Dell™ Remote Console Switch-System

Benutzerhandbuch

Wichtige Hinweise, Vorsichtsmaßnahmen und Warnhinweise

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

VORSICHT: VORSICHT weist auf mögliche Hardware-Schäden oder Datenverlust hin, wenn die Anweisungen nicht befolgt werden.

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

590-1021-503C

Modell 1082DS/2162DS/4322DS Remote Console Switch

Juli 2012

Inhalt

1

Produktüberblick

Die Dell 1082DS2162/4322DS/DS RCS (RCS) digitalen Tastatur-, Video- und Maus-(KVM)-over-IP- sowie seriellen Konsolen-Switches verbinden analoge und digitale Technologie für eine flexible, zentralisierte Steuerung von Servern im Rechenzentrum und vereinfachen Betrieb, Aktivierung und Wartung von Remote-Zweigstellen, für die keine ausgebildeten Bediener zur Verfügung stehen. Das IP-basierte RCS ermöglicht Ihnen über die RCS-Software oder die integrierte Weboberfläche (OBWI) eine flexible Zielgeräteverwaltung und einen gesicherten Remote-Zugriff zu jeder Zeit und von jedem beliebigen Ort.

Merkmale und Vorteile

Der RCS bietet Unternehmenskunden die folgenden Merkmale und Optionen:

- erhebliche Reduzierung des Kabelvolumens
- Virtual Media-Funktionalität (VM), konfigurierbar für analoge (lokale) und digitale (Remote) Konnektivität
- Smart Card-/Common Access Card (CAC)-Funktion
- echte serielle Funktionalität über Secure Shell (SSH) und Telnet
- erweiterte Unterstützung für Bildschirmauflösungen bis zu 1600 x 1200 oder 1680 x 1050 (Breitbild), nativ von Ziel zu Remote
- optionale Dual-Stromversorgung für bessere Redundanz
- optionale Unterstützung zur Verwaltung von intelligenten Stromverwaltungsgeräten
- duale, unabhängige Videopfade am lokalen Port (dediziert auf ACI)

- Dual-Stack-IPv4 (DHCP) und IPv6 (DHCPv6 und statusfreie Auto-Konfiguration) für simultanen Zugriff
- Zugriffsmöglichkeit auf Zielgeräte über 10/100/1000BaseT-LAN-Ports
- ein Modem-Port, der V.34-, V.90- oder V.92-kompatible Modems unterstützt, die verwendet werden können, wenn eine Ethernet-Verbindung nicht verfügbar ist
- FIPS Support

Verringern des Kabelvolumen

Mit stetig wachsenden Serverdichten stellt das Kabelvolumen immer noch eines der Hauptprobleme für Netzwerkadministratoren dar. Der RCS verringert den KVM-Kabelaufwand im Rack deutlich, indem er innovative SIP-Module und einfache UTP-Kabel nach Industriestandard verwendet. Dies erlaubt eine höhere Serverdichte und bietet dennoch erhöhten Luftdurchfluss und eine bessere Kühlkapazität.

KVM-Switching-Funktionen

Der RCS unterstützt SIPs, die direkt vom Zielgerät mit Strom versorgt werden und eine Keep Alive-Funktionalität bieten, wenn der Switch nicht mit Strom versorgt wird. Die SIPs mit CAT 5-Design reduzieren das Kabelaufkommen entscheidend und bieten gleichzeitig optimale Bildschirmauflösungen und Monitoreinstellungen. Der integrierte Speicher der SIPs vereinfacht die Konfiguration durch Zuweisen und Speichern eindeutiger Gerätenamen oder elektronischer Kennnummern (EID) für jedes angeschlossene Gerät.

Es sind PS/2- und USB-SIPs erhältlich, die eine direkte KVM-Konnektivität zu Geräten ermöglichen. Zudem steht ein USB2+CAC-SIP zur Verfügung. Der RCS ist mit 8, 16 oder 32 Analog Rack Interface (ARI)-Ports ausgestattet, an die SIPs angeschlossen werden können. Mit dem SIP kann das RCS-System mit zusätzlichen Switches erweitert werden. Mit dieser Flexibilität kann die Leistungsfähigkeit Ihres Systems an zunehmende Datenmengen angepasst werden.

Multi-Plattform-Support

Die für die Verwendung mit dem RCS erhältlichen Dell SIPs unterstützen PS/2-, USB-, USB-2 und USB2+CAC-Geräteumgebungen. Wenn diese Module in Verbindung mit OBWI eingesetzt werden, ist ein einfaches Wechseln zwischen Plattformen möglich.

Zum Anschluss von Geräten an den RCS kann auch auf die Interoperabilität mit der intelligenten Verkabelung des Avocent® IQ-Moduls zurückgegriffen werden. Erhältlich sind PS/2-, USB-, Sun®- und serielle Moduloptionen. Weitere Informationen entnehmen Sie der entsprechenden Avocent Installations- und Bedienungsanleitung für Ihr Produkt oder besuchen Sie die Website www.avocent.com/manuals.

Echte serielle Fähigkeiten

Der RCS unterstützt SIPs, die echte serielle Funktionalität über Telnet bieten. Mithilfe eines SIP können Sie über die OBWI eine SSH-Sitzung eröffnen oder einen seriellen Viewer starten, um eine Verbindung mit an einen RCS angeschlossenen seriellen Zielgeräten herzustellen.

Lokale und Remote-Benutzeroberflächen

Sie können über die lokale Benutzeroberfläche eine direkte Verbindung mit dem lokalen Port herstellen, um den RCS zu verwalten. Sie können auch die integrierte Weboberfläche remote verwenden, um Ihren Switch zu verwalten. Die integrierte Weboberfläche ist browserbasiert und wird direkt vom Switch aus aufgerufen. Alle Geräte, die an den Switch angeschlossen sind, werden automatisch erkannt.

Virtual Media- und Smart Card-fähige Switches

Der RCS ermöglicht das Anzeigen von auf virtuellen Speichergeräten gespeicherten Daten auf einem beliebigen Zielgerät. Außerdem können die Daten von den Speichergeräten auf das Zielgerät 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 Backups von Zielgeräten über Remote-Zugriff ermöglicht werden.

Der RCS ermöglicht außerdem die Verwendung von Smart Cards in Verbindung mit Ihrem Switch-System. Smart Cards sind Karten im Taschenformat, die Daten speichern und verarbeiten. Smart Cards, wie z. B. CAC, können für die Speicherung von Identifizierungs- und Authentifizierungsinformationen verwendet werden, um Zugriff bzw. Zugang zu Computern, Netzwerken und gesicherten Räumen und Gebäuden zu erhalten.

Virtual Media- und Smart Card-Lesegeräte können direkt an die USB-Ports des Switches angeschlossen werden. Darüber hinaus können Virtual Media- und Smart Card-Lesegeräte an alle Remote-Workstations angeschlossen werden, auf denen die Remote-OBWI, die Dell RCS-Software oder die Avocent-Managementsoftware ausgeführt wird und die über eine Ethernet-Verbindung an den Switch angeschlossen sind.

HINWEIS: Um eine Virtual Media- oder Smart Card-Sitzung mit einem Zielgerät zu öffnen, muss das Zielgerät zunächst mit einem SIP an den Switch angeschlossen werden.

Integrierte Weboberfläche

Die OBWI bietet ähnliche Managementfunktionen wie die RCS-Software, erfordert jedoch weder Software-Server noch Installation. Die OBWI wird direkt über den Switch gestartet, und alle eventuell an den RCS angeschlossenen Server werden automatisch erkannt. Mithilfe der OBWI können Sie den RCS über einen Webbrowser konfigurieren. Rufen Sie den Viewer über die OBWI auf, um eine KVM- und Virtual Media-Sitzung mit den Zielgeräten einzurichten. Die OBWI unterstützt zudem auch die LDAP-Authentifizierung, welche die Verwaltung von Berechtigungen für mehrere RCSs über eine einzige Schnittstelle ermöglicht.

Zugriff auf den Switch über ein standardmäßiges TCP/IP-Netzwerk

Der Switch bietet agentenlosen Remote-Zugriff und Remote-Steuerung. Für angeschlossene Server oder Clients werden keine speziellen Softwareprogramme

oder Treiber benötigt.

HINWEIS: Der Client stellt über einen Internetbrowser eine Verbindung mit dem Switch her.

Sie können über Ethernet oder über ein V.34, V.90 oder V.92-Modem von einem Client-Computer aus auf den Switch und alle angeschlossenen Systeme zugreifen. Die Client-Computer können überall dort aufgestellt sein, wo sich eine gültige Netzwerkverbindung befindet.

Verschlüsselung

Der RCS unterstützt 128-Bit-SSL(ARCFOUR)- sowie AES-, DES- und 3DES-Verschlüsselung von Tastatur-/Maus-, Video- und Virtual Media-Sitzungen.

Bildschirm

Der RCS bietet eine optimale Bildschirmauflösung für Analog-VGA, -SVGA und XGA. Je nach Kabelabstand zwischen Switch und Servern können Auflösungen von bis zu 1600 x 1200 bzw. 1680 x 1050 (Breitbildformat) erzielt werden.

Flash-aktualisierbar

Sie können Ihren RCS und die SIPs jederzeit aktualisieren und damit gewährleisten, dass Ihr System immer mit der neuesten Firmware-Version ausgeführt wird. Flash-Upgrades können über die OBWI oder über die serielle Konsole gestartet werden. Der RCS kann so konfiguriert werden, dass er automatische Firmware-Aktualisierungen der SIPs durchführt. Nähere Informationen finden Sie unter „RCS-Firmware aktualisieren“ auf Seite 55.

Gestufte Erweiterung

Der RCS ermöglicht eine Stufung mit zusätzlichen Dell RCSs über jeden ARI-Port (Analog Rack Interface) am Switch. Die gestuften Switches werden genau wie andere Geräte angeschlossen. Mithilfe dieser zusätzlichen gestuften Einheiten können Sie bis zu 1024 Server in einem System verbinden. Siehe „Hinzufügen eines gestuften Switches“ auf Seite 33.

Avocent-Management Software Plug-In

Die Avocent-Managementsoftware kann in Verbindung mit dem Switch verwendet werden, um es IT-Administratoren zu ermöglichen, mit Remote-Zugriff über eine einzige, webbasierte Benutzeroberfläche auf Zielgeräte auf mehreren Plattformen zuzugreifen und diese zu überwachen und zu steuern. Nähere Informationen entnehmen Sie der Technischen Anleitung zur Avocent-Managementsoftware.

Verschlüsselungsmodul gemäß FIPS

Die RCS-Switches unterstützen die Verschlüsselungsanforderungen gemäß FIPS 140-2 Level 1. Der FIPS-Modus kann über die OBWI oder den lokalen Port aktiviert bzw. deaktiviert und nach einem Neustart ausgeführt werden. Wenn der FIPS-Modus aktiviert ist, dauert ein Neustart des Switches etwa zwei Minuten länger, da eine Integritätsprüfung durchgeführt wird. Wenn für Tastatur-, Maus- oder Videosignale 128-Bit-SSL (ARCFOUR) oder DES als Verschlüsselungsebene ausgewählt ist, wird die Verschlüsselungsebene bei aktiviertem FIPS-Modus automatisch in AES geändert.

HINWEIS: Der FIPS-Modus ist anfänglich deaktiviert und muss erst aktiviert werden.

HINWEIS: Das FIPS-Modul wird durch die Werkseinstellung für den Setup-Port automatisch deaktiviert.

HINWEIS: Der FIPS-Modus kann über das DSView Software-Plug-in geändert werden.

RCS-Switches verwenden ein integriertes, nach FIPS 140-2 validiertes Kryptografiemodul (Zertifikat-Nr. 1051), das auf einer Linux PPC-Plattform gemäß FIPS 140-2 Implementation Guidance, Abschnitt G.5 ausgeführt wird.

Der FIPS-Modus kann über die OBWI, den lokalen Port oder das DSView Plug-in aktiviert bzw. deaktiviert werden. Zur Aktivierung bzw. Deaktivierung des FIPS-Modus ist ein Neustart erforderlich. Durch eine Firmware-Aktualisierung auf diese Version oder das Zurücksetzen in den Standardzustand (Menü „Setup-Port“) wird der FIPS-Modus deaktiviert.

Im FIPS-Modus sind die Verschlüsselungscodes auf AES oder 3DES beschränkt. Wenn für Tastatur-, Maus- oder Videosignale 128-Bit-SSL oder DES als

Verschlüsselungsebene ausgewählt ist, wird die Verschlüsselungsebene bei aktiviertem FIPS-Modus automatisch zu AES geändert. Bei aktiviertem FIPS-Modus werden diese Dateien über einen FIPS-kompatiblen Algorithmus, AES, gespeichert (bzw. wiederhergestellt). Wenn der FIPS-Modus deaktiviert wird, werden die Dateien der Benutzerdatenbank und zur Gerätekonfiguration, die als externe Dateien auf das Gerät gespeichert oder davon wiederhergestellt werden, über DES verschlüsselt (bzw. entschlüsselt).

Das gilt auch dann, wenn der Benutzer für den Parameter „Kennwort“ im Dialogfeld „Speichern“ (oder „Laden“) in der OBWI keine Angabe macht. In diesem Fall wird für die Ver- bzw. Entschlüsselung ein vom OEM vergebenes Kennwort verwendet.

Eine Folge der Aktivierung des FIPS-Moduls ist, dass zuvor gespeicherte Dateien aus Benutzerdatenbanken und zur Gerätekonfiguration nicht länger kompatibel sind. In diesem Fall können Sie das FIPS-Modul vorübergehend deaktivieren, die Einheit neu starten, die zuvor gespeicherte Datenbank- oder Konfigurationsdatei wiederherstellen, das FIPS-Modul wieder aktivieren, einen Neustart durchführen und die Datei anschließend bei aktiviertem FIPS-Modul erneut extern speichern. Die neu gespeicherte, externe Datei ist mit der Einheit kompatibel, solange die Einheit mit aktiviertem FIPS-Modus betrieben wird.

Das Gegenteil trifft ebenfalls zu. Datenbank- und Konfigurationsdateien, die bei aktiviertem FIPS-Modul gespeichert werden, sind nicht kompatibel zur Wiederherstellung auf einer Einheit ohne aktiviertes FIPS-Modul oder einer Einheit mit älterer Firmware, von der das FIPS-Modul nicht unterstützt wird.

Beispielkonfiguration

Abbildung 1.1. Beispielkonfiguration für einen RCS

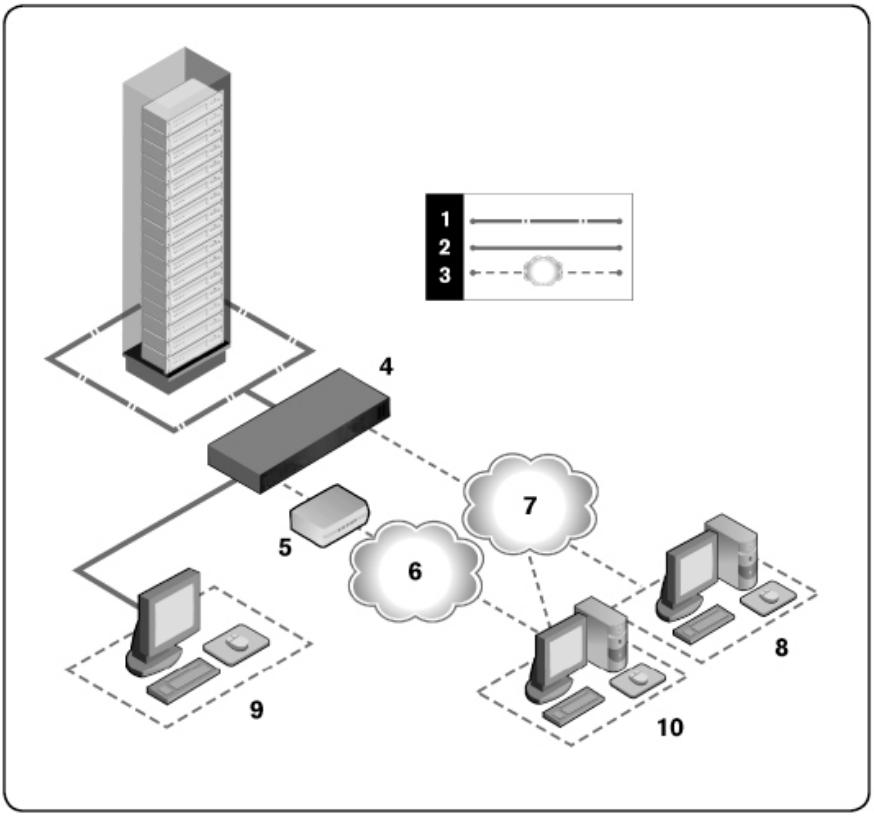


Tabelle 1.1: Beschreibungen für Abbildung 1.1

Nummer	Beschreibung	Nummer	Beschreibung
1	UTP-Verbindung	6	Telefonnetz
2	KVM-Verbindung zum RCS	7	Ethernet
3	Remote-IP-Verbindung	8	Avocent-Managementsoftware-Server
4	RCS	9	Analoger Benutzer (lokale Benutzeroberfläche)
5	Modem	10	Digitaler Benutzer (Computer mit Internet-Browser für Remote-OBWI oder Dell RCS-Software)

Sicherheitsvorkehrungen

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

VORSICHT: Die Stromversorgung Ihres Systems kann möglicherweise hohe Spannungen und Energiegefahrenquellen erzeugen, die Verletzungen verursachen können. Nur autorisierte Wartungstechniker dürfen Abdeckungen entfernen und auf Komponenten innerhalb des Systems zugreifen. Dieser Warnhinweis gilt für Dell™ Remote Console Switch, Dell™ PowerEdge™ Server und Dell PowerVault™ Speichersysteme.

Dieses Dokument bezieht sich nur auf den Dell 1082DS/2162DS/4322DS Remote Console Switch. Sie sollten außerdem die ergänzenden Sicherheitsanweisungen lesen und befolgen.

- Benutzerhandbuch für den Dell Remote Console Switch

- Dell Sicherheitsdatenblatt
- Dell RTF regulatorisches technisches Datenblatt

Allgemeine Sicherheitshinweise

- Beachten und befolgen Sie die Wartungsbeschriftungen.
- Warten Sie die 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 dürfen 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 Stromversorgung des Produkts 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 ist mit Wasser in Kontakt gekommen.
- Das Produkt ist heruntergefallen und/oder wurde beschädigt.
- Das Produkt arbeitet bei Befolgen der Bedienungsanleitung nicht ordnungsgemäß.

- - 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 Produkt 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.

HINWEIS: Um Schäden am System zu vermeiden, stellen Sie sicher, dass der Spannungswahlschalter (falls vorhanden) an der Stromversorgung auf die Spannung eingestellt ist, die der Wechselstromspannung in Ihrer Region am nächsten kommt. Stellen Sie auch sicher, dass der Bildschirm und die angeschlossenen Geräte mit der geeigneten Stromversorgung betrieben werden.

- Stellen Sie sicher, dass der Bildschirm und die angeschlossenen Geräte mit der am Standort verfügbaren Stromversorgung entsprechend ihrer Nennwerte betrieben werden können.
- Verwenden Sie nur die mit dem Produkt gelieferten Stromkabel.
- 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 keinesfalls den Erdungsanschluss eines Kabels.
- 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 Überspannungsschutzes, Spannungsstabilisierers 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 Änderungen an Stromkabeln und Steckern vor. Nehmen Sie bzgl. baulicher Änderungen Kontakt mit einem qualifizierten Elektriker oder Ihrer Elektrizitätsgesellschaft auf. Befolgen Sie stets die maßgeblichen Verkabelungsvorschriften.

