <Eingabetaste> drücken.

13 Der Remote Console Switch prüft, ob die heruntergeladene Datei gültig ist. Sie werden aufgefordert, die Aktualisierung zu bestätigen. Geben Sie `y` oder `yes` ein, und drücken Sie die <Eingabetaste>.

14 Der Remote Console Switch startet den FLASH-Aktualisierungsprozess. Eine Anzeige auf dem Bildschirm gibt den Fortschritt der Aktualisierung an. Wenn der Upload abgeschlossen ist, setzt sich der Remote Console Switch zurück und aktualisiert die internen Subsysteme.

15 Wenn die Aktualisierung abgeschlossen ist, wird die Startmeldung aus Schritt 4 im Terminal-Bildschirm angezeigt.

Aktualisieren der Remote Console Switch Firmware über die OSCAR-Benutzeroberfläche

Sie können die Firmware-Version des Remote Console Switches direkt über die OSCAR-Benutzeroberfläche aktualisieren. Wenn Sie den IPv4-Modus verwenden, können Sie einen TFTP-Server oder einen FTP-Server verwenden. Im IPv6-Modus müssen Sie einen FTP-Server verwenden. Zum Aktualisieren der Firmware müssen Sie die IP-Adresse des Servers und den Dateinamen der Firmware-FLASH-Datei kennen. Wenn Sie einen FTP-Server verwenden, benötigen Sie zudem den Benutzernamen und das Kennwort für den FTP-Server. Darüber hinaus müssen Sie sicherstellen, dass sich die Datei im entsprechenden Ordner befindet.

So aktualisieren Sie die Remote Console Switch-Firmware:

1 Betätigen Sie die Taste <Druck>. Das **Hauptmenü** wird angezeigt.

2 Klicken Sie auf **Befehle – Versionen anzeigen**. Das Dialogfeld **Version** wird angezeigt.

3 Klicken Sie auf **Aktualisieren**. Das Dialogfeld **Herunterladen** wird angezeigt.

Abbildung D-1. Dialogfeld „Herunterladen“

4 Wenn Sie im IPv4-Modus einen TFTP-Server verwenden, wählen Sie **TFTP** aus.

– oder –

Wenn Sie im IPv4-Modus einen FTP-Server verwenden, wählen Sie **FTP** aus.

HINWEIS: Im IPv6-Modus wird die FTP-Schaltfläche automatisch ausgewählt. Die TFTP-Schaltfläche wird ausgeblendet und kann nicht ausgewählt werden.

5 Geben Sie im Feld **IP-Adresse** die IP-Adresse des TFTP- bzw. FTP-Servers ein, auf dem sich die FLASH-Datei für die Remote Console Switch-Firmware befindet.

6 Geben Sie im Feld **Dateiname** den Verzeichnispfad und den Dateinamen der Firmware-FLASH-Datei ein.

7 Wenn Sie einen FTP-Server verwenden, geben Sie den Benutzernamen und das Kennwort für den FTP-Server in den Feldern **Benutzername** und **Kennwort** ein.

8 Klicken Sie auf **Herunterladen.** Die Firmware-Aktualisierung wird ausgeführt.

9 Eine Warnmeldung wird angezeigt. Klicken Sie auf **OK** Wenn die Firmware-Aktualisierung abgeschlossen ist, wird der Remote Console Switch automatisch neu gestartet.

Wiederherstellen nach einer fehlgeschlagenen FLASH-Aktualisierung

HINWEIS: Das Wiederherstellen nach einer fehlgeschlagenen FLASH-Aktualisierung ist nur im IPv4-Modus möglich.

HINWEIS: Wenn die grüne LED-Betriebsanzeige auf der Vorder- und Rückseite des Remote Console Switch ohne Unterbrechung blinkt, befindet sich der Remote Console Switch im Wiederherstellungsmodus.

So führen Sie die Wiederherstellung nach einer fehlgeschlagenen Flash-Aktualisierung aus:

1. Laden Sie die neueste Flash-Firmware herunter.
2. Speichern Sie die Flash-Aktualisierungsdatei in dem entsprechenden Verzeichnis auf dem TFTP-Server.
3. Richten Sie den TFTP-Server mit der Server-IP-Adresse 10.0.0.3 ein.
4. Benennen Sie die heruntergeladene Datei in CMN-xxxx.fl um, wobei xxxx die Nummer auf dem Zulassungsschild an der Unterseite des Remote Console Switch bezeichnet. Speichern Sie die Datei dann im TFTP-Stammverzeichnis auf dem TFTP-Server.
5. Schalten Sie den Remote Console Switch ein, wenn er nicht schon eingeschaltet ist. Der Wiederherstellungsprozess sollte automatisch gestartet werden.

Aktualisieren der Firmware des SIP-Moduls

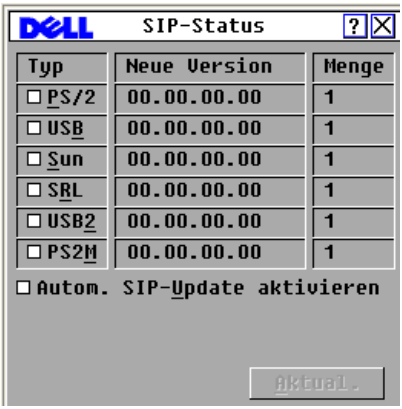
Die SIP-Module können einzeln oder gleichzeitig aktualisiert werden.