LAN-Optionen

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

2

Installation

Der RCS übermittelt KVM- und serielle Informationen zwischen Bedienern und mit dem Switch verbundenen Zielgeräten entweder über eine Ethernet- oder eine lokale Verbindung. Der RCS verwendet TCP/IP für die Kommunikation über Ethernet. Die beste Leistung wird durch die Verwendung eines dedizierten, geswitchten 100BaseT- oder 1000BaseT-Netzwerks erzielt. Sie können auch 10BaseT-Ethernet verwenden.

Der RCS verwendet das Point-to-Point-Protokoll (PPP) zur Kommunikation über ein V.34, V.90 oder V.92-Modem. Mithilfe von OBWI oder der Avocent-Managementsoftware können KVM- und serielle Switching-Aufgaben ausgeführt werden. Weitere Informationen zur Avocent-Managementsoftware erhalten Sie unter http://www.avocent.com.

Das RCS-Paket enthält den RCS, die RCS-Software und die OBWI. Nach Wahl können Sie entweder die RCS-Software oder die OBWI zur Verwaltung Ihres Systems nutzen. Über die OBWI können Sie einen einzelnen RCS und dessen Anschlüsse, über die RCS-Software hingegen mehrere Switches und deren Anschlüsse verwalten. Sollten Sie nur die OBWI verwenden wollen, müssen Sie die RCS-Software nicht installieren.

HINWEIS: Die RCS-Software kann zum Verwalten bestimmter Switches verwendet werden. Weitere Informationen entnehmen Sie der entsprechenden Installations- und Bedienungsanleitung für Ihr Produkt.

HINWEIS: Stellen Sie sicher, dass alle RCSs auf die entsprechende aktuelle Firmware-Version aktualisiert wurden. Nähere Informationen zur Aktualisierung eines RCS über die OBWI finden Sie unter „RCS-Extras“ auf Seite 54.

RCS-Schnelleinrichtung

Nachfolgend sehen Sie eine Auflistung für die Schnelleinrichtung. Die ersten Schritte zum Einbau des RCS in ein Rack und nähere Installationsanweisungen entnehmen Sie dem Abschnitt „Vor der Installation“ auf Seite 15.

1 Stellen Sie die Mausbeschleunigung auf jedem Server auf „Langsam“ oder „Keine“ ein.

2 Installieren Sie die RCS-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 RCS an und schließen Sie die Tastatur-, Monitor- und Mausstecker an den Analogport des RCS an.

3 Verbinden Sie die Peripheriegeräte des lokalen Ports mit den entsprechenden Anschlüssen an der Rückseite des RCS und führen Sie die Netzwerk-Konfiguration durch. Die IP-Adresse kann hier oder über die RCS-Software eingestellt werden. Zur einfacheren Konfiguration empfiehlt Dell die Verwendung einer statischen IP-Adresse.

4 Geben Sie unter Verwendung des lokalen Ports alle Servernamen über die OBWI-Benutzeroberfläche ein.

So richten Sie die RCS-Software ein (siehe auch Benutzerhandbuch für die RCS-Software):

1 Installieren Sie die RCS Software auf jeder Client-Workstation.

2 Starten Sie die RCS-Software von einer Client-Workstation.

3 Klicken Sie auf die Taskschaltfläche **Neuer RCS**, um der RCS-Software-Datenbank einen neuen Switch hinzuzufügen. Wenn Sie die IP-Adresse wie oben beschrieben konfiguriert haben, wählen Sie **Ja**, das Produkt hat bereits eine IP-Adresse aus. Andernfalls wählen Sie **Nein**, das Produkt hat keine IP-Adresse.

Die RCS-Software sucht alle angeschlossenen RCSs und SIPs und zeigt deren Namen im Explorer an.

HINWEIS: Neben Hinzufügen und Verwalten von Dell RCSs mithilfe der RCS-Software können Sie auch einige Avocent-Switches hinzufügen und verwalten.

4 Stellen Sie die Eigenschaften und Gruppenserver nach Ihren Wünschen mit dem Explorer unter Aufstellungsort, Standort oder Verzeichnis ein.

5 Erstellen Sie Benutzerkonten in der OBWI. Nähere Informationen finden Sie unter „Einrichten von Benutzerkonten“ auf Seite 83.

6 Sobald eine Client-Workstation eingerichtet ist, wählen Sie **Datei – Datenbank – Speichern** aus, um eine Kopie der Datenbank mit allen Einstellungen zu speichern.

7 Klicken Sie an der zweiten Client-Workstation auf **Datei – Datenbank – Laden** und suchen Sie die gespeicherte Datei. Markieren Sie die Datei und klicken Sie auf „Laden“.

8 Wenn der lokale Benutzer SIPs hinzufügt, löscht oder umbenennt, nachdem Sie diese Datei hochgeladen haben, können Sie Ihren lokalen Switch neu synchronisieren. Wählen Sie dazu den RCS aus und klicken Sie auf **Resynchronisieren**. Um einen angeschlossenen Server zu steuern, wählen Sie ihn im Explorer aus und klicken Sie auf die Taskschaltfläche **Video verbinden**, um eine Serversitzung im Viewer zu starten.

9 Stellen Sie die Auflösung (Ansicht – Skalierung) und Qualität (Ansicht – Farben) des Servervideos im Viewer ein.

Vor der Installation

Im Lieferumfang des Remote Console Switches sind die folgenden Elemente enthalten. Legen Sie vor der Installation des RCS die erforderlichen Elemente bereit, um eine ordnungsgemäße Installation zu gewährleisten.

- Remote Console Switch
- Brückenkabel
- 0-HE-Befestigungshalterung

- Hardware-Kit für die 1-HE Befestigungshalterung (der Kit-Bausatz enthält zwei zusätzliche Schienen, die vorab am RCS montiert sind)
- Kabel und Adapter für SETUP und MODEM
- Benutzerhandbuch auf CD-ROM für das Remote Console Switch-System
- Dell Sicherheitsdatenblatt
- Dell RTF regulatorisches technisches Datenblatt

Zusätzlich benötigte Teile:

- Ein Dell SIP- oder Avocent IQ-Modul pro angeschlossenem Gerät
- Ein CAT 5-Patchkabel pro angeschlossenem Gerät (bis zu 45 Meter)

Optionales Zubehör:

- V.34-, V.90- oder V.92-kompatibles Modem und Kabel
- Stromverwaltungsgerät(e)
- Port Expansion Module (PEM)

HINWEIS: Ist der Server über ein PEM angeschlossen, können Sie keine Virtual Media- oder CAC-Sitzung öffnen.

Netzwerk-Setup

Der Switch verwendet IP-Adressen, um den Switch und die Zielgeräte eindeutig zu identifizieren. Der RCS unterstützt sowohl DHCP (Dynamic Host Configuration Protocol) als auch die statische IP-Adressvergabe. Stellen Sie sicher, dass für jeden Switch eine IP-Adresse reserviert ist und dass die IP-Adressen statisch bleiben, wenn der Switch an das Netzwerk angeschlossen ist.

Tastaturen

An den Analogport des RCS kann eine USB-Tastatur und -Maus angeschlossen werden.

HINWEIS: Der RCS 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.

Rack-Montage des RCS

Sie können den RCS entweder im Rackgestell oder direkt in einem 19 Zoll breiten, EIA-310-E-kompatiblen Rack (mit 4 Stützen, 2 Stützen oder Gewindebohrung) installieren. Das Dell ReadyRails™-System eignet sich für die Montage-Optionen 1-HE-Front-Rack, 1-HE-Heck-Rack und mit 2 Stützen. Das ReadyRails-System beinhaltet zwei separat verpackte Schienen-Bausätze und zwei Schienen, die bereits an den Seiten des RCS vorinstalliert sind. Darüber hinaus enthält der Lieferumfang eine Befestigungshalterung für 0-HE-Konfigurationen sowie eine Verblendung für Heck-Rack-Installationen.

⚠ **WARNUNG: Hierbei handelt es sich um eine gekürzte Produktbeschreibung. Lesen Sie deshalb vor der Installation die vollständigen Sicherheitsanweisungen in der Broschüre mit Sicherheits-, Umwelt- und rechtlichen Informationen.**

HINWEIS: Die in diesem Dokument gezeigten Abbildungen beziehen sich auf keinen spezifischen Switch.

Sicherheitsvorkehrungen bei Rackbefestigung

- Rackbelastung: Überladung oder ungleichmäßige Rackbestückung kann zur Beschädigung von Regalen oder des Racks führen und mögliche Personenschäden nach sich ziehen. Vor dem Bestücken müssen die Racks an ihren vorgesehenen Standorten stabilisiert werden. Das Rack muss von unten nach oben mit Komponenten bestückt werden. Die Rack-Belastungswerte dürfen nicht überschritten werden.
- Überlegungen zur Stromversorgung: Schließen Sie das Gerät nur an eine auf der Einheit angegebene Stromversorgung an. Achten Sie bei der Installation von mehreren elektrischen Komponenten in einem Rack darauf, dass die Gesamtstromaufnahme die Stromkreiskapazität nicht übersteigt. Überlastete Stromversorgungen und Verlängerungskabel stellen eine erhöhte Brand- und Stromschlaggefahr dar.
- Erhöhte Umgebungstemperaturen: 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 für

den Switch maximal zulässige Umgebungstemperatur von 50 °C 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.
- Zuverlässige Geräteerdung: Stellen Sie sicher, dass rackmontierte Geräte stets zuverlässig geerdet sind. Achten Sie vor allem auf Versorgungsanschlüsse, die nicht direkt an den Verzweigungsschaltkreis angeschlossen sind (z. B. Verwendung von Mehrfachsteckdosen).
- Das Gerät sollte nicht so installiert werden, dass die hintere Gehäuseplatte nach unten zeigt.

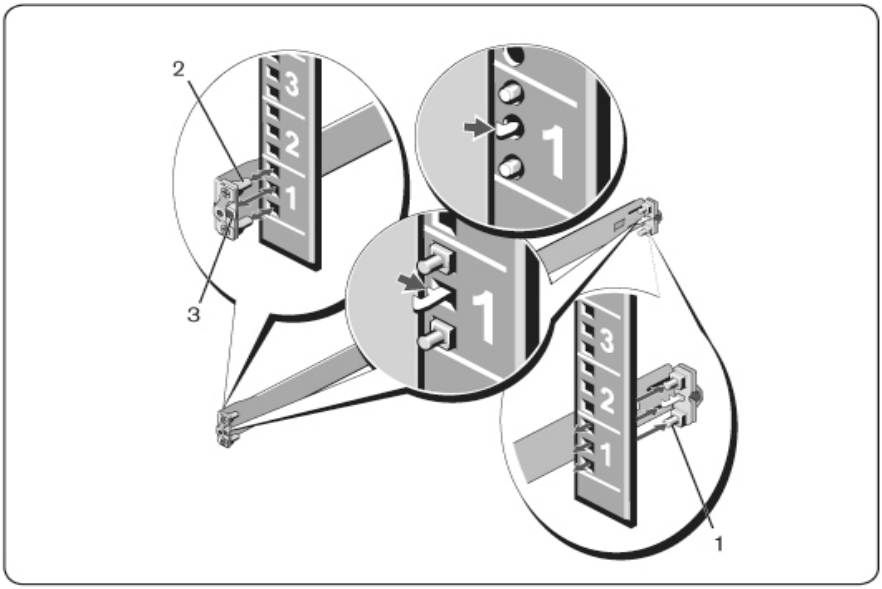
Installation des Dell ReadyRails™-Systems

Das ReadyRails-System ermöglicht Ihnen die einfache Konfiguration Ihres Racks für die Installation eines RCS. Das ReadyRails-System kann mithilfe der werkzeuglosen 1-HE-Methode oder mithilfe einer von drei möglichen verschraubten 1-HE-Methoden (bündig mit 2 Stützen, mittig mit 2 Stützen oder Gewindebohrungsrack mit 4 Stützen) installiert werden.

Werkzeuglose 1-HE-Konfiguration (Vierkantbohrungs- oder Rundbohrungsracks mit 4 Stützen)

1 Positionieren Sie bei nach außen zeigenden ReadyRails-Flanschohren eine Schiene zwischen den linken und rechten vertikalen Stützen. Richten Sie die Zapfen der hinteren Flanschschiene aus und befestigen Sie diese am Flansch der hinteren vertikalen Stütze. In Abbildung 2.1 zeigen Element 1 und dessen Auszüge, wie die Zapfen sowohl in die Vierkant- als auch in die Rundbohrungsöffnungen eingepasst werden müssen.

Abbildung 2.1. Werkzeuglose 1-HE-Konfiguration



2 Richten Sie die Zapfen des vorderen Flanschs aus und befestigen Sie diese an der Vorderseite der vertikalen Stütze (Element 2).

3 Wiederholen Sie diese Schritte für die zweite Schiene.

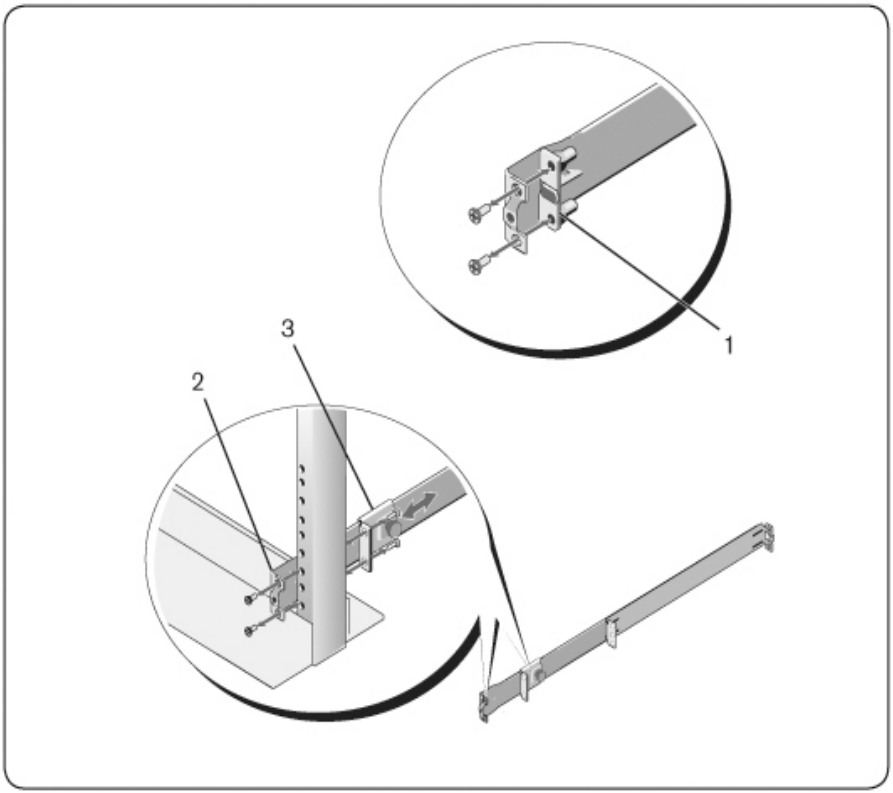
4 Um die Schienen zu entfernen, ziehen Sie am Entriegelungsmechanismus jedes Flanschohrs (Element 3) und lösen Sie die einzelnen Schienen.

Konfiguration 2 Stützen bündig

1 Für diese Konfiguration müssen die Beschläge von der Vorderseite jeder ReadyRails-Baugruppe entfernt werden (Abbildung 2.2, Element 1). Lösen Sie die beiden Schrauben von den vorderen Flanschohren (an der Geräteseite der Schiene) mit einem Torx™-Schraubendreher und entfernen Sie die Beschläge. Bewahren Sie die Beschläge für die eventuelle zukünftige

Verwendung am Rack auf. Die hinteren Flanschbeschläge müssen nicht entfernt werden.

Abbildung 2.2. Konfiguration 2 Stützen bündig



2 Befestigen Sie eine Schiene mithilfe von zwei Schrauben (nicht im Lieferumfang enthalten) am Flansch der vorderen Stütze (Element 2).

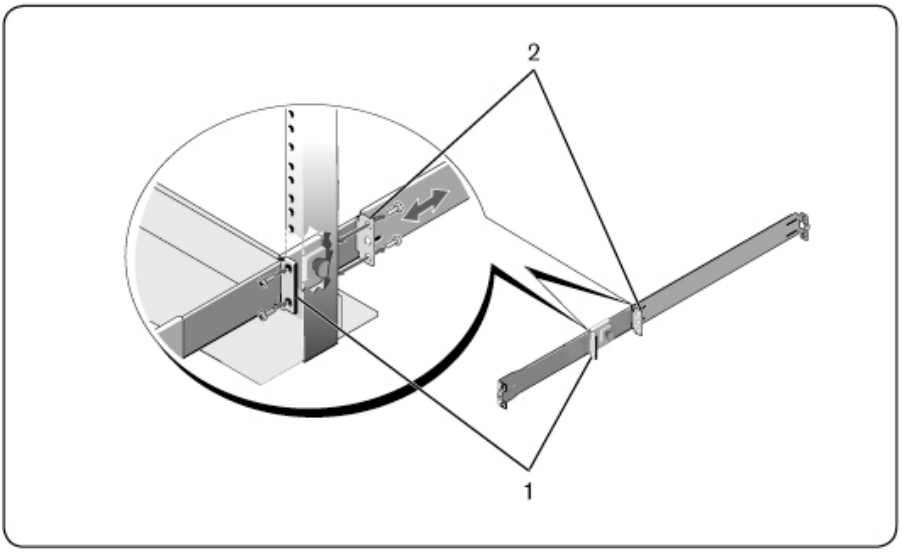
3 Schieben Sie den Haltebügel nach vorn in Richtung der vertikalen Stütze und befestigen Sie diesen mithilfe von zwei Schrauben (nicht im Lieferumfang enthalten) am Stützenflansch (Element 3).

4 Wiederholen Sie diese Schritte für die zweite Schiene.

Konfiguration 2 Stützen mittig

1 Schieben Sie den Haltebügel nach hinten, bis dieser in seiner Position einrastet, und befestigen Sie diesen mithilfe von zwei Schrauben (nicht im Lieferumfang enthalten) am Flansch der vorderen Stütze (Abbildung 2.3, Element 1).

Abbildung 2.3. Konfiguration 2 Stützen mittig



2 Schieben Sie den hinteren Bügel in Richtung der Stütze und befestigen Sie diesen mithilfe von zwei Schrauben (nicht im Lieferumfang enthalten) am Stützenflansch (Element 2).

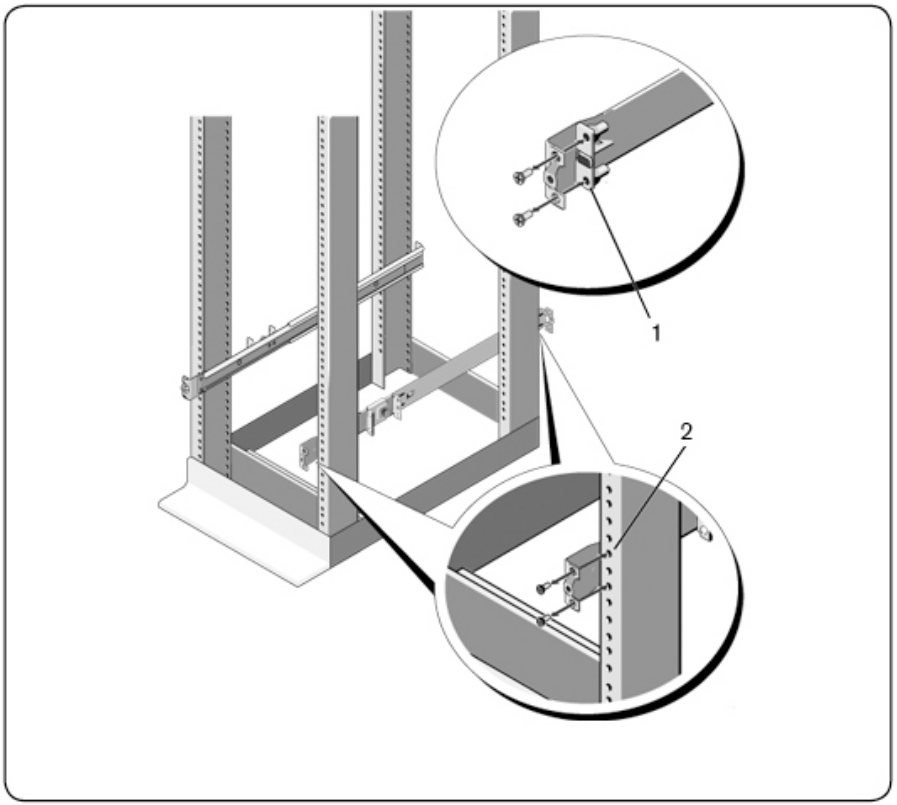
3 Wiederholen Sie diese Schritte für die zweite Schiene.

Konfiguration Gewindebohrungsrack mit 4 Stützen

1 Bei dieser Konfiguration müssen die Beschläge der Flanschohren von allen Seiten der ReadyRails-Baugruppen entfernt werden. Lösen Sie die beiden Schrauben von den beiden Flanschohren mit einem Torx™-Schraubendreher und entfernen Sie die Beschläge(Abbildung 2.4, Element 1).Bewahren Sie die Beschläge für die eventuelle zukünftige Verwendung am Rack auf.

2 Befestigen Sie bei jeder Schiene den vorderen und den hinteren Flansch mithilfe von zwei Schrauben (nicht im Lieferumfang enthalten) an den Stützenflanschs (Element 2).

Abbildung 2.4. Konfiguration Gewindebohrungsrack mit 4 Stützen



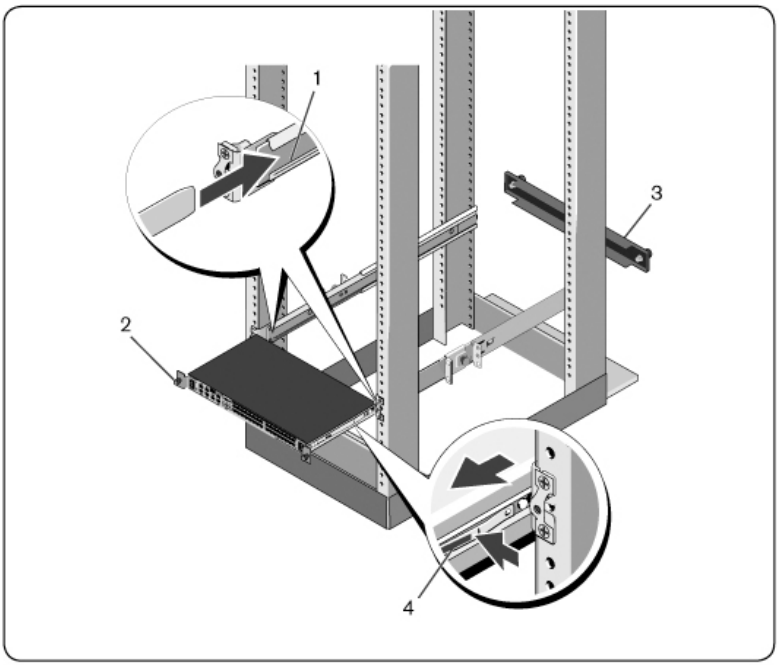
Installation des RCS

Der Switch kann in den Konfigurationen 1-HE-Heck-Rack, 1-HE-Front-Rack, 1-HE mit 2 Stützen (bündig und mittig) und 0 HE montiert werden. Nachfolgend sehen Sie Beispiele für die Konfigurationen 1-HE-Heck-Rack, 1-HE Front-Rack und 0-HE.Für Konfigurationen vom Typ 1 HE mit 2 Stützen (bündig und mittig) können Sie den Switch ebenso in die Schienen schieben wie bei 4-Stützen-Konfigurationen.

Installation des 1-HE-Heck-Racks

1 Setzen Sie die Enden der am Switch angebrachten Schienen in die ReadyRails-Baugruppe ein und drücken Sie den Switch in das Rack (Abbildung 2.5, Element 1).

Abbildung 2.5. Installation des 1-HE-Heck-Racks



2 Ziehen Sie die Rändelschraube jeder Switch-Schiene fest (Element 2).

3 (Optional) Bringen Sie die Verblendung an den Schienen an der Vorderseite des Racks an und ziehen Sie die Rändelschrauben fest (Element 3).

So entfernen Sie den Switch aus dem Rack:

1 Lösen Sie die Rändelschrauben und ziehen Sie die Switch-Baugruppe so weit aus dem Rack, bis die Anschläge erreicht sind. Die angebrachten Anschläge dienen zur Neupositionierung der Schienengriffe; sie sind nicht für die Durchführung von Wartungsmaßnahmen vorgesehen.

2 Lokalisieren Sie die blauen Ösen an den Seiten der Switch-Schienen (Element 4).

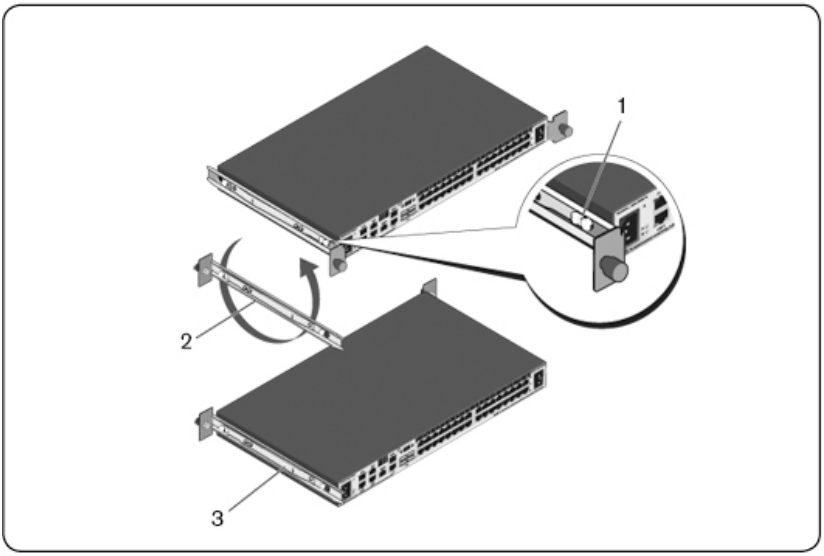
3 Drücken Sie die Ösen nach innen und ziehen Sie die Baugruppe weiter heraus, bis Sie die ReadyRails-Baugruppen vollständig aus den Switch-Schienen entnehmen können.

Installation des 1-HE-Front-Racks

Vor der Installation müssen die am Switch angebrachten Schienen neu konfiguriert werden.

1 Heben Sie an jeder Switch-Schiene die Öse unter dem vorderen Abstandsbolzen an und schieben Sie die Schiene nach vorn, während Sie die Schiene vom Switch abheben (Abbildung 2.6, Element 1).

Abbildung 2.6. Drehen der Switch-Schienen



2 Drehen Sie jede Schiene um 180° (Element 2) und befestigen Sie diese anschließend wieder am Switch (Element 3).

3 Informationen zur Montage und Demontage der Switch-Baugruppe in das bzw. aus dem ReadyRails-System entnehmen Sie der 1-HE-Heck-Rack Anleitung.

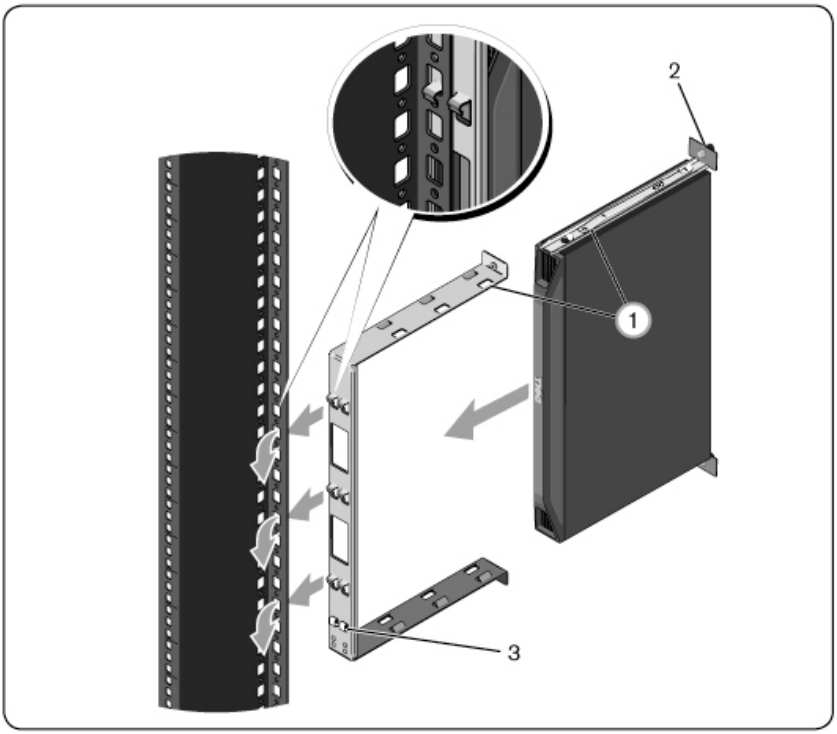
HINWEIS: Für diese Konfiguration ist keine Verblendung erforderlich.

Installation des 0-HE-RCS

1 Richten Sie die 0-HE-Befestigungshalterung aus und befestigen Sie diese an den Switch-Schienen (Abbildung 2.7, Element 1). Ziehen sie die Rändelschrauben fest (Element 2).

2 Führen Sie die Haken der Befestigungshalterung in die Bohrungen im Rack ein und drücken Sie diese nach unten, bis der blaue Knopf herausspringt und die Halterung verankert.

Abbildung 2.7. 0-HE-Installation



Zum Entfernen der Switch-Baugruppe drücken Sie den blauen Knopf (Element 3), um die Halterung zu lösen, und entnehmen Sie anschließend die Baugruppe aus den Stützen.

Anschluss der RCS-Hardware

Das unten abgebildete Diagramm stellt eine mögliche Konfiguration für Ihre RCS-Hardware dar.

Abbildung 2.8. Standard-RCS-Konfiguration

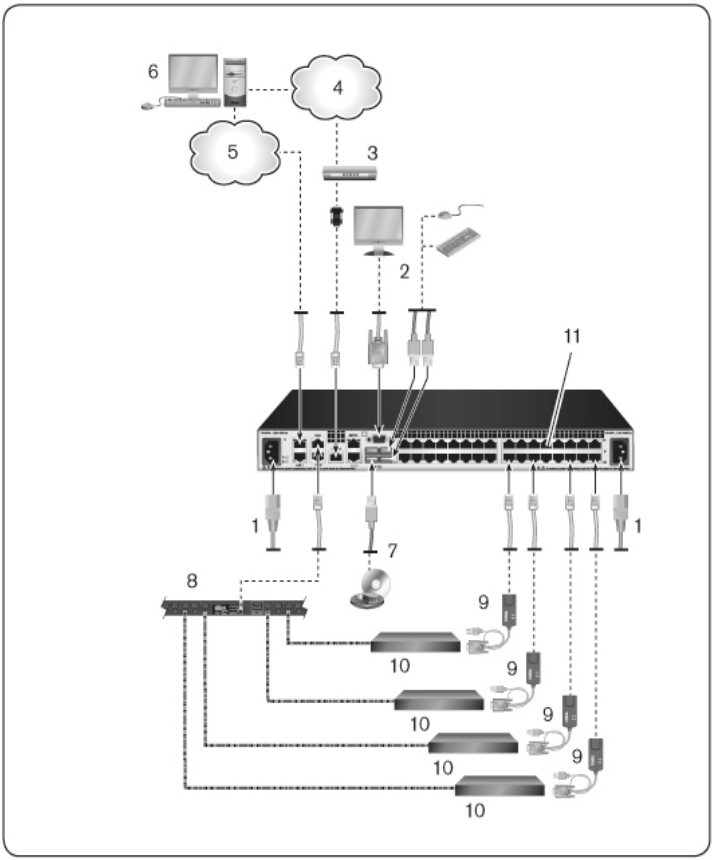


Tabelle 2.1: Beschreibung der Standard-RCS-Konfiguration

Nummer	Beschreibung	Nummer	Beschreibung
1	Brückenkabel	7	Externe Virtual Media
2	Analoger Benutzer	8	Stromüberwachungsgerät
3	Modem	9	SIPs
4	Telefonnetz	10	Zielgeräte
5	Netzwerk	11	RCS (Abbildung: Modell mit 32 Ports)
6	Digitaler Benutzer		

So schließen Sie den Switch an und schalten ihn ein:

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

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.

- Das Netzkabel muss immer ordnungsgemäß geerdet sein. Der Masseanschluss ist ein wichtiges Sicherheitsmerkmal.
- Stecken Sie das Brückenkabel in eine geerdete Schukosteckdose, die jederzeit leicht zugänglich sein muss.
- Das Brückenkabel entweder aus der Steckdose oder aus dem Gerät ziehen, um die Stromversorgung über das Gerät zu unterbrechen.

- Der Wechselstromeingang ist die Haupt-Stromtrennung, um die Stromversorgung des Geräts zu unterbrechen. Bei Geräten mit mehr als einem Wechselstromeingang müssen alle Netzkabel abgezogen werden, um die Stromversorgung vollständig zu unterbrechen.
- Dieses Gerät enthält keine Komponenten, die vom Benutzer gewartet werden müssen. Die Geräteabdeckung darf nicht geöffnet oder entfernt werden.

1 Schließen Sie einen VGA-Monitor und USB-Tastatur- und Mauskabel an die entsprechenden Ports an.

2 Schließen Sie ein Ende eines UTP-Kabels (4-paarig, bis zu 45 m) an einen nummerierten Port an. Schließen Sie das andere Ende an einen RJ-45-Anschluss eines SIP an.

3 Schließen Sie einen SIP an den entsprechenden Port an der Rückseite des Zielgeräts an. Wiederholen Sie die Schritte 2 und 3 für alle Zielgeräte, die angeschlossen werden sollen.

HINWEIS: Beim Anschluss eines Zielgeräts von Sun Microsystems muss ein Multisync-Monitor verwendet werden, der sowohl Sun Rechner mit VGA- als auch Sync-on-Green oder Composite-Sync unterstützt.

4 Verbinden Sie ein UTP-Kabel (nicht im Lieferumfang enthalten) über das Ethernet-Netzwerk mit einem LAN-Port an der Rückseite des RCS. Netzwerk-Benutzer greifen über diesen Port auf den RCS zu. Die Verbindung der redundanten LAN-Ports mit separaten Ethernet-Switches sorgt für zusätzliche Redundanz beim eventuellen Ausfall eines Ethernet-Switches.

5 (Optional) Auf den Switch kann auch über ein ITU V.92-, V.90- oder V.24-kompatibles Modem zugegriffen werden. Schließen Sie ein Ende eines RJ-45-Kabels an den MODEM-Port des Switches an. Schließen Sie das andere Ende am im Lieferumfang enthaltenen RJ-45-auf-DB-9 (Stecker-)Adapter an, der dann mit dem entsprechenden Port an der Modemrückseite verbunden wird.

HINWEIS: Die Leistungsfähigkeit Ihres Switches wird eingeschränkt, wenn eine Modemverbindung anstelle einer LAN-Verbindung verwendet wird.

6 (Optional) Schließen Sie eine unterstützte PDU an den RCS an, indem Sie ein Ende eines CAT 5-Kabels mit dem PDU1-Port des Switches verbinden. Verbinden Sie das andere Ende mit der PDU. Schließen Sie die Netzkabel der Zielgeräte an die PDU an. Schließen Sie die PDU an die Stromversorgung an. Wiederholen Sie diesen Vorgang für den PDU2-Port, um bei Bedarf eine zweite PDU anzuschließen.

7 Schalten Sie alle Zielgeräte ein und legen Sie das/die Brückenkabel bereit, das/die im Lieferumfang des Switches enthalten ist/sind. Stecken Sie das eine Kabelende in den Stromanschluss an der Rückseite des Switches. Stecken Sie das andere Ende in eine geeignete Netzsteckdose. Bei Verwendung eines RCS mit dualer Stromversorgung schließen Sie das zweite Brückenkabel an den zweiten Stromanschluss an der Rückseite des RCS an und stecken Sie das andere Ende in eine andere Steckdose.

HINWEIS: Schließen Sie die Redundanz-Stromversorgungen an voneinander unabhängige Abzweigleitungen an, um zusätzliche Redundanz im Falle einer fehlerhaften Wechselstromquelle sicherzustellen.

8 (Optional) Schließen Sie die Virtual Media-Geräte oder Smart Card-Lesegeräte an einen der USB-Ports am Switch an.

HINWEIS: Bei allen Virtual Media-Sitzungen muss ein USB2- oder USB2+CAC-SIP verwendet werden.

Anschließen eines SIPs

So schließen Sie ein SIP an jeden Server an:

1 Legen Sie die SIPs für Ihren RCS bereit.

2 Falls Sie einen PS/2-SIP-Anschluss nutzen, schließen Sie die farbcodierten Enden des SIP-Kabels an die entsprechenden Tastatur-, Monitor- und Mausports des ersten Servers an, den Sie mit diesem RCS verbinden. Wenn Sie eine USB-Verbindung verwenden, schließen Sie den Stecker des SIP an den USB-Port am ersten Server an, der mit dieser Remote Console Switch-Einheit verbunden werden soll.

3 Schließen Sie ein Ende des CAT 5-Kabels, mit dem Ihr SIP mit dem RCS verbunden wird, an den RJ-45-Stecker an. Siehe Abbildung 2.9.

4 Schließen Sie das andere Ende des CAT 5-Kabels an den gewünschten ARI-Port (Avocent Rack Interface) auf der Rückseite Ihres RCS an.

5 Wiederholen Sie die Schritte 2 - 4 für alle Server, die angeschlossen werden sollen.

HINWEIS: Fahren Sie den RCS vor Wartungsarbeiten herunter. Ziehen Sie das Brückenkabel stets aus der Steckdose.