So aktualisieren Sie mehrere SIP-Module gleichzeitig:

1. Betätigen Sie die Taste <Druck>. Das **Hauptmenü** wird angezeigt.
2. Klicken Sie auf **Befehle – SIP-Status**. Das Dialogfeld **SIP-Status** wird angezeigt.

HINWEIS: Wenn die Option „Autom. SIP-Update aktivieren“ im Dialogfeld „SIP-Status“ ausgewählt ist, wird die SIP-Firmware automatisch dann aktualisiert, wenn die Remote Console Switch-Firmware aktualisiert wird oder wenn nach einer Firmware-Aktualisierung ein neues SIP vom Remote Console Switch erkannt wird. SIPs, die bereits erkannt wurden, aber während der Firmware-Aktualisierung nicht am Remote Console Switch angeschlossen sind, müssen manuell aktualisiert werden.

Abbildung D-2. Dialogfeld „SIP-Status“



3 Klicken Sie auf die zu aktualisierenden Modultypen. Klicken Sie auf **Aktualisieren**.

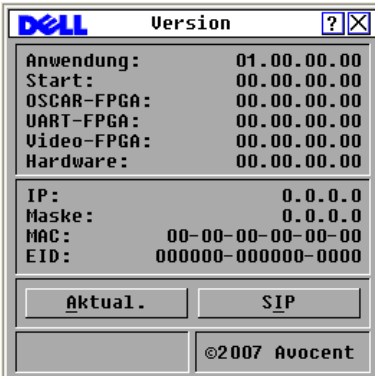
4 Das Dialogfeld **SIP-Aktualisierung** wird angezeigt. Klicken Sie auf **OK**, um die Aktualisierung zu starten und zum Dialogfeld **SIP-Status** zurückzukehren.

So aktualisieren Sie die Firmware für einzelne SIP-Module:

1 Betätigen Sie die Taste <Druck>. Das **Hauptmenü** wird angezeigt.

2 Klicken Sie auf **Befehle – Versionen anzeigen**. Das Dialogfeld **Version** wird angezeigt.

Abbildung D-3. Dialogfeld „Version“



3 Klicken Sie auf **SIP**, um Versionsinformationen zu individuellen SIP-Modulen anzuzeigen. Das Dialogfeld **SIP-Auswahl** wird angezeigt.

4 Wählen Sie ein SIP-Modul zur Aktualisierung aus und klicken Sie auf die Schaltfläche **Version**. Das Dialogfeld **SIP-Version** wird angezeigt.

5 Klicken Sie auf die Schaltfläche **Firmware laden**. Das Dialogfeld **SIP laden** wird angezeigt.

6 Klicken Sie auf **OK**, um die Aktualisierung zu starten und zum Dialogfeld SIP-Status **zurückzukehren**.

HINWEIS: Die SIP-Statusanzeige im Hauptmenü während einer Aktualisierung ist gelb. Das SIP-Modul ist während der Aktualisierung nicht verfügbar. Wenn eine Aktualisierung gestartet wird, werden alle aktuellen Verbindungen mit dem Server über das SIP-Modul beendet.

HINWEIS: Wenn Sie ein SIP auf die werkseitigen Einstellungen zurücksetzen möchten, klicken Sie im Dialogfeld „Version“ auf SIP. Das Dialogfeld „SIP-Version“ wird angezeigt. Klicken Sie auf „Zurücksetzen“ und dann auf „OK“, um das SIP auf die werkseitigen Einstellungen zurückzusetzen.

E

Anhang E: Technische Daten

Tabelle E-1. 2161DS-2/4161DS Remote Console Switch – Produktspezifikationen

Serverports	
Anzahl	16
Typen	Dell PS/2- und USB-SIP-Module; Avocent PS/2-, PS2M-, USB-, Sun- und serielle IQ-Module
Anschlüsse	RJ-45
Sync-Arten	Unabhängig horizontal und vertikal
Plug and Play	DDC2B
Bildschirmauflösung	Analogport max.: 1280 x 800 bei 60Hz
Netzwerkkonfigurationsport	
Anzahl	1
Typ	Seriell RS-232
Stecker	DB9-Buchse
Analogports	
Anzahl	1
Typ	PS/2, USB, VGA und ACI
Anschlüsse	PS/2 miniDIN, 15-polig D, RJ-45
Abmessungen	
Abmessungen (H x B x T)	4,45 x 43,18 x 27,94 cm, Formfaktor 1 HE (1,75 x 17,00 x 11,00 Zoll)
Gewicht	3,6 kg ohne Kabel
Wärmeabstrahlung	92 BTU/Std
Luftzufuhr	8 Kubikfuß pro Minute (cfm)
Stromverbrauch	12,5 W

Tabelle E-1. 2161DS-2/4161DS Remote Console Switch – Produktspezifikationen (Fortsetzung)