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

Abbildung 2.9. SIP-Anschluss

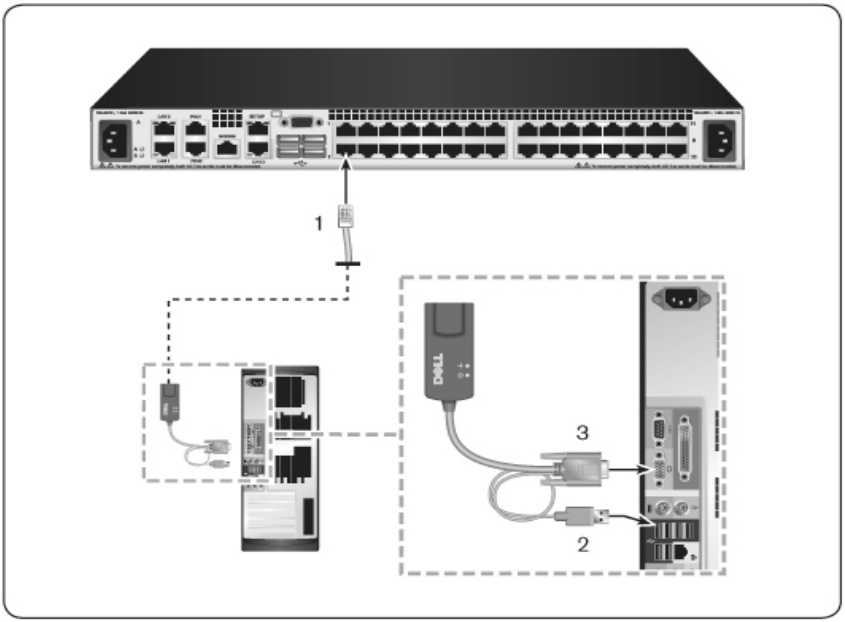


Tabelle 2.2: Beschreibungen für Abbildung 2.9

Nummer	Beschreibung
1	CAT 5
2	USB-Verbindung
3	VGA-Anschluss

So schließen Sie einen SIP mit einem UTP-Stecker an ein serielles Gerät an:

1 Verbinden Sie den RJ-45-Anschluss des SIP mit dem seriellen Gerät.

- oder -

Schließen Sie den SIP an die Buchse eines RJ-45-auf-9-Pin-Adapters an. Schließen Sie den Adapter an den seriellen Port des seriellen Geräts an.

2 Schließen Sie ein Ende eines UTP-Kabels (4-paarig, 150 bis zu 45 m) an einen nummerierten Port auf der Rückseite des Switches an. Schließen Sie das andere Ende an einen RJ-45-Anschluss des Switches an.

3 Schließen Sie das USB-zu-Stromkabel an den Stromstecker am SIP an. Schließen Sie den USB-Anschluss am USB-zu-Stromkabel an einen verfügbaren USB-Port am seriellen Zielgerät an.

Hinzufügen eines gestuften Switches

HINWEIS: Der RCS unterstützt keinen EL80-DT.

HINWEIS: Das modulare Gehäuse M1000e wird in einer gestuften Konfiguration unterstützt. Schließen Sie ein Ende eines CAT 5 Kabels an den Ziel-Port am RCS-Switch an. Verbinden Sie das andere Ende mit dem mit der Analog Console Interface (ACI) kompatiblen RJ45-Port am iKVM-Modul auf der Rückseite des M1000e-Gehäuses. Firmware-Aktualisierungen für die Komponenten des modularen Gehäuses M1000e sind über diese gestufte Konfiguration nicht möglich.

Sie können bis zu zwei Ebenen von Switches stufen und es Benutzern so ermöglichen, Verbindungen mit bis zu 1024 Servern herzustellen. In einem gestuften System wird jeder Zielgeräte-Port am Haupt-Switch an den ACI-Port

jedes gestuften Switches angeschlossen. Jeder gestufte Switch kann dann an ein Gerät mit SIP oder Avocent IQ-Module angeschlossen werden.

So stufen Sie mehrere Switches:

1 Schließen Sie ein Ende eines UTP-Kabels an einen Zielgeräte-Port am Switch an.

2 Schließen Sie das andere Ende des UTP-Kabels an den ACI-Port auf der Rückseite des gestuften Switches an.

3 Schließen Sie die Zielgeräte an den gestuften Switch an.

4 Wiederholen Sie diese Schritte für alle gestuften Switches, die Sie an Ihr System anschließen möchten.

HINWEIS: Die beiden Switches werden automatisch „zusammengelegt". Alle Switches, die an den gestuften Switch angeschlossen sind, werden in der Haupt-Switch-Liste in der lokalen Benutzeroberfläche angezeigt.

HINWEIS: Der Switch unterstützt einen gestuften Switch pro Zielgeräte-Port am Haupt-Switch. Sie können keinen Switch an den gestuften Switch anschließen.

HINWEIS: Beim Kaskadieren mit einem RCS werden analoge Console Switches mit 8 oder 16 Ports nicht als Primäreinheit in einer gestuften Konfiguration unterstützt. Der RCS muss die Primäreinheit bilden.

Abbildung 2.10. Stufen des RCS mithilfe eines UTP-Analog-Switches

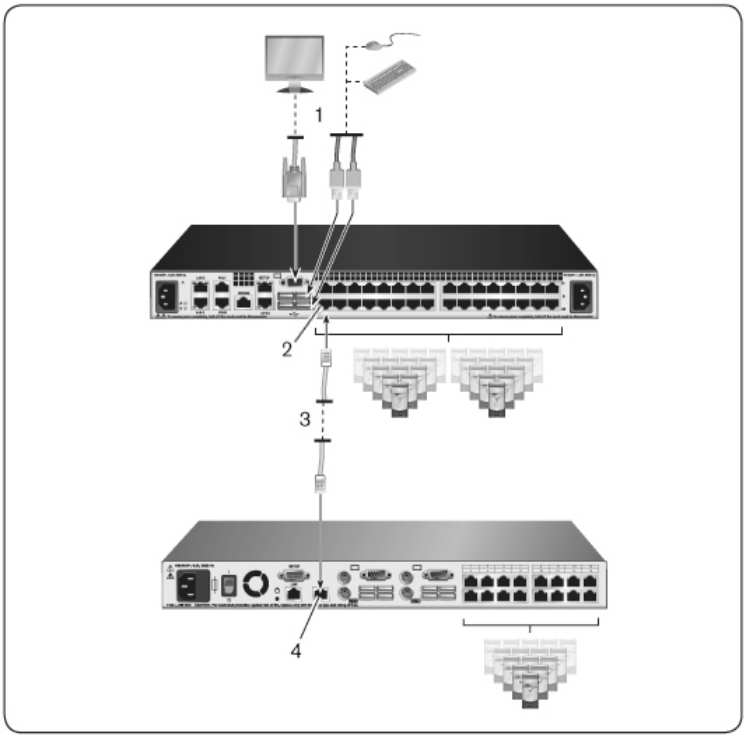


Tabelle 2.3: Beschreibungen für Abbildung 2.10

Nummer	Beschreibung
1	Lokaler Benutzer
2	ARI-Anschluss
3	UTP-Verbindung
4	ACI-Anschluss

Kaskadieren mit Legacy-Switches

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

1 Installieren Sie den Switch im Rack. Legen Sie ein UTP-Kabel bereit, um den RCS mit dem Legacy-Switch zu verbinden.

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

3 Schließen Sie das andere Ende des UTP-Kabels an ein PS/2-SIP an.

4 Schließen Sie den SIP entsprechend der Herstellerempfehlungen an Ihren Legacy-Switch an.

5 Wiederholen Sie die Schritte 1 - 4 für alle Legacy-Switches, die mit dem Switch verbunden werden sollen.

HINWEIS: Der RCS unterstützt nur einen Switch pro ARI-Port. Unter diesem ersten Switch kann kein weiterer Switch kaskadiert werden.

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

Abbildung 2.11. Kaskadieren von Legacy-Switches

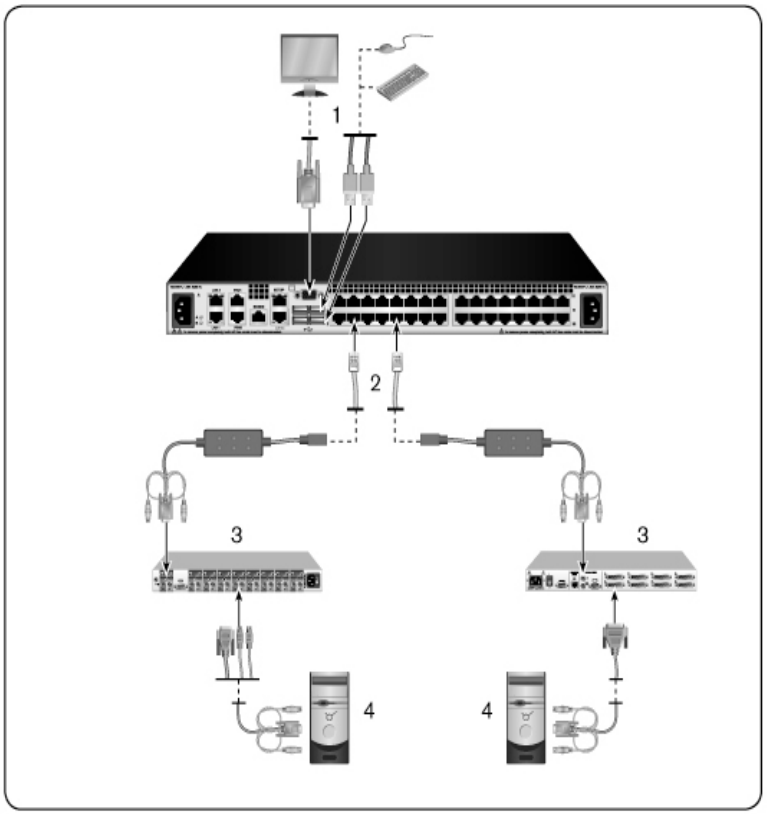


Tabelle 2.4: Beschreibungen für Abbildung 2.11

Nummer	Beschreibung
1	Lokaler Benutzer
2	ARI-Anschluss

Nummer	Beschreibung
3	PS2-Anschluss
4	Zielgeräte-Anschluss

Hinzufügen eines PEM (optional)

Mithilfe eines PEM (Port Expansion Module) kann jeder ARI-Port so erweitert werden, dass bis zu acht Geräte (anstatt lediglich einem Gerät) angeschlossen werden können. Nähere Informationen hierzu entnehmen Sie der Abbildung und der Tabelle mit den Erläuterungen zur Abbildung.

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: Die Verwendung von VM- oder CAC-SIPs hinter einem PEM wird nicht unterstützt.

HINWEIS: True Serial SIP funktioniert hinter einem PEM nicht.

So fügen Sie ein PEM hinzu (optional):

1 Bauen Sie das PEM im Rack ein. Unter Verwendung von bis zu neun UTP-Kabeln verbinden Sie den RCS über ein Kabel mit dem PEM. Mithilfe der anderen acht Kabel verbinden Sie das PEM mit dem an jedes Gerät angeschlossenen SIP.

2 Schließen Sie ein Ende des UTP-Kabels, mit dem das PEM mit dem RCS verbunden wird, an den RJ-45-Stecker an, der etwas versetzt von den anderen Steckern am PEM liegt. Schließen Sie das andere Ende des UTP-Kabels an den gewünschten ARI-Port auf der Rückseite des RCS an.

3 Schließen Sie die UTP-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 Ende des UTP-Kabels an den ersten SIP an.

5 Wiederholen Sie die Schritte 3 - 4 für alle Geräte, die verbunden werden sollen.

Abbildung 2.12. RCS-Konfiguration mit einem PEM

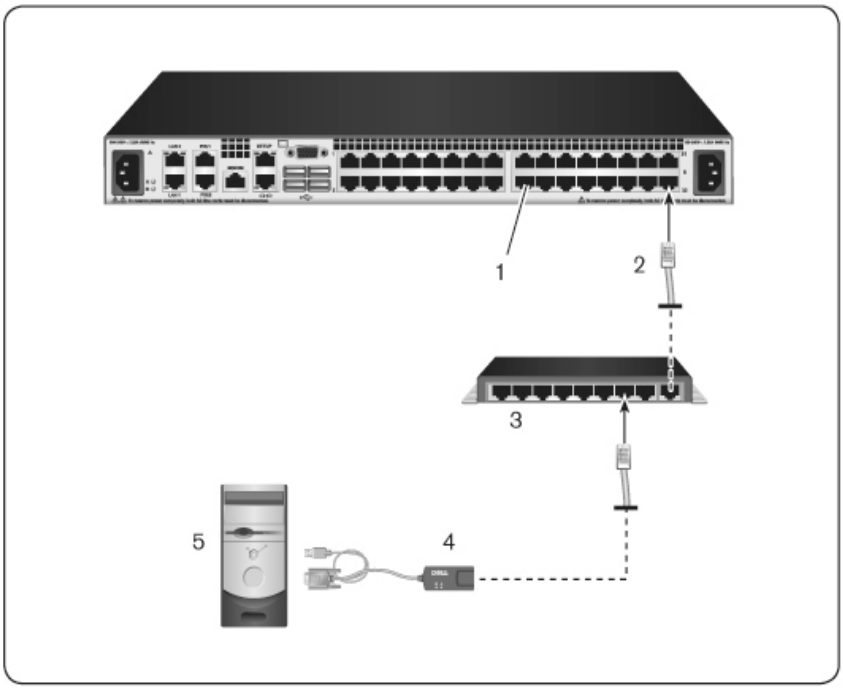


Tabelle 2.5: Beschreibungen für Abbildung 2.12

Nummer	Beschreibung
1	ARI-Port
2	UTP

Nummer	Beschreibung
3	PEM
4	SIP oder Avocent IQ-Modul
5	Server

Konfiguration des Remote Console Switches

Nachdem alle physischen Verbindungen hergestellt sind, müssen Sie den Switch für die Verwendung im Switch-System konfigurieren. Dies kann auf zweierlei Arten durchgeführt werden:

Anweisungen zur Konfiguration des Switches mithilfe der Avocent-Managementsoftware entnehmen Sie dem entsprechenden Installations-/Benutzerhandbuch von Avocent.

So konfigurieren Sie den Switch über die lokale Benutzeroberfläche:

Detaillierte Anweisungen zur Verwendung der lokalen Benutzeroberfläche für die erstmalige Netzwerkeinrichtung finden Sie unter „Netzwerkeinstellungen“ auf Seite 58.

Einrichten des integrierten Webservers

Sie können über einen integrierten Webserver auf den Switch zugreifen, der den Großteil der normalen Aufgaben des Switches verwaltet. Bevor Sie über den Webserver auf den Switch zugreifen, müssen Sie zuerst über den SETUP-Port auf der Rückseite des Switches oder über die lokale Benutzeroberfläche eine IP-Adresse festlegen. Detaillierte Anweisungen zur Verwendung der Switch-Benutzeroberfläche finden Sie in Kapitel 3.

Verbinden mit der OBWI durch eine Firewall

Für Switch-Installationen, die über die OBWI auf den Switch zugreifen, müssen die folgenden Ports in der Firewall geöffnet werden, wenn Zugriff von außen

gewünscht ist.

Tabelle 2.6: OBWI-Ports mit einer Firewall

Portnummer	Funktion
TCP 22	Wird verwendet für SSH zu seriellen Sitzungen mit einem SIP.
TCP 23	Wird für Telnet (wenn aktiviert) verwendet.
TCP 80	Wird für den anfänglichen Download des Video Viewers verwendet. Der RCS-Administrator kann diesen Wert ändern.
TCP 443	Wird von der Webbrowseroberfläche zur Verwaltung des Switches und zum Starten von KVM-Sitzungen verwendet. Der RCS-Administrator kann diesen Wert ändern.
TCP 2068	Übertragung von KVM-Sitzungsdaten (Maus + Tastatur) oder Videoübertragung an Switches.
TCP/UDP 3211	Erkennung.
TCP 389	(Optional) Verwendet von LDAP-Verzeichnisdiensten; standardmäßiger Zugriffs-Port
TCP 636	(Optional) Verwendet von LDAP-Verzeichnisdiensten; Secure-/SSL-Port
TCP 3268	(Optional) Verwendet von Microsoft Active Directory-Diensten; standardmäßiger Zugriffs-Port
TCP 3269	(Optional) Verwendet von Microsoft Active Directory-Diensten; Secure-/SSL-Zugriffs-Port

Die nachfolgende Abbildung und Tabelle zeigen eine typische Konfiguration, bei der sich der Computer des Benutzers außerhalb und der Switch innerhalb der Firewall befindet.

Abbildung 2.13. Typische RCS-Firewall-Konfiguration

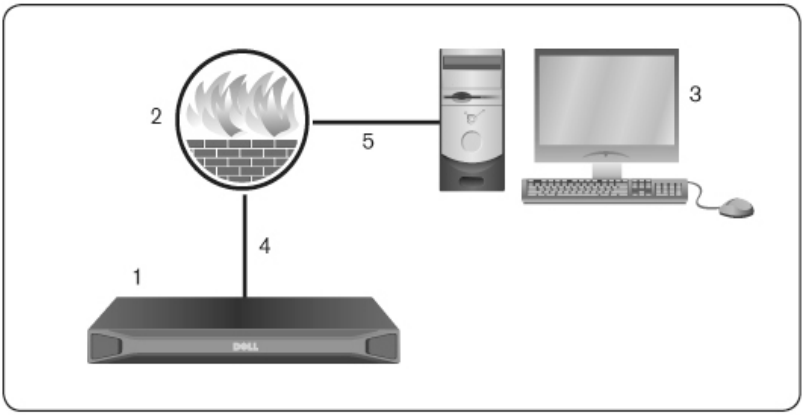


Tabelle 2.7: Beschreibungen für Abbildung 2.13

Nummer	Beschreibung
1	RCS
2	Firewall
3	Computer des Benutzers
4	Firewall leitet HTTP-Anfragen und KVM-Daten an den Switch
5	Benutzer sucht nach der externen IP-Adresse der Firewall

So konfigurieren Sie die Firewall:

Um von außerhalb einer Firewall auf den Switch zuzugreifen, konfigurieren Sie Ihre Firewall so, dass die Ports 22, 23 (wenn Telnet aktiviert ist), 80, 443, 2068 und 3211 von der externen Oberfläche zum KVM-Switch über die interne Oberfläche der Firewall weitergeleitet werden. Weitere Informationen zur Portweiterleitung finden Sie in der Bedienungsanleitung Ihrer Firewall.

HINWEIS: Die Ports 80 und 443 können durch einen Administrator neu konfiguriert werden.

Informationen zum Aufrufen der OBWI finden Sie unter „Integrierte Weboberfläche (OBWI)“ auf Seite 47.

Überprüfen der Verbindungen

Ethernet-Verbindungs-LEDs auf der Geräterückseite

Der RCS verfügt auf der Geräterückseite über zwei LEDs, die den Verbindungsstatus der Ethernet-LAN1-Verbindung anzeigen und zwei LEDs, die den Verbindungsstatus der Ethernet-LAN2-Verbindung anzeigen.

- Die grünen LEDs leuchten, wenn eine gültige Netzwerkverbindung hergestellt ist, und blinken, um Aktivität am Port anzuzeigen.
- Die zweifarbigen LEDs leuchten entweder grün oder gelb.
  - Bei einer Übertragungsgeschwindigkeit von 1000 M/Bit leuchten sie grün.
  - Bei einer Übertragungsgeschwindigkeit von 100 M/Bit leuchten sie gelb.
  - Liegt die Übertragungsgeschwindigkeit bei 10 M/Bit leuchten sie nicht.

Netzstromstatus-LEDs auf der Geräterückseite

An der Geräterückseite des RCS befindet sich jeweils eine LED pro Netzanschluss. Es gibt zwei Netzstrom-LEDs bei Modellen mit dualer Stromversorgung (16 Ports und 32 Ports) und nur eine LED beim 8-Port-Modell. Die LEDs leuchten grün auf, wenn der Switch eingeschaltet und normal in Betrieb ist.

- Die LED leuchtet nicht, wenn die Stromversorgung nicht eingeschaltet ist oder ein Fehler vorliegt.
- Die LED leuchtet, wenn die Einheit betriebsbereit ist.
- Die LED blinkt, wenn der Switch hochgefahren oder eine Aktualisierung durchgeführt wird.

- Die LED blinkt „SOS“, wenn ein Fehlerzustand vorliegt, wie z. B. ein Ausfall der Stromversorgung, eine zu hohe Umgebungstemperatur oder ein Gebläsefehler. Die LED blinkt kontinuierlich „SOS“, so lange der Fehler vorliegt.

Der Switch verhindert eine serielle Unterbrechung der angeschlossenen Geräte, sollte die Stromversorgung des Moduls unterbrochen werden. Der Benutzer kann jedoch eine serielle Unterbrechung durch Drücken der Taste **Serial Break** im Serial Session Viewer erzeugen.

Anpassen der Mauseinstellungen ein Zielgeräte

Bevor ein an den Switch angeschlossener Computer zur Remote-Benutzersteuerung verwendet werden kann, müssen Sie die Mausgeschwindigkeit des Zielgeräts einstellen und die Mausbeschleunigung ausschalten. Verwenden Sie für Computer unter Microsoft® Windows® (Windows NT®, 2000, XP, Server 2003) den standardmäßigen PS/2-Maustreiber.

Damit die lokalen Mausbewegungen und die Anzeige des Remote-Cursors synchron bleiben, muss die Mausbeschleunigung für alle Benutzerkonten, die auf eine Remote-System über einen KVM-Switch zugreifen, auf „Keine“ eingestellt sein. Die Mausbeschleunigung muss auch auf jedem Remote-System auf „Keine“ eingestellt sein. Stellen Sie sicher, dass keine speziellen Cursor verwendet werden und Anzeigeoptionen, wie Mausspur, Cursorpositionsanimationen mit der *Strg*-Taste, Mausschatten und Ausblenden des Cursors deaktiviert sind.

HINWEIS: Wenn Sie die Mausbeschleunigung nicht über ein Windows-Betriebssystem deaktivieren können oder wenn Sie nicht die Einstellungen all Ihrer Zielgeräte einstellen möchten, können Sie den Befehl *Extras – Einzelcursormodus* im Video Viewer-Fenster verwenden. Mit diesem Befehl wird das Video Viewer-Fenster in den „Nicht sichtbaren“-Mausmodus versetzt, mit dem man manuell zwischen der Anzeige des Mauszeigers auf dem Zielsystem und auf dem Client-Computer umschalten kann.

3

Lokale und Remote-Konfiguration

Der RCS ist mit zwei „Point-and-Click“-Oberflächen ausgestattet: einer lokalen Benutzeroberfläche und einer Remote-OBWI. Mit den Konfigurationsoptionen, die Ihnen diese Benutzeroberflächen bieten, können Sie den Switch auf Ihre Anwendung zuschneiden, angeschlossene Geräte steuern und alle grundlegenden KVM- oder seriellen Switch-Anforderungen verwalten.

HINWEIS: Die lokale Benutzeroberfläche und die Remote-OBWI sind fast identisch. Wenn nicht ausdrücklich angegeben, beziehen sich alle Informationen in diesem Kapitel auf beide Benutzeroberflächen.

Aus beiden Benutzeroberflächen heraus können Sie zwei verschiedene Sitzungsarten starten:

- Mit dem Video Viewer-Fenster können Sie in Echtzeit die Tastatur-, Bildschirm- und Mausfunktionen eines einzelnen Zielgeräts übernehmen, das an den Switch angeschlossen ist. Es können auch vordefinierte globale Makros verwendet werden, um Aktionen innerhalb des Video Viewer-Fenster auszuführen. Informationen zur Verwendung des Video Viewers finden Sie in Kapitel 4.
- Mit dem seriellen Viewer-Fenster können Sie einzelne serielle Zielgeräte entweder mit Befehlen oder mit Skripten verwalten.

Lokale Benutzeroberfläche

Auf der Rückseite des Switches befindet sich ein lokaler Port. Über diesen Port können Sie eine Tastatur, einen Bildschirm und eine Maus direkt an den Switch anschließen und die lokale Benutzeroberfläche verwenden.

Sie können nach Belieben einen der nachfolgenden Tastenanschläge konfigurieren, sodass über diesen die lokalen Benutzeroberfläche geöffnet oder zwischen der lokalen Benutzeroberfläche und einer aktiven Sitzung gewechselt werden kann. <Drucken>, <Strg + Strg>, <Umschalt + Umschalt> und <Alt + Alt>. Standardmäßig werden <Drucken> und <Strg-Strg> verwendet.

So starten Sie die lokale Benutzeroberfläche:

1 Schließen Sie die Kabel von Bildschirm, Tastatur und Maus an den Switch an. Weitere Informationen finden Sie unter „Anschluss der RCS-Hardware“ auf Seite 28.

2 Verwenden Sie eine der aktivierten Tastenfolgen, um die lokale Benutzeroberfläche zu starten.

3 Sofern die Authentifizierung der lokalen Benutzeroberfläche aktiviert wurde, geben Sie Ihren Benutzernamen und Kennwort ein.

HINWEIS: Wenn der Switch einem Avocent-Managementsoftware-Server zugeordnet wurde, wird auf diesen Server zugegriffen, um den Benutzer zu authentifizieren. Wenn der Switch keinem Avocent-Managementsoftware-Server zugeordnet wurde oder nicht auf den Avocent-Managementsoftware-Server zugegriffen werden kann, dann wird die lokale Benutzerdatenbank des Switches verwendet, um den Benutzer zu authentifizieren. Der Standard-Benutzername ist Admin und es ist kein Kennwort erforderlich. Bei Benutzernamen in der lokalen Datenbank wird nach Groß- und Kleinschreibung unterschieden.

Verbundene Zielgeräte in der Benutzeroberfläche des lokalen Ports können über zwei Fenster angezeigt und verwaltet werden, die über die Navigationsleiste auf der linken Seite ausgewählt werden können. Für weniger als 20 Ziele empfehlen wir zur Navigation das Fenster „Zielliste - Einfach“. Für mehr als 20 verbundene Zielgeräte bietet das Fenster „Zielliste - Vollständig“ zusätzliche Navigationswerkzeuge. Im Fenster „Zielliste - Vollständig“ können Sie durch Eingabe der Seitennummer, mithilfe der Navigationstasten oder durch die Verwendung von Filtern navigieren. Beide Fenster können als Standardfenster zur Auswahl von Zielgeräten verwendet werden.

Filter

Sie können die Liste der Zielgeräte filtern, indem Sie eine Zeichenfolge angeben, die zur Suche nach passenden Einträgen verwendet wird. Eine Filterung kann eine kürzere und präzisere Liste liefern. Wenn eine Filterung durchgeführt wird, wird die Spalte „Name“ nach der angegebenen Zeichenfolge durchsucht. Bei den Suchfunktionen wird die Groß- und Kleinschreibung nicht beachtet. Bei der Filterung können Sie vor oder nach der Zeichenfolge ein Sternchen als Platzhalter verwenden. Wenn Sie beispielsweise **E-Mail-Server*** eingeben und auf *Filtern* klicken, werden Listeneinträge angezeigt, die mit der Zeichenfolge „E-Mail-Server“ beginnen (z. B. E-Mail-Server oder E-Mail-Server-Sicherung).

Integrierte Weboberfläche (OBWI)

Die OBWI des Switches ist eine remote, webbrowserbasierte Benutzeroberfläche. Weitere Informationen zur Einrichtung Ihres Systems finden Sie unter „Anschluss der RCS-Hardware“ auf Seite 28. In der nachfolgend aufgeführten Tabelle sind die Betriebssysteme und Browser aufgeführt, die von der OBWI unterstützt werden. Vergewissern Sie sich, dass Sie über die neueste Version des Webbrowsers verfügen.

Tabelle 3.1: Von der OBWI unterstützte Betriebssysteme

Betriebssystem	Browser	
	Microsoft® Internet Explorer ab Version 6.0 SP1	Firefox ab Version 2.0
Microsoft Windows 2000 Workstation oder Server mit Service Pack 2	Ja	Ja
Microsoft Windows Server® 2003 Standard, Enterprise oder Web Edition	Ja	Ja

Betriebssystem	Browser	
	Microsoft® Internet Explorer ab Version 6.0 SP1	Firefox ab Version 2.0
Microsoft Windows Server® 2008 Standard, Enterprise oder Web Edition	Ja	Ja
Windows XP Professional mit Service Pack 3	Ja	Ja
Windows Vista® Business mit Service Pack 1	Ja	Ja
Red Hat Enterprise Linux® 4 und 5 Standard, Enterprise oder Web Edition (Smart Card wird u. U. nicht vom Betriebssystem unterstützt)	Nein	Ja
Sun Solaris® 9 und (Smart10 Card wird u. U. nicht vom Betriebssystem unterstützt)	Nein	Ja
Novell SUSE Linux Enterprise 10 und 11 (Smart Card wird u. U. nicht vom Betriebssystem unterstützt)	Nein	Ja
Ubuntu 8 Workstation (Smart Card wird vom Betriebssystem unter Umständen nicht unterstützt)	Nein	Ja

So melden Sie sich an der Switch-OBWI an:

1 Starten Sie einen Webbrowser.

2 Geben Sie im Adressfeld des Browsers die IP-Adresse oder den Host-Namen ein, die/der dem Switch, auf den Sie zugreifen möchten, zugewiesen ist. Verwenden Sie https://xxx.xx.xx.xx oder https://hostname als Format.

HINWEIS: Wenn Sie den IPv6-Modus verwenden, müssen Sie die IP-Adresse in eckige Klammern einschließen. Verwenden Sie hierbei das Format //[<IP-Adresse-].

3 Wenn der Browser die Verbindung mit dem Switch hergestellt hat, geben Sie Ihren Benutzernamen und Ihr Kennwort ein und klicken Sie dann auf *Anmelden*. Die integrierte Weboberfläche des Switches wird angezeigt.

HINWEIS: Der Standard-Benutzername ist Admin und es ist kein Kennwort erforderlich.

Wiederholen Sie den obigen Vorgang, um sich von außerhalb einer Firewall an der Switch-OBWI anzumelden, und geben Sie dabei die externe IP-Adresse der Firewall ein.

HINWEIS: Der RCS versucht zu erkennen, ob Java bereits auf Ihrem PC 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_11 oder höher 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.

Verwenden der Benutzeroberflächen

Nach der Authentifizierung wird die Benutzeroberfläche angezeigt. Sie können Ihren Switch anzeigen, darauf zugreifen und ihn verwalten, sowie Systemeinstellungen festlegen und Profileinstellungen ändern. Die nachfolgende Abbildung zeigt die Fensterbereiche der Benutzeroberfläche. Beschreibungen der Bildschirme entnehmen Sie der nachfolgenden Tabelle.

Abbildung 3.1. Fenster der Benutzeroberfläche

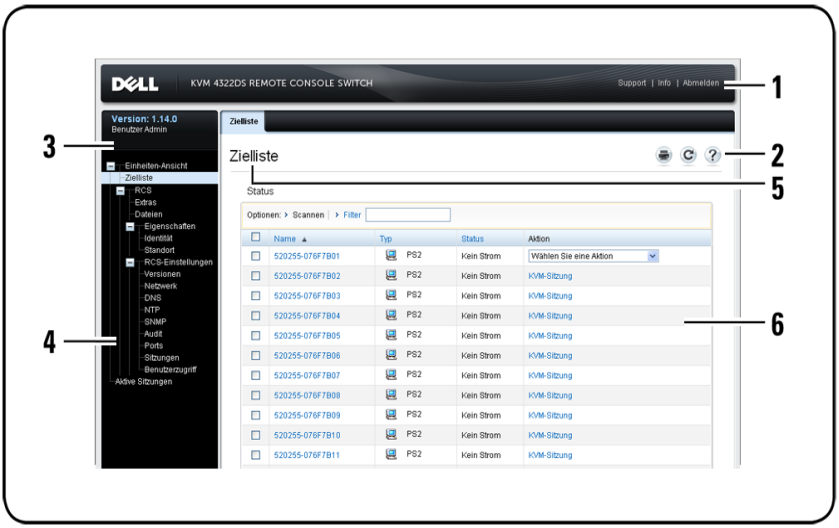


Tabelle 3.2: Beschreibungen der Benutzeroberfläche

Nummer	Beschreibung
1	Obere Optionsleiste: Über die obere Optionsleiste können Sie sich mit dem technischen Kundendienst in Verbindung setzen, die allgemeinen Informationen der Software einsehen oder sich aus einer OBWI-Sitzung abmelden.
2	Zweite Optionsleiste: Über diese Optionsleiste können Sie eine Website ausdrucken, die aktuelle Website aktualisieren oder auf das Hilfe-Tool zugreifen.

Nummer	Beschreibung
3	Versions-Info-Block: Auf der linken Seite der oberen Optionsleiste werden die Firmware-Version des Produkts und der Benutzername des aktuell angemeldeten Benutzers angezeigt.
4	Seitliche Navigationsleiste: Über die seitliche Navigationsleiste können Sie auswählen, welche Informationen angezeigt werden sollen. Verwenden Sie die seitliche Navigationsleiste zum Anzeigen von Fenstern, in denen Einstellungen geändert oder Aktionen ausgeführt werden.
5	Navigationsleisten: Über die ausgewählte Navigationsleiste werden die Systeminformationen im Inhaltsbereich angezeigt. Einige Leisten enthalten Unterregister, die angeklickt werden können, um Einzelheiten innerhalb einer Kategorie anzuzeigen und zu überarbeiten.
6	Inhaltsbereich: Verwenden Sie den Inhaltsbereich, um das OBWI-System des Switches anzuzeigen oder Änderungen vorzunehmen.

Starten einer Sitzung

HINWEIS: Java 1.6.0_11 oder höher wird benötigt, um eine Sitzung zu starten.

So starten Sie eine Sitzung:

1 Klicken Sie in der seitlichen Navigationsleiste auf Zielgeräte. Es wird eine Liste der verfügbaren Geräte angezeigt.

2 Die entsprechende Aktion (KVM-Sitzung oder serielle Sitzung) wird in der Aktionsspalte angezeigt und variiert je nach Zielgerät, welches zum Start der Sitzung ausgewählt wurde. Stehen für das jeweilige Zielgerät mehrere Aktionen zur Verfügung, klicken Sie auf den Dropdown-Pfeil und wählen Sie die gewünschte Aktion aus der angezeigten Liste aus.

Wenn das Zielgerät momentan verwendet wird, haben Sie ggf. die Möglichkeit, eine Verbindung zu diesem Gerät zu erzwingen, sofern Ihre Unterbrechnungsebene gleich oder höher als die des aktuellen Benutzers ist.

Der RCS erlaubt zudem über ein externes Telnet oder eine SSH-Anwendung wie PuTTY serielle Sitzungen mit seriellen SIPs. Telnet- und SSH-Sitzungen werden ausschließlich zur Verbindung serieller SIPs genutzt und können nicht verwendet werden, um auf RCS- oder KVM-Zielgeräte zuzugreifen bzw. diese zu verwalten.

So starten Sie eine serielle Sitzung über eine Telnet- oder SSH-Anwendung:

1 Geben Sie die Host-IP-Adresse des RCS ein, mit dem der serielle SIP verbunden ist.

2 Geben Sie <RCS-Benutzername>:<Serial-SIP-Name> ein, z. B. jsmith:router.

3 Geben sie das Kennwort des RCS-Benutzers ein.

HINWEIS: Die Telnet-Funktion ist standardmäßig deaktiviert. Um den Telnet-Support zu aktivieren, lesen Sie „Konfiguration von seriellen Sitzungen“ auf Seite 82.

So schalten Sie über die lokalen Benutzeroberfläche auf die aktive Sitzung um (nur lokale Benutzer):

1 Klicken Sie in der seitlichen Navigationsleiste auf **Lokale Sitzung**.

2 Aktivieren Sie das Kontrollkästchen **Aktive Sitzung fortsetzen**. Das Video Viewer-Fenster wird angezeigt.

Scanmodus

Im Scan-Modus scannt der Switch mehrere Zielgeräte. Die Scan-Reihenfolge wird von der Position des Zielgeräts in der Liste bestimmt. Sie können außerdem die Zeitspanne definieren, die verstreicht, bis das nächstfolgende Zielgerät gescannt wird.

HINWEIS: Die Schaltfläche „Scannen“ ist deaktiviert, wenn eine Verbindung zu einem Modem besteht.

So fügen Sie Zielgeräte zur Scan-Liste hinzu:

1 Klicken Sie in der seitlichen Navigationsleiste auf **Einheiten-Ansicht – Zielliste**, um den Bildschirm „Zielgeräte“ aufzurufen.

2 Aktivieren Sie die Kontrollkästchen neben den Zielgeräten, die gescannt werden sollen.

3 Klicken Sie auf **Scannen**.

So konfigurieren Sie die Scandauer:

1 Klicken Sie in der seitlichen Navigationsleiste auf **Ports – Benutzeroberfläche des lokalen Ports**, um den Einstellungsbildschirm für die Benutzeroberfläche des lokalen Ports aufzurufen.

2 Geben Sie unter der Scan-Modus-Überschrift in das Scandauer-Feld die Dauer in Sekunden (von 3 - 255) ein.

3 Klicken Sie auf **Speichern**.

Anzeigen von Systeminformationen

Auf der Benutzeroberfläche können Sie sich verschiedene Switch- und Zielgeräteinformationen auf den folgenden Bildschirmen anzeigen lassen.

Tabelle 3.3: Systeminformationen

Kategorie	Wählen Sie Folgendes aus:	Um dies anzuzeigen:
RCS	*Einheiten-Anzeige – RCS – Extras*	RCS-Name und -Typ und RCS-Extras (Wartung, Diagnose, Zertifikate und Trap-MIB)
	Einheiten-Anzeige – RCS – Dateien	RCS-Konfiguration, Benutzerdatenbank und Zielgerät
	Einheiten-Anzeige – RCS – Eigenschaften – Identität	Artikelnummer, Seriennummer und EID

Kategorie	Wählen Sie Folgendes aus:	Um dies anzuzeigen:
	Einheiten-Anzeige – RCS – Eigenschaften – Standort	Aufstellungsort, Abteilung und Standort
	Einheiten-Anzeige – RCS-Einstellungen – Versionen	Aktuelle Anwendungs- und Bootversionen
Zielgerät	*Einheiten-Anzeige – Zielliste*	Liste der angeschlossenen Geräte sowie Name, Typ, Status und Aktion des jeweiligen Geräts Klicken Sie auf das Zielgerät, um die folgenden zusätzlichen Informationen anzuzeigen: Name, Typ, EID, verfügbare Sitzungsoption und Verbindungspfad

RCS-Extras

Der Einheiten-Name und -Typ wird auf dem Bildschirm „Extras – Wartung – Überblick“ angezeigt. Zusätzlich können grundlegende Einheiten-Aufgaben ausgeführt werden.

Neustarten des RCS

So starten Sie den RCS neu:

1 Klicken Sie in der seitlichen Navigationsleiste auf **Einheiten-Ansicht – RCS – Extras – Wartung – Überblick**, um den Bildschirm „Einheiten-Wartung“ aufzurufen.

2 Klicken Sie auf *Neustart*.

3 Ein Dialogfeld weist Sie darauf hin, dass alle aktiven Sitzungen getrennt werden. Klicken Sie auf *OK*.

HINWEIS: Wenn Sie die lokale Benutzeroberfläche verwenden, werden während des Neustarts auf dem Bildschirm keine Informationen angezeigt. Wenn Sie die Remote-OBWI verwenden, wird eine Nachricht angezeigt, dass die Benutzeroberfläche wartet, bis der Neustart der abgeschlossen ist.

RCS-Firmware aktualisieren

Sie können den RCS mit der aktuellsten Firmware aktualisieren.