Wechselstrom-Eingangsleistung	Max. 40 W
Wechselstrom-Eingangsspannung	100 bis 240 V AC, automatische Umschaltung
Wechselstrom-Eingangsspannungswert	0,5 A
Wechselstrom-Stromversorgungskabel	Dreiadriges 18 AWG-Kabel mit dreipoliger IEC-320-Buchse am Stromzuführungsende und länder- oder gebietsabhängigem Stecker am Stromquellenende
Wechselstromfrequenz	50/60 Hz
Temperatur	0bis 50 °Celsius (32 bis 122 °Fahrenheit) bei Betrieb -20 bis 60 °Celsius (-4 bis 140 °Fahrenheit) nicht in Betrieb
Luftfeuchtigkeit	20 bis 80 %, nicht kondensierend, in Betrieb 5 bis 95 %, nicht kondensierend, nicht in Betrieb
Sicherheits- und EMV-Zulassungen und -Kennzeichnungen	
	UL / cUL, CE – EU, N (Nemko), GOST, C-Tick, NOM / NYCE, MIC (BCC), SASO, TUV-GS, IRAM, FCC, ICES, VCCI, SoNCAP, SABS, Bellis, FIS / Kvalitet, Koncar, CKT, INSM, Ukrtest, STZ

Tabelle E-2. 2321DS Remote Console Switch – Produktspezifikationen

Remote Console Switch – Technische Daten	
Serverports	
Anzahl	32
Typen	Dell PS/2- und USB-SIP-Module; Avocent PS/2-, PS2M-, USB-, Sun- und serielle IQ-Module
Anschlüsse	RJ-45
Sync-Arten	Unabhängig horizontal und vertikal
Plug and Play	DDC2B
Bildschirmauflösung	Analogport max.: 1280 x 800 bei 60 Hz

Tabelle E-2. 2321DS Remote Console Switch – Produktspezifikationen (Fortsetzung)

Remote Console Switch – Technische Daten	
Netzwerkkonfigurationsport	
Anzahl	1
Typ	Seriell RS-232
Stecker	RJ-45
Analogports	
Anzahl	1
Typ	PS/2, USB, VGA und ACI
Anschlüsse	PS/2 miniDIN, 15-polig D, RJ-45
Serieller Port für die Stromüberwachung (PDU)	
Anzahl	2
Typ	RS-232 seriell
Stecker	8-polig modular (RJ45)
Abmessungen	
Abmessungen (H x B x T)	4,37 x 43,18 x 35,62 cm, Formfaktor 1 HE (1,72 x 17,00 x 14,025 Zoll)
Gewicht	4,5 kg ohne Kabel
Wärmeabstrahlung	45,0 BTU/Std.
Luftzufuhr	8 Kubikfuß pro Minute (cfm)
Stromverbrauch	13,2 W
Wechselstrom-Eingangsleistung	Max. 40 W
Wechselstrom-Eingangsspannung	100 bis 240 V AC, automatische Umschaltung
Wechselstrom-Eingangsspannungswert	1,25 A
Wechselstrom-Stromversorgungskabel	Dreiadriges 18 AWG-Kabel mit dreipoliger IEC-320-Buchse am Stromzuführungsende und länder- oder gebietsabhängigem Stecker am Stromquellenende
Wechselstromfrequenz	50/60 Hz

Tabelle E-2. 2321DS Remote Console Switch – Produktspezifikationen (Fortsetzung)

Remote Console Switch – Technische Daten	
Temperatur	0 bis 50 °Celsius (32 bis 122 °Fahrenheit) bei Betrieb -20 bis 60 °Celsius (-4 bis 140 °Fahrenheit) nicht in Betrieb
Luftfeuchtigkeit	20 bis 80 %, nicht kondensierend, in Betrieb 5 bis 95 %, nicht kondensierend, nicht in Betrieb
Sicherheits- und EMV-Zulassungen und -Kennzeichnungen	
	UL / cUL, CE – EU, N (Nemko), GOST, C-Tick, NOM / NYCE, MIC (BCC), SASO, GS, IRAM, FCC, ICES, VCCI, SoNCAP, SABS, Bellis, FIS / Kvalitet, Koncar, KUCAS, INSM, Ukrtest, STZ

F

Anhang F: Technischer Kundendienst

Unser technischer Kundendienst steht Ihnen jederzeit bei Fragen hinsichtlich Installations- oder Betriebsproblemen mit Ihrem Produkt von Dell zur Verfügung. Verfahren Sie wie folgt zur schnellstmöglichen Problemlösung.

So gehen Sie zur Problemlösung vor:

1. Sehen Sie im entsprechenden Abschnitt der Betriebsanleitung nach, ob das Problem mit den vorgeschlagenen Abhilfemaßnahmen gelöst werden kann.
2. Besuchen Sie unsere Website unter **www.dell.com/support**, um auf die Knowledge Base zuzugreifen oder die Online-Serviceanforderung in Anspruch zu nehmen.
3. Wenden Sie sich an den technischen Kundendienst von Dell in Ihrer Nähe.

Stichwortverzeichnis

O

P

R

S

T

U

V

Z