Nachdem der Flash-Speicher mit der Aktualisierung neu programmiert wurde, führt der Switch einen Warmstart durch, bei dem alle SIP-Sitzungen getrennt werden. Ein Zielgerät, bei dem die SIP-Firmware aktualisiert wird, wird möglicherweise nicht oder als nicht verbunden angezeigt. Das Zielgerät wird wie gewohnt angezeigt, sobald die Flash-Aktualisierung beendet ist.

Achtung: Wenn ein SIP während der Aktualisierung der Firmware oder während eines Neustarts des Zielgeräts getrennt wird, funktioniert das SIP nicht mehr und muss zur Reparatur ans Werk eingeschickt werden.

So aktualisieren Sie die Firmware des Switches:

1 Klicken Sie in der seitlichen Navigationsleiste auf *Einheiten-Ansicht – RCS – Extras – Wartung – Aktualisieren*, um den Bildschirm „RCS-Firmwareaktualisierung“ aufzurufen.

2 Klicken Sie auf *Aktualisieren*, um den Bildschirm „Einheiten-Firmware aktualisieren“ aufzurufen.

3 Wählen Sie eine der folgenden Methoden, um die Firmware-Datei zu laden: *Filesystem*, *TFTP*, *FTP* oder *HTTP*.

HINWEIS: Die Option „Dateisystem“ ist nur über die Remote-OBWI verfügbar.

4 Wenn die Option „Dateisystem“ ausgewählt wurde, wählen Sie *Durchsuchen*, um den Speicherort der Firmware-Aktualisierungsdatei festzulegen.

- oder -

Sofern TFTP ausgewählt wurde, geben Sie die Server-IP-Adresse und die Firmware-Datei ein, die Sie laden möchten.

- oder -

Sofern FTP oder HTTP ausgewählt wurde, geben Sie die Server-IP-Adresse und die Firmware-Datei ein, die Sie laden möchten, sowie den Benutzernamen und das Benutzerkennwort.

5 Klicken Sie auf *Aktualisieren*.

Speichern und Wiederherstellen von RCS-Konfigurationen und RCS-Benutzerdatenbanken

Sie können die Switch-Konfiguration in einer Datei speichern. Die Konfigurationsdatei enthält Informationen über die verwaltete Einheit. Sie können außerdem die lokale Benutzerdatenbank auf dem Switch speichern. Nach dem Speichern der Dateien können Sie eine zuvor gespeicherte Konfigurationsdatei oder lokale Benutzerdatenbank-Datei auf den Switch hochladen.

So speichern Sie eine Konfiguration oder eine Benutzerdatenbank einer verwalteten Einheit:

1 Klicken Sie in der seitlichen Navigationsleiste auf das Register *Einheiten-Ansicht - RCS - Dateien*.

2 Klicken Sie entweder auf das Register *RCS-Konfiguration* oder auf das Register *Benutzerdatenbank* und dann auf das Register *Speichern*.

3 Wählen Sie das Verfahren zum Speichern der Datei: **Dateisystem**, **TFTP**, **FTP** oder **HTTP PUT**.

4 Sofern TFTP ausgewählt wurde, geben Sie die Server-IP-Adresse und den Namen der Firmware-Datei ein, die Sie laden möchten.

- oder -

Sofern FTP oder HTTP ausgewählt wurde, geben Sie die Server-IP-Adresse, den Benutzernamen, das Benutzerkennwort und den Namen der Firmware-Datei ein, die Sie laden möchten.

5 Geben Sie ein Verschlüsselungskennwort ein, wenn sie die Daten vor dem Herunterladen verschlüsseln wollen.

6 Klicken Sie auf *Herunterladen*. Das Dialogfeld „Speichern unter“ wird geöffnet.

7 Navigieren Sie zum gewünschten Speicherort und geben Sie einen Dateinamen ein. Klicken Sie auf **Speichern**.

So stellen Sie eine Konfiguration oder eine Benutzerdatenbank einer verwalteten Einheit wieder her:

1 Klicken Sie in der seitlichen Navigationsleiste auf das Register *Einheiten-Ansicht - RCS - Dateien*.

2 Klicken Sie entweder auf das Register *RCS-Konfiguration* oder auf das Register *Benutzerdatenbank* und dann auf das Register *Wiederherstellen*.

3 Wählen Sie das Verfahren zum Speichern der Datei: **Dateisystem**, **TFTP**, **FTP** oder **HTTP**.

4 Wenn die Option „Dateisystem“ ausgewählt wurde, wählen Sie *Durchsuchen*, um den Speicherort der Firmware-Aktualisierungsdatei festzulegen.

- oder -

Sofern TFTP ausgewählt wurde, geben Sie die Server-IP-Adresse und den Namen der Firmware-Datei ein, die Sie laden möchten.

- oder -

Sofern FTP oder HTTP ausgewählt wurde, geben Sie die Server-IP-Adresse, den Benutzernamen, das Benutzerkennwort und den Namen der Firmware-Datei ein, die Sie laden möchten.

5 Klicken Sie auf **Durchsuchen**. Navigieren Sie zum gewünschten Speicherort und wählen Sie einen Dateinamen aus. Klicken Sie auf **Hochladen**.

6 Geben Sie das Entschlüsselungskennwort ein, wenn die Originaldatei verschlüsselt wurde.

7 Nachdem der Bestätigungsbildschirm angezeigt wurde, starten Sie die Managed Appliance neu, um die wiederhergestellte Konfiguration zu aktivieren. Siehe „Neustarten des RCS“ auf Seite 54.

So beheben Sie einen Fehler bei der Flash-Aktualisierung:

Startet der RCS nach einem Flash-Vorgang nicht in der neuen Firmware-Version, können Sie über die folgenden Schritte wieder die frühere Firmware-Version aufrufen.

1 Schließen Sie ein serielles Kabel an den SETUP-Port an der Rückseite des RCS an.

2 Starten Sie ein Terminalprogramm auf dem mit dem Setup-Port verbundenen PC. Die Einstellungen des seriellen Ports sollten lauten: 9600 baud, 8 data bits, 1 stop bit, no parity und no flow control.

3 Schalten Sie den RCS ein.

4 Drücken Sie eine beliebige Taste, sobald im Terminalprogramm die Aufforderung „Hit any key to stop autoboot“ angezeigt wird. Ein Menü wird angezeigt.

5 Geben Sie <1> (Boot Alternate) ein und betätigen Sie die <Eingabetaste>. Der RCS wird automatisch in der früheren Firmware-Version neu gestartet.

6 Nach dem Neustart des RCS können Sie versuchen, die Flash-Aktualisierung zu wiederholen.

Netzwerkeinstellungen

HINWEIS: Nur Switch-Administratoren könne Änderungen im Dialogfeld für die Netzwerkeinstellungen vornehmen. Andere Benutzer können sich diese Einstellungen lediglich anzeigen lassen.

Klicken Sie in der seitlichen Navigationsleiste auf **Netzwerk**, um die Register „Allgemein“, „IPv4“ und „IPv6“ anzuzeigen.

So konfigurieren Sie die allgemeinen Netzwerkeinstellungen:

1 Klicken Sie auf das Register *Netzwerk* und dann auf das Register **Allgemein**, um den Bildschirm für die allgemeinen Netzwerkeinstellungen des RCS anzuzeigen.

2 Wählen Sie eine der folgenden Optionen aus dem Dropdownmenü für die LAN-Geschwindigkeit: *Automatische Erkennung*, *10 MBit/s Halbduplex*, *10 MBit/s Vollduplex*, *100 MBit/s Halbduplex*, *100 MBit/s Vollduplex* oder *1 GBit/s Vollduplex*.

HINWEIS: Sie müssen einen Neustart ausführen, wenn der Ethernet-Modus geändert wurde.

3 Wählen Sie entweder *Aktiviert* oder *Deaktiviert* im Dropdownmenü „ICMP-Ping-Antwort“.

4 Prüfen oder ändern Sie die HTTP- bzw. HTTPS-Ports. Die Einstellungen werden standardmäßig auf HTTP 80 und HTTPS 443 gesetzt.

5 Klicken Sie auf *Speichern*.

So konfigurieren Sie IPv4-Netzwerkeinstellungen:

1 Klicken Sie auf das Register **IPv4**, um den Bildschirm „IPv4-Einstellungen“ anzuzeigen.

2 Klicken Sie, um das Kontrollkästchen **IPv4 aktivieren** zu aktivieren oder zu deaktivieren.

3 Geben Sie die gewünschten Informationen in die Adress-, Subnetz- und Gateway-Felder ein. IPv4-Adressen werden durch Punkte getrennt eingegeben, z. B. xxx.xxx.xxx.xxx.xxx.

4 Wählen Sie entweder *Aktiviert* oder *Deaktiviert* im Dropdown-Menü „DHCP“ aus.

HINWEIS: Wenn Sie DHCP aktivieren, werden alle Informationen, die Sie in die Adress-, Subnetz- und Gateway-Felder eingeben, nicht beachtet.

5 Klicken Sie auf *Speichern*.

So konfigurieren Sie IPv6-Netzwerkeinstellungen:

1 Klicken Sie auf das Register **IPv6**, um den Bildschirm „IPv6-Einstellungen“ anzuzeigen.

2 Klicken Sie, um das Kontrollkästchen **IPv6 aktivieren** zu aktivieren oder zu deaktivieren.

3 Geben Sie die gewünschten Informationen in die Adress-, Subnetz- und Präfix-Länge-Felder ein. IPv6-Adressen werden eingegeben im Format FD00:172:12:0:0:0:0:33 oder abgekürzt FD00:172:12::33 Hex-Notation.

4 Wählen Sie entweder *Aktiviert* oder *Deaktiviert* im Dropdown-Menü „DHCP“ aus.

HINWEIS: Wenn Sie DHCPv6 aktivieren, werden alle Informationen, die Sie in die Adress-, Gateway- und Präfix-Länge-Felder eingeben, nicht beachtet.

5 Klicken Sie auf *Speichern*.

DNS-Einstellungen

Sie können den DNS-Server entweder manuell zuweisen oder die über DHCP oder DHCPv6 erhaltenen Adressen verwenden.

So konfigurieren Sie DNS-Einstellungen manuell:

1 Klicken Sie in der seitlichen Navigationsleiste auf *DNS*, um den Bildschirm „RCS DNS-Einstellungen“ anzuzeigen.

2 Wählen Sie *Manuell*, *DHCP* (bei aktiviertem IPv4) oder *DHCPv6* (bei aktiviertem IPv6) aus.

3 Geben Sie bei der Auswahl von *Manuell* die DNS-Servernummern in die Felder für primär, sekundär und tertiär ein.

4 Klicken Sie auf *Speichern*.

NTP-Einstellungen

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 über das NTP abgefragt wird. Lesen Sie dazu „Konfigurieren der NTP-Einstellungen (Network Time Protocol)“ in Kapitel 5.

SNMP-Einstellungen

SNMP ist ein Protokoll, das verwendet wird, um Verwaltungsinformationen zwischen Netzwerk-Verwaltungsanwendungen und dem Switch zu übertragen. SNMP-Manager können mit dem Switch über Zugriff auf MIB-II kommunizieren. Wenn Sie den Bildschirm „SNMP“ aufrufen, ruft die integrierte Weboberfläche die SNMP-Parameter von der Einheit ab.

Im Bildschirm „SNMP“ können Sie die Systeminformationen und Community-Zeichenketten eingeben. Außerdem können Sie festlegen, welche Konsolen den Switch verwalten und SNMP-Traps vom Switch empfangen können. Wenn Sie **SNMP aktivieren** auswählen, antwortet die Einheit auf SNMP-Anforderungen über UDP-Port 161.

So konfigurieren Sie allgemeine SNMP-Einstellungen:

1 Klicken Sie auf **SNMP**, um den Bildschirm „SNMP“ zu öffnen.

2 Aktivieren Sie das Kontrollkästchen **SNMP aktivieren**, damit der Switch auf SNMP-Anfragen über UDP-Port 161 antworten darf.

3 Geben Sie den vollständigen System-Domainnamen in das Namensfeld ein, sowie eine Node-Kontaktperson im Kontaktfeld.

4 Geben Sie die Lese-, Schreib- und Trap-Community-Namen ein. Damit werden die Community-Zeichenketten festgelegt, die für SNMP-Aktionen verwendet werden müssen. Die Zeichenketten für Lesen und Schreiben gelten nur für SNMP über den UPD-Port 161 und fungieren als Kennwörter, die den Zugriff auf den Switch schützen. Die Eingaben können eine

maximale Länge von 64 Zeichen haben. Diese Felder dürfen nicht leer bleiben.

5 Geben Sie die Adressen von bis zu vier Management-Workstations in die Felder „Zugelassene Manager“ ein, die diesen Switch verwalten sollen. Sie können diese Felder auch leer lassen, sodass der RCS von allen Konsolen verwaltet werden kann.

6 Klicken Sie auf **Speichern**.

Audit-Ereigniseinstellungen

Ein Ereignis ist eine Benachrichtigung, die vom Switch zu einer Managementkonsole gesendet wird, und die angibt, dass ein Ereignis aufgetreten ist, das ggf. Ihre Aufmerksamkeit erfordert.

So aktivieren Sie einzelne Ereignisse:

1 Klicken Sie auf **Audit**, um den Bildschirm „Ereignisse“ zu öffnen.

2 Bestimmen Sie durch Aktivieren der entsprechenden Kontrollkästchen in der Liste die Ereignisse, die Benachrichtigungen auslösen sollen.

- oder -

Aktivieren oder deaktivieren Sie das Kontrollkästchen neben „Ereignisname“, um die gesamte Liste auszuwählen bzw. die gesamte Auswahl aufzuheben.

3 Klicken Sie auf **Speichern**.

Einstellen von Ereignis-Zielen

Sie können Audit-Ereignisse so konfigurieren, dass sie an SNMP-Trap-Ziele und Syslog-Server gesendet werden. Die Ereignisse, die auf dem Ereignis-Bildschirm aktiviert sind, werden an alle auf dem Bildschirm „Ereignis-Ziele“ aufgeführten Server gesendet.

1 Klicken Sie auf **Audit** und auf das Register **Ziele**, um den Bildschirm „Ereignis-Ziele“ zu öffnen.

2 Geben Sie die Adressen von bis zu vier Management-Workstations ein, an die dieser Switch Ereignisse in den SNMP-Trap-Adress-Feldern sowie an bis zu vier Syslog-Server sendet.

3 Klicken Sie auf **Speichern**.

Ports –SIPs konfigurieren

Vom Switch aus können Sie eine Liste der angeschlossenen SIPs sowie die folgenden Informationen über jeden SIP anzeigen: EID (elektronische Kennung), Port, Status, Anwendung, Schnittstellentyp und USB-Geschwindigkeit. Klicken Sie auf ein SIP, um die folgenden zusätzlichen Informationen anzuzeigen: Switch-Typ, Boot-Version, Anwendungsversion, Hardware-Version, FPGA-Version, verfügbare Version und Aktualisierungsstatus.

Zusätzlich können Sie die folgende Aufgaben ausführen: Offline-SIPs löschen, SIP-Firmware aktualisieren, USB-Geschwindigkeit einstellen oder Kabel außer Betrieb nehmen.

So löschen Sie Offline-SIPs:

1 Klicken Sie in der seitlichen Navigationsleiste auf *Ports – SIPs*, um den SIP-Bildschirm zu öffnen.

2 Klicken Sie auf *Offline löschen*.

SIPs aktualisieren

Über die „Flash-Upgrade“-Funktion für den SIP können RCS-Administratoren den SIP mit der neuesten Firmware aktualisieren. Diese Aktualisierung kann über die Switch-Benutzeroberfläche oder die Avocent-Managementsoftware durchgeführt werden.

Nachdem der Flash-Speicher mit der Aktualisierung neu programmiert wurde, führt der Switch einen Warmstart durch, bei dem alle SIP-Sitzungen getrennt werden. Ein Zielgerät, bei dem die SIP-Firmware aktualisiert wird, wird

möglicherweise nicht oder als nicht verbunden angezeigt. Das Zielgerät wird wie gewohnt angezeigt, sobald die Flash-Aktualisierung beendet ist.

Falls der RCS auf automatische Aktualisierung für SIP-Adapter eingestellt ist, werden die SIPs bei der Aktualisierung des Switches automatisch aktualisiert. Informationen zum Aktualisieren der Switch-Firmware finden Sie unter „RCS-Extras“ auf Seite 54 oder in der Online-Hilfe der Avocent-Managementsoftware. Wenn während des normalen Aktualisierungsvorgangs Probleme auftreten, können Sie SIPs bei Bedarf auch manuell aktualisieren.

HINWEIS: Firmware-Aktualisierungsdateien sind auf http://www.dell.com zu finden.

So ändern Sie die Funktion zur automatischen Aktualisierung für SIP-Adapter:

1 Klicken Sie in der seitlichen Navigationsleiste auf *Ports – SIPs*, um den SIP-Bildschirm zu öffnen.

2 Aktivieren Sie die Kontrollkästchen neben den SIPs, die Sie aktualisieren möchten, und klicken Sie auf *Automatische Aktualisierung aktivieren*.

Achtung: Wenn ein SIP während der Aktualisierung der Firmware oder während eines Neustarts des Zielgeräts getrennt wird, funktioniert das SIP nicht mehr und muss zur Reparatur ans Werk eingeschickt werden.

So aktualisieren Sie die SIP-Firmware:

1 Klicken Sie in der seitlichen Navigationsleiste auf *Ports – SIPs*, um den SIP-Bildschirm zu öffnen.

2 Aktivieren Sie die Kontrollkästchen neben den SIPs, die Sie ändern möchten.

3 Wählen Sie *Wählen Sie eine Aktion* und klicken Sie auf *Aktualisieren*.

4 Sind die Einstellungen korrekt, klicken Sie auf *Aktualisieren*.

So stellen Sie die USB-Geschwindigkeit ein:

HINWEIS: Dieser Abschnitt gilt nur für das USB2-SIP.

1 Klicken Sie in der seitlichen Navigationsleiste auf *Ports – SIPs*, um den SIP-Bildschirm zu öffnen.

2 Aktivieren Sie die Kontrollkästchen neben den SIPs, die Sie ändern möchten.

3 Wählen Sie *Wählen Sie eine Aktion* und klicken Sie entweder auf *USB 1.1 - Geschwindigkeit festlegen* oder auf *USB 2.0 -Geschwindigkeit festlegen*.

Stromverwaltungsgeräte-Einstellungen

HINWEIS: Sie müssen über Administrator-Zugriffsrechte verfügen, um die Stromverwaltungsgeräte-Einstellungen zu ändern.

HINWEIS: Unter www.dellkvm.com finden Sie eine Auflistung der unterstützten PDUs.

Auf dem Bildschirm „RCS-Stromverwaltungsgeräte“ wird eine Liste der angeschlossenen Stromverwaltungsgeräte und die folgenden zu jedem Stromverwaltungsgerät gehörenden Informationen angezeigt: Name, Port, Status, Version, Modell, Tonsignal, Alarm und Temperatur. Sie können auch erst ein Stromverwaltungsgerät und dann **Einstellungen** auswählen, um die folgenden detaillierten Informationen über das Stromverwaltungsgerät anzuzeigen: Name, Beschreibung, Status, Version, Ausgänge, Herstellername, Model und Eingangs-Feeds.

Wenn ein Zielgerät an einen Stromverwaltungsgeräte-Ausgang angeschlossen ist, können Sie das Zielgerät ein-, aus- bzw. aus- und wieder einschalten.

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

1 Klicken Sie in der seitlichen Navigationsleiste auf *Ports – Stromverwaltungsgeräte*, um den Stromverwaltungsgeräte-Bildschirm zu öffnen.

2 Klicken Sie auf den Namen der Einheit, die Sie konfigurieren möchten, und wählen Sie *Ausgangsliste* aus.

3 Aktivieren Sie die Kontrollkästchen links neben den Ausgängen, die Sie konfigurieren möchten.

4 Klicken Sie auf *Ein*, *Aus* oder auf *Aus- und einschalten*.

So löschen Sie Stromverwaltungsgeräte, die offline sind:

1 Klicken Sie in der seitlichen Navigationsleiste auf *Ports – Stromverwaltungsgeräte*, um den Stromverwaltungsgeräte-Bildschirm zu öffnen.

2 Klicken Sie auf *Offline löschen*.

So ändern Sie die Minimum-Ein-Zeit, Aus-Zeit oder den Wachzustand:

1 Klicken Sie in der seitlichen Navigationsleiste auf *Ports – Stromverwaltungsgeräte*, um den Stromverwaltungsgeräte-Bildschirm zu öffnen.

2 Klicken Sie auf den Namen der Einheit, die Sie konfigurieren möchten, und wählen Sie *Ausgänge* aus.

3 Klicken Sie auf den Ausgangsnamen, den Sie ändern möchten.

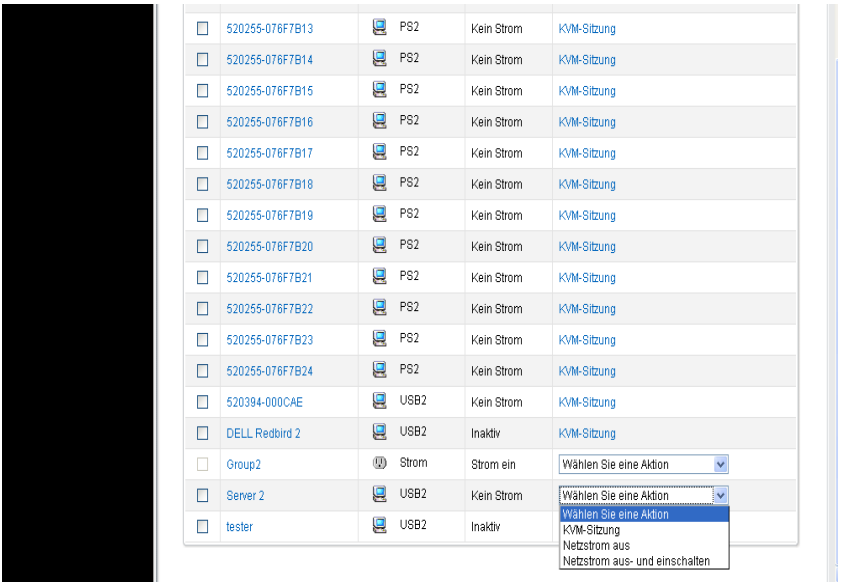
4 Verwenden Sie die Dropdown-Fenster, um die gewünschten Einstellungen vorzunehmen, und klicken Sie auf *Speichern*.

Zugehörige Zielserver und Netzanschlüsse

Auf der Seite „Zielliste“ der OBWI können Stromverwaltungsmaßnahmen für ein Ziel mit verknüpften Ausgängen ausgewählt werden. Durch Auswahl der Register „Ports“–„Stromverwaltungsgeräte“ und Klicken auf einen Gerätenamen werden die Register „Geräteeinstellungen“, „Gerätefirmware-Aktualisierung“ und „Ausgangsliste“ angezeigt. Klicken Sie auf das Register „Ausgangsliste“, um die mit dem Zielgerät verbundenen Ausgänge anzuzeigen.

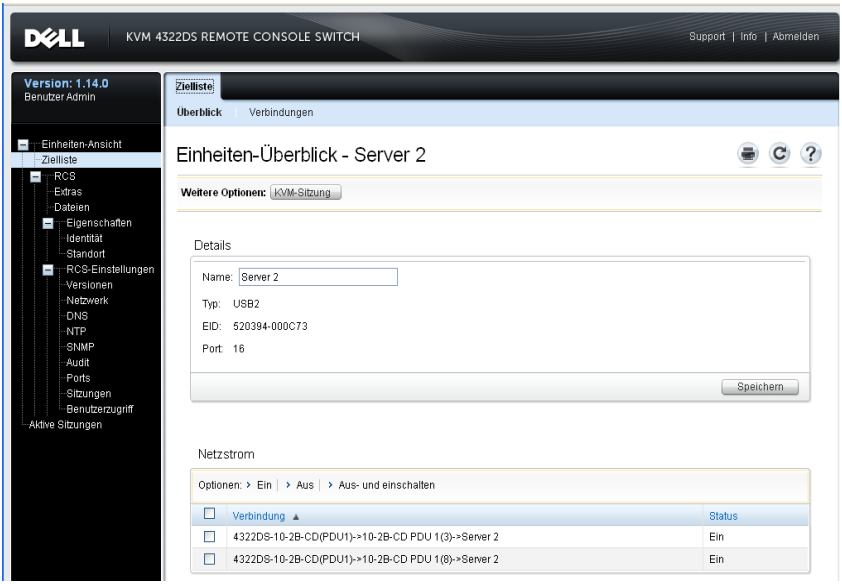
Das mit Server2 in der folgenden Abbildung bezeichnete Zielgerät verfügt über verknüpfte Ausgänge. Durch Klicken auf den Pfeil des Dropdown-Menüs in der Spalte „Aktion“ werden die verfügbaren Aktionen für Netzanschlüsse angezeigt.

Abbildung 3.2. Zielliste



In der folgenden Abbildung werden auf der Zieleinheiten-Überblickseite für Server2 die Netzanschlüsse angezeigt, wobei Ausgang 3 und Ausgang 8 von PDU 1 mit Server2 verknüpft sind.

Abbildung 3.3. Zielübersicht Server2



Zusammenfassen von Stromausgängen zu Gruppen

Die Ausgänge können zur einfacheren Steuerung mit dem Zielserver verbunden oder verknüpft werden. Um Ausgänge (oder Ausgänge an Servern) zu einer Gruppe zusammenzufassen, muss das erste Geräte über die manuelle Namenszuweisung benannt werden. Verknüpfen Sie das zweite und die folgenden Geräte über die Verbindung zum Zielgeräte-Menü und wählen Sie dann den Zielnamen für das erste Gerät aus der Dropdownliste aus.

Stromverwaltungsaktionen, die auf der Seite „Zielliste“ durchgeführt werden, werden auf die jeweiligen Ausgänge angewandt. Stromverwaltungsaktionen für bestimmte Stromausgänge eines Zielgeräts können auf der Einheiten-Überblick-Seite durchgeführt werden. In der folgenden Abbildung besteht das mit Gruppe2 bezeichnete Zielgerät aus den Stromausgängen 5 und 6 der PDU 1.

So gruppieren Sie die Ausgänge 5 und 6:

1 Wählen Sie Ausgang 5, um die Seite *Stromverwaltungsgeräte – Ausgangseinstellungen* anzuzeigen.

2 Klicken Sie auf *Manuell* und geben Sie Gruppe2 ein.

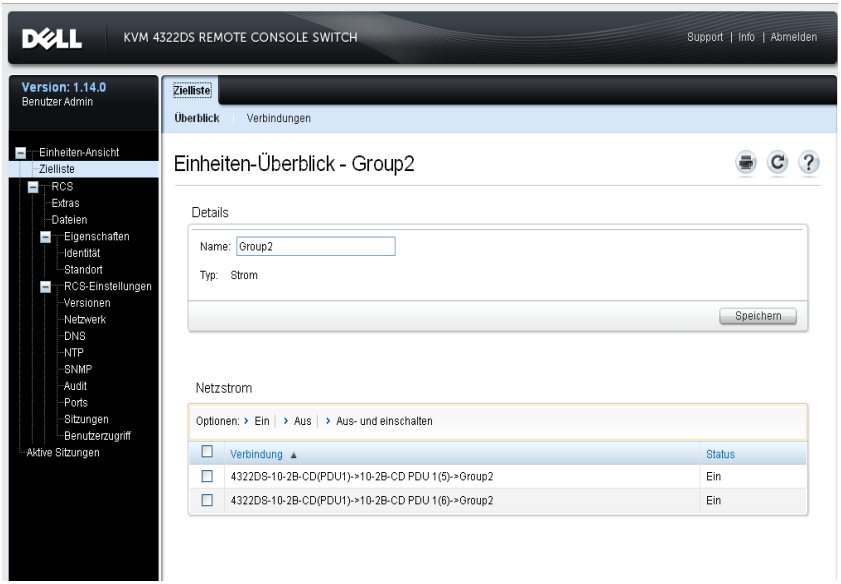
3 Klicken Sie auf *Speichern*.

4 Wählen Sie Ausgang 6, um die Seite *Stromverwaltungsgeräte – Ausgangseinstellungen* anzuzeigen.

5 Wählen Sie *Verbindung zum Zielgerät* und *Gruppe2* aus dem Dropdown-Menü aus.

6 Klicken Sie auf *Speichern*. Wenn die Ausgangsliste wieder angezeigt wird, haben Ausgang 5 und 6 den gleichen Namen.

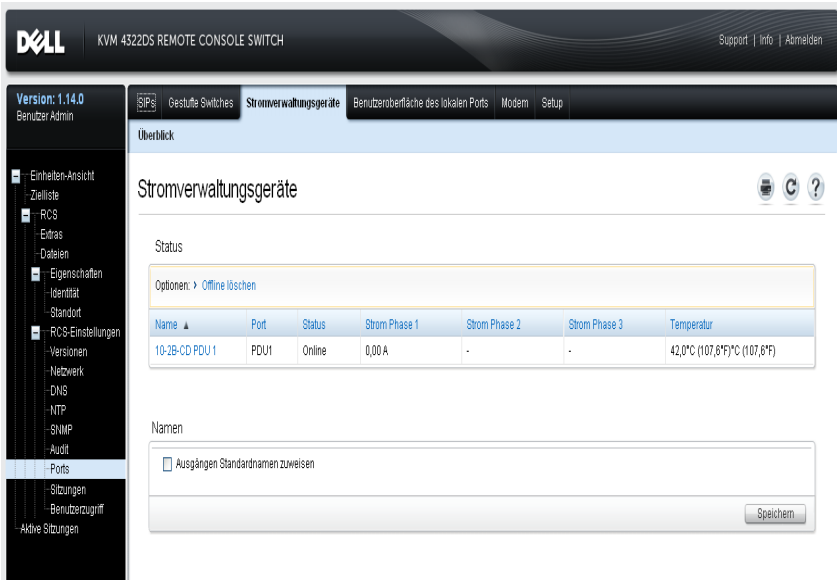
Abbildung 3.4. Zielübersicht für Gruppe2



Standardausgangsnamen

Auf der Seite „Stromverwaltungsgeräte“ kann mit dem Kontrollkästchen „Ausgängen Standardnamen zuweisen“ festgelegt werden, ob den Ausgängen von Stromverwaltungsgeräten Standardnamen zugeteilt werden (siehe folgende Abbildung). Nur Stromausgänge mit Namen werden auf der Zielseite aufgeführt. Standardmäßig zugewiesene Namen von Netzanschlüssen können durch Deaktivieren des Kontrollkästchens „Ausgängen Standardnamen zuweisen“ gelöscht werden. Stromausgängen ohne Namen können durch Aktivieren des Kontrollkästchens „Ausgängen Standardnamen zuweisen“ und Speichern der Einstellung Standardnamen zugewiesen werden.

Abbildung 3.5. Seite „RCS-Stromverwaltungsgeräte“

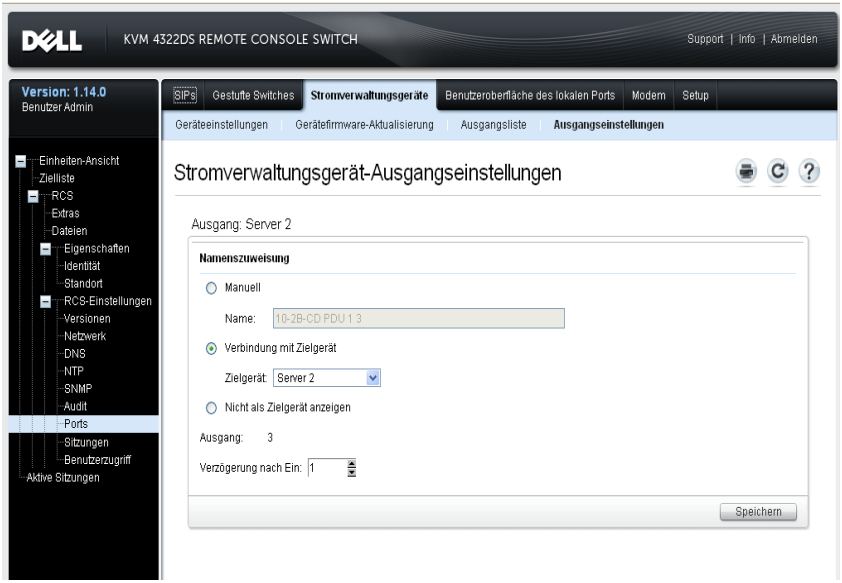


Zuweisen eines Ausgangsnamens

Auf der Seite „Einstellungen für Stromverwaltungsgeräte-Ausgang“ sind drei Optionen verfügbar, um einem Ausgang einen Namen zuzuweisen (siehe

folgende Abbildung). Die Optionen sind „Manuelle Namenszuweisung“, „Verbindung mit Zielgerät“ und „Nicht als Zielgerät anzeigen“

Abbildung 3.6. Seite „Stromverwaltungsgeräte –Ausgangseinstellungen“



- Mit der Option „Manuelle Namenszuweisung“ wird dem Ausgang ein eindeutiger Name zugewiesen. Der Name für alle SIPs und Ausgänge muss eindeutig sein. Wenn ein Name manuell vergeben wird und dieser nicht eindeutig ist, tritt ein Fehler auf und der Name wird nicht gespeichert.
- Mit der Zuweisung von „Verbindung mit Zielgerät“ wird der Ausgang mit einem anderen Zielnamen für die Stromverwaltung des benannten Ziels verknüpft (entweder ein Ausgang oder SIP). Wenn ein Ausgang mit einem SIP-Zielnamen verknüpft wird, versorgt der Ausgang normalerweise den an den SIP-Adapter angeschlossenen Server physisch mit Strom.
- Mit der Option „Nicht als Zielgerät anzeigen“ erhält der Ausgang keinen Namen und wird somit auch nicht auf der Zielgeräteseite angezeigt. Diese

Option kann für unbelegte Ausgänge verwendet werden, um diese von der Seite „Zielliste“ zu entfernen.

Zugriffssteuerungsübernahme

Wenn ein Stromverwaltungsgeräte-Ausgang durch das Verknüpfen mit einem Ziel geändert wird, so übernimmt der Ausgang die bereits konfigurierte Zugriffssteuerung für diesen Zielnamen. Wenn ein SIP-Adapter hinzugefügt wird und der vom SIP-Adapter erhaltene Name mit einem Namen eines bestehenden Ziels übereinstimmt, erbt der neue SIP-Adapter die Zugriffssteuerung von diesem Ziel. Wenn ein Zielgerät unbenannt wird, werden alle SIP-Adapter und Ausgänge dieses Ziels umbenannt, und übernehmen die zuvor konfigurierte Zugriffssteuerung des alten Zielnamens.

Umbenennen eines Zielgeräts

Auf der Überblickseite der Zielliste kann der Name dieses Ziels in einen eindeutigen Zielnamen umbenannt werden. Der Name muss für alle Ziele eindeutig sein, einschließlich SIPs und Stromverwaltungsgeräte-Ausgänge. Wenn ein Ziel umbenannt wird, erhalten alle Ausgänge, die mit diesem Ziel verknüpft sind, den neuen Zielnamen.

Priorisierter Status von Zielgeräten

Auf der Seite „Zielliste“ steuert ein Ziel mit verknüpften Stromverwaltungsgeräte-Ausgängen mehrere Geräte. Der Statuswert, der für ein Ziel angezeigt wird, wird als höchste Priorität aller Statuswerte der Geräte ausgewählt. In der folgenden Tabelle werden die möglichen Statuswerte in Prioritätsfolge (absteigend) und die jeweiligen Zielgerätetypen angezeigt.

Tabelle 3.4: Zielstatuswerte

Statuswert	Zutreffend für:		Status-Beschreibung
	SIP	Stromausgang	
In Verwendung	x	-	Eine Sitzung ist aktiv

Statuswert	Zutreffend für:		Status-Beschreibung
	SIP	Stromausgang	
Pfad blockiert	x	-	Pfad zum Ziel wird von einer anderen Sitzung verwendet
Aktualisierung läuft	x	-	SIP wird aktualisiert
Einschalten	-	x	Mindestens ein Ausgang wird eingeschaltet
Ausschalten	-	x	Mindestens ein Ausgang wird ausgeschaltet
Kein Strom	x	-	SIP wird nicht mit Strom versorgt
Teilweise Stromversorgung	-	x	Ziel hat ein- und ausgeschaltete Ausgänge
Gesperrt aus	-	x	Mindestens ein Ausgang ist gesperrt (ein)
Ausgeschaltet	-	x	Mindestens ein Ausgang ist ausgeschaltet
Gesperrt ein	-	x	Mindestens ein Ausgang ist gesperrt (aus)
Inaktiv	x	-	Keine Sitzung aktiv; SIP wird mit Strom versorgt
Eingeschaltet	-	x	Ausgänge sind eingeschaltet

Wenn ein Zielgerät über mehrere Stromausgänge verfügt, die per Namen verknüpft sind, und diese nicht über einen gemeinsamen Stromzustand verfügen, so kann der RCS den Ausgangsstatus „Gesperrt aus“ als „aus“ und den

Ausgangsstatus „Gesperrt ein“ als „ein“ erkennen. Die folgende Tabelle zeigt die resultierenden Statuswerte aus der Kombination von zwei Ausgangsstatuswerten.

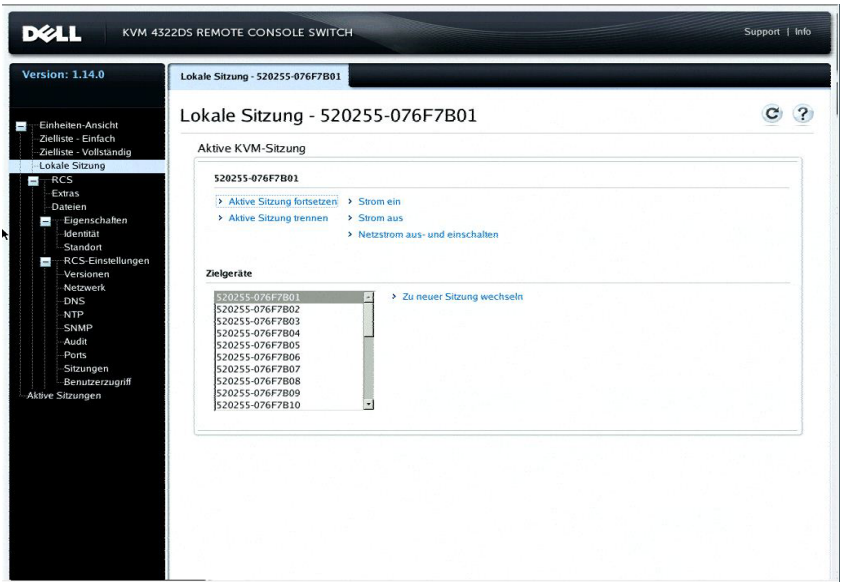
Tabelle 3.5: Mehrfache Ausgangsstatuswerte und angezeigter Status

Status Ausgang 1	Status Ausgang 2	Resultierender Status
Aus	Aus	Aus
Aus	Ein	Teilweise Stromversorgung
Ein	Ein	Eingeschaltet
Gesperrt ein	Ein	Eingeschaltet
Gesperrt ein	Gesperrt ein	Gesperrt ein
Gesperrt ein	Aus	Teilweise Stromversorgung
Gesperrt aus	Ein	Teilweise Stromversorgung
Gesperrt aus	Gesperrt aus	Gesperrt aus
Gesperrt aus	Aus	Ausgeschaltet
Gesperrt ein	Gesperrt aus	Teilweise Stromversorgung

Lokale Sitzungsseite am lokalen Port

Auf der lokalen Sitzungsseite des lokalen Ports werden drei Stromverwaltungsgeräte unter der aktiven Sitzung angezeigt, wenn das Ziel der aktiven Sitzung verknüpfte Stromausgänge besitzt. Die folgende Abbildung zeigt die angezeigten Stromverwaltungsgeräte, die für eine aktive lokale Port-Sitzung für ein Ziel namens „Server2“ angezeigt werden.

Abbildung 3.7. Lokale Sitzungsseite Mit Stromverwaltungsgeräten



Einstellungen für die Benutzeroberfläche des lokalen Ports

So ändern Sie, wie die lokale Benutzeroberfläche aufgerufen wird:

1 Klicken Sie in der seitlichen Navigationsleiste auf *Ports – Benutzeroberfläche des lokalen Ports*, um den Einstellungsbildschirm für die Benutzeroberfläche des lokalen Ports aufzurufen.

2 Aktivieren Sie unter der Überschrift „Benutzeroberfläche des lokalen Ports“ ein Kontrollkästchen neben mindestens einer der aufgeführten Methoden.

3 Klicken Sie auf *Speichern*.

Die Authentifizierung der Benutzeroberfläche des lokalen Ports kann ein- oder ausgeschaltet und eine Benutzer-Zugriffsstufe ausgewählt werden. Wenn die

Authentifizierung der Benutzeroberfläche des lokalen Ports eingeschaltet wird, ist eine Anmeldung erforderlich, bevor die Oberfläche verwendet werden kann.

Des Weiteren kann die Tastatursprache des lokalen Ports und die Scan-Moduszeit eingestellt sowie das Kennwort des lokalen Ports aktiviert bzw. deaktiviert und eine Benutzerunterbrechungsebene ausgewählt werden. Die Benutzerunterbrechungsebene bestimmt, ob Benutzer eine andere serielle oder KVM-Sitzung mit einem Zielgerät trennen können. Es gibt die Benutzerunterbrechungsebenen 1 bis 4, wobei 4 die höchste Ebene darstellt. Beispiel: Ein Benutzer mit einer Benutzerunterbrechungsebene von 4 kann andere Benutzer mit Ebene 4 sowie der Ebenen 1, 2 und 3 unterbrechen.

So ändern Sie die Benutzerauthentifizierung am lokalen Port (nur für Administratoren):

1. Klicken Sie in der seitlichen Navigationsleiste auf **Ports – Benutzeroberfläche des lokalen Ports**, um den Einstellungsbildschirm für die Benutzeroberfläche des lokalen Ports aufzurufen.
2. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Benutzerauthentifizierung am lokalen Port deaktivieren**.
3. Ist das Kontrollkästchen **Benutzerauthentifizierung am lokalen Port deaktivieren** markiert, wählen sie eine der folgenden Optionen aus dem Dropdown-Menü „Benutzer-Zugriffsstufe“: **Benutzer**, **Benutzer-Administrator** oder **RCS-Administrator**.
4. Klicken Sie auf **Speichern**.

Modemeinstellungen

Vom Bildschirm „RCS-Modemeinstellungen“ aus können Sie verschiedene Modemeinstellungen vornehmen sowie die folgenden Modemeinstellungen ansehen: Lokale Adresse, Remote-Adresse, Subnetzmaske und Gateway.

Weitere Informationen zum Anschließen des Switches an ein Modem finden Sie unter „Anschluss der RCS-Hardware“ auf Seite 28.

So konfigurieren Sie die Modemeinstellungen:

1 Klicken Sie in der seitlichen Navigationsleiste auf **Ports – Modem**, um den Bildschirm „Modemeinstellungen“ zu öffnen.

2 Aktivieren oder deaktivieren Sie das Kontrollkästchen **Modemsitzungen können digitale Sitzungen unterbrechen**.

3 Wählen Sie ein Authentifizierungs-Timeout von 30 bis 300 Sekunden und ein Inaktivitäts-Timeout von 1 bis 60 Sekunden.

4 Klicken Sie auf **Speichern**.

Setup-Einstellungen – Port-Sicherheit

Über den seriellen Setup-Port können Sie die Netzwerkkonfiguration der Einheit ändern, Debug-Informationen aktivieren und die Einheit zurücksetzen.

So aktivieren Sie ein Kennwort zur Einschränkung des Zugriffs auf den seriellen Setup-Port:

1 Klicken Sie in der seitlichen Navigationsleiste auf *RCS-Einstellungen - Ports - Setup*, um die Einstellungseite für den Setup-Port anzuzeigen.

2 Klicken Sie auf das Kontrollkästchen *Sicherheit für Setup-Port aktivieren*.

3 Geben Sie das Kennwort ein und bestätigen Sie dieses.

4 Klicken Sie auf *Speichern*.

Sitzungen

Auf dem Bildschirm „Aktive Sitzungen“ wird eine Liste aktiver Sitzungen und die folgenden zu jeder Sitzung gehörenden Informationen angezeigt: Zielgerät, Besitzer, Remote-Host, Dauer und Typ.

Konfiguration allgemeiner Sitzungen

So konfigurieren Sie allgemeine Sitzungseinstellungen:

1 Klicken Sie in der seitlichen Navigationsleiste auf *Sitzungen – Allgemein*. Der Bildschirm „Allgemeine Sitzungseinstellungen“ wird angezeigt.

2 Aktivieren oder deaktivieren Sie das Kontrollkästchen *Inaktivitäts-Timeout aktivieren*.

3 Geben Sie im Feld „Inaktivitäts-Timeout“ die Inaktivitätszeit ein, die vergehen soll, bis die Sitzung geschlossen wird (von 1 bis 90 Minuten).

4 Geben Sie im Feld „Anmeldungs-Timeout“ die Inaktivitätszeit ein, die vergehen soll, bis eine erneute Anmeldung erforderlich ist (von 21 bis 120 Sekunden).

5 Aktivieren oder deaktivieren Sie das Kontrollkästchen Timeout für Trennung aktivieren.

6 Geben Sie im Feld „Timeout für Trennung“ die Zeit (von 1 bis 120 Sekunden) ein, in der ein Hinweis angezeigt wird und Ihnen mitteilt, dass Ihre Sitzung getrennt wird.

7 Wählen Sie die verfügbaren Optionen zum Teilen von Sitzungen (Teilungs-Modus aktiviert, automatisches Teilen, exklusive Verbindung oder getarnte Verbindung) aus.

8 Wählen Sie ein Timeout der Eingabekontrolle zwischen 1 und 50 aus, wobei 1 für eine Zehntelsekunde steht.

9 Klicken Sie auf **Speichern**.

Konfiguration von KVM-Sitzungen

So konfigurieren Sie KVM-Sitzungseinstellungen:

1 Klicken Sie in der seitlichen Navigationsleiste auf Sitzungen – KVM. Der Bildschirm „KVM-Sitzungseinstellungen“ wird angezeigt.

2 Wählen Sie eine Verschlüsselungsebene für Tastatur- und Maussignale (128-Bit-SSL(**ARCFOUR**), DES, 3DES oder AES) und für Videosignale (128-Bit-SSL(**ARCFOUR**), DES, 3DES, **AES** oder Keine).

3 Wählen Sie eine Sprache im Dropdown-Menü „Tastatur“ aus.

4 Wenn in Ihrer Hardware ein USB2+CAC-SIP enthalten ist, wählen Sie die Bildschirmauflösung aus.

5 Klicken Sie auf **Speichern**.

Konfigurieren von lokalen Virtual Media-Sitzungen

So legen Sie Virtual Media-Optionen fest:

1 Klicken Sie in der seitlichen Navigationsleiste auf **Sitzungen – Virtual Media**, um den Bildschirm „Virtual Media-Sitzungseinstellungen“ zu öffnen.

2 Aktivieren oder deaktivieren Sie das Kontrollkästchen *Virtual Media gesperrt für KVM-Sitzungen*.

3 Aktivieren oder deaktivieren Sie das Kontrollkästchen **Reservierte Sitzungen zulassen**.

4 Wählen Sie eine der folgenden Optionen aus dem Dropdownmenü für den Virtual Media-Zugriffsmodus: *Schreibgeschützt* oder *Lese-/Schreibzugriff*.

5 Wählen Sie eine der Verschlüsselungsstufen, die verwendet werden soll.

6 Klicken Sie auf *Speichern*.

7 Aktivieren Sie das Kontrollkästchen neben dem SIP, für den Sie Virtual Media aktivieren möchten, und klicken Sie auf *VM aktivieren*.

- oder -

Aktivieren Sie das Kontrollkästchen neben dem SIP, für den Sie Virtual Media deaktivieren möchten, und klicken Sie auf *VM deaktivieren*.

Virtual Media-Optionen

Sie können das Verhalten des Switches während einer Virtual Media-Sitzung mithilfe der Optionen im Bildschirm „Virtual Media-Sitzungseinstellungen“

festlegen. In Tabelle 3.4 sind die Optionen dargestellt, die für Virtual Media-Sitzungen eingerichtet werden können.

Weitere Informationen zur Verwendung von Virtual Media in einer KVM-Sitzung finden Sie unter „Virtual Media“ auf Seite 103.

Tabelle 3.6: Virtual Media-Sitzungseinstellungen

Einstellung	Beschreibung
Sitzungseinstellungen: Virtual Media gesperrt für KVM-Sitzungen	Die Option „Gesperrt“ gibt an, ob eine Virtual Media-Sitzung für die KVM-Sitzung auf dem Zielgerät gesperrt wurde. Wenn die Option „Gesperrt“ aktiviert ist (Standardeinstellung) und die KVM-Sitzung geschlossen wird, wird auch die Virtual Media-Sitzung geschlossen. Wenn „Gesperrt“ deaktiviert ist und die KVM-Sitzung geschlossen wird, bleibt die Virtual Media-Sitzung weiterhin aktiv.
Sitzungseinstellungen: Reservierte Sitzungen zulassen	Stellt sicher, dass der Zugriff auf eine Virtual Media-Verbindung nur mit Ihrem Benutzernamen möglich ist und kein anderer Benutzer eine KVM-Verbindung zu diesem Zielgerät 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.

Einstellung	Beschreibung
Laufwerkzuordnungen: Virtual Media-Zugriffsmodus	Sie können den Zugriffsmodus für zugeordnete Laufwerke auf „Nur Lesezugriff“ bzw. „Lese- und Schreibzugriff“ einstellen. Im schreibgeschützten Zugriffsmodus können keine Daten auf das zugeordnete Laufwerk des Client-Servers geschrieben werden. Wenn der Zugriffsmodus Lese- und Schreibzugriff ist, können Sie Daten auf das zugeordnete Laufwerk schreiben bzw. von diesem lesen. Wenn das zugeordnete Laufwerk typenbedingt schreibgeschützt ist (beispielsweise bestimmte CD-ROM, DVD-ROM oder ISO-Images), wird der konfigurierte Schreib-Lese-Zugriff ignoriert. Das Festlegen des schreibgeschützten Zugriffsmodus ist nützlich, wenn ein Laufwerk mit Schreib-Lese-Zugriff, wie z. B. ein Massenspeichergerät oder ein USB-Wechselmedium, zugeordnet wird und Sie verhindern möchten, dass der Benutzer Daten darauf schreibt. Sie können ein DVD-Laufwerk und ein Massenspeichergerät gleichzeitig zuweisen. Ein CD-ROM-, DVD-Laufwerk oder eine ISO-Image-Datei wird als virtuelles CD-/DVD-Laufwerk zugewiesen.
Verschlüsselungsstufe	Sie können Verschlüsselungsstufen für Virtual Media-Sitzungen konfigurieren. Die folgenden Verschlüsselungsstufen stehen zur Verfügung: Keine (Standardeinstellung), 128-Bit-SSL (ARCFOUR), DES, 3DES und AES.
Virtual Media-Zugriff über SIP: VM aktivieren/deaktivieren	Im Abschnitt „Virtual Media-Zugriff über SIP-Adapter“ finden Sie alle Virtual Media-SIPs aufgelistet. Diese Auflistung enthält Einzelheiten über jedes Kabel, einschließlich der Option, Virtual Media für jedes Kabel zu aktivieren bzw. zu deaktivieren.

Lokale Benutzer

Lokale Benutzer können außerdem vom lokalen Sitzungsbildschirm das Verhalten von Virtual Media bestimmen. Zusätzlich zum Aktivieren und Deaktivieren

einer Virtual Media-Sitzung können Sie die Einstellungen aus folgender Tabelle konfigurieren.

Tabelle 3.7: Lokale Virtual Media-Sitzungseinstellungen

Einstellung	Beschreibung
CD-ROM/ DVD-ROM	Ermöglicht Virtual Media-Sitzungen mit dem ersten erkannten CD-ROM- oder DVD-ROM-Laufwerk (schreibgeschützt). Aktivieren Sie dieses Kontrollkästchen, um eine Virtual Media CD-ROM- oder DVD-ROM-Verbindung mit einem Zielgerät herzustellen. Deaktivieren Sie dieses Kontrollkästchen, um eine Virtual Media CD-ROM- oder DVD-ROM-Verbindung mit einem Zielgerät zu beenden.
Massenspeicher	Ermöglicht Virtual Media-Sitzungen mit dem ersten erkannten Massenspeichergerät. Aktivieren Sie dieses Kontrollkästchen, um eine Virtual Media-Verbindung zwischen einem Massenspeichergerät und einem Zielgerät herzustellen. Deaktivieren Sie das Kontrollkästchen, um eine Virtual Media-Verbindung zwischen einem Massenspeichergerät und einem Zielgerät zu beenden.
Reserviert	Stellt sicher, dass der Zugriff auf eine Virtual Media-Verbindung nur mit Ihrem Benutzernamen möglich ist und kein anderer Benutzer eine KVM-Verbindung zu diesem Zielgerät herstellen kann.

Konfiguration von seriellen Sitzungen

So konfigurieren Sie serielle Sitzungseinstellungen:

1 Klicken Sie in der seitlichen Navigationsleiste auf *Sitzungen – Seriell*, um den Bildschirm „Serielle Sitzungseinstellungen“ anzuzeigen.

2 Aktivieren oder deaktivieren Sie das Kontrollkästchen *Telnet-Zugriff aktiviert*.

3 Klicken Sie auf **Speichern**.

Einrichten von Benutzerkonten

Verwalten lokaler Benutzerkonten

Die Switch-OBWI bietet lokale und Anmeldungssicherheit durch vom Administrator definierte Benutzerkonten. Durch Auswahl von *Benutzerkonten* in der seitlichen Navigationsleiste können Administratoren Benutzer hinzufügen und löschen, Benutzerunterbrechungen und Zugriffsebenen festlegen und Kennwörter ändern.

Zugriffsebenen

Sobald ein Benutzerkonto hinzugefügt wird, kann der Benutzer zu den folgenden Zugriffsstufen zugewiesen werden: RCS-Administratoren, Benutzeradministratoren und Benutzer.

Tabelle 3.8: Zulässige Aktionen nach jeweiliger Zugriffsstufe

Vorgang	RCS-Benutzeradministrator	Benutzeradministrator	Benutzer
Einstellungen der Benutzeroberflächen-Zugriffsstufe konfigurieren	Ja	Nein	Nein
Zugriffsrechte konfigurieren	Ja	Ja	Nein
Benutzerkonten hinzufügen, ändern und löschen	Ja, für alle Zugriffsstufen	Ja, jedoch nur für Benutzer und Benutzeradministratoren	Nein
Eigenes Kennwort ändern	Ja	Ja	Ja

Vorgang	RCS-Benutzeradministrator	Benutzeradministrator	Benutzer
Auf Zielgerät zugreifen	Ja, alle Zielgeräte	Ja, alle Zielgeräte	Ja, falls zulässig

So fügen Sie ein neues Benutzerkonto hinzu (nur Benutzeradministratoren oder RCS-Administratoren):

1 Klicken Sie in der seitlichen Navigationsleiste auf *Benutzerkonten – Lokale Benutzerkonten*, um den Bildschirm „Lokale Benutzerkonten“ zu öffnen.

2 Klicken Sie auf die Schaltfläche *Hinzufügen*.

3 Geben Sie den Namen und das Kennwort des neuen Benutzers in die dafür vorgesehenen Felder ein.

4 Wählen Sie die Zugriffsebene für den neuen Benutzer aus.

5 Wählen Sie die jeweiligen verfügbaren Zielgeräte aus, die dem Benutzerkonto zugewiesen werden sollen, und klicken Sie auf **Hinzufügen**.

HINWEIS: Benutzeradministratoren und RCS-Administratoren können auf alle Zielgeräte zugreifen.

6 Klicken Sie auf *Speichern*.

So löschen Sie ein Benutzerkonto (nur Benutzeradministratoren oder RCS-Administratoren):

1 Klicken Sie in der seitlichen Navigationsleiste auf *Benutzerkonten – Lokale Benutzerkonten*, um den Bildschirm „Lokale Benutzerkonten“ zu öffnen.

2 Aktivieren Sie das Kontrollkästchen links neben jedem Konto, das Sie löschen möchten, und klicken Sie dann auf *Löschen*.

So bearbeiten Sie ein Benutzerkonto (nur Administratoren oder aktive Benutzer):

1 Klicken Sie in der seitlichen Navigationsleiste auf *Benutzerkonten – Lokale Benutzerkonten*. Der Bildschirm „Lokale Benutzerkonten“ wird angezeigt.

2 Klicken Sie auf den Namen des Benutzers, dessen Konto bearbeitet werden soll. Das Benutzerprofil wird angezeigt.

3 Geben Sie auf diesem Bildschirm die Benutzerinformationen ein und klicken Sie auf *Speichern*.

IP-Adressen der Avocent-Managementsoftware-Geräte

Sie können einen nicht verwalteten Switch mit einem Avocent-Managementsoftware-Server verbinden und anmelden, indem Sie die IP-Adresse des Managementsoftware-Servers angeben.

So konfigurieren Sie die IP-Adresse eines Servers:

1 Klicken Sie in der seitlichen Navigationsleiste auf *Benutzerkonten – **A**vocent*. Der Bildschirm „Einstellungen der Avocent-Managementsoftware“ wird angezeigt.

2 Geben Sie die IP-Adressen des Servers ein, mit dem Sie sich verbinden möchten. Bis zu vier Adressen sind zulässig.

3 Nutzen Sie die Bildlaufleiste, um das gewünschte Wiederholungsintervall auszuwählen.

4 Zum Trennen eines am Server angemeldeten RCS klicken Sie auf die Schaltfläche **Trennen**.

5 Klicken Sie auf *Speichern*.

LDAP

Mithilfe der Dell RCS-Software oder OBWI mit LDAP-Unterstützung (Lightweight Directory Assistance Protocol) kann der Dell 1082DS/2162DS/4322D RCS Benutzer über eine lokale Datenbank oder einen externen, skalierbaren, dezentralisierten Verzeichnisdienst authentifizieren und

autorisieren. Nähere Informationen zur Konfiguration und Nutzung des LDAP am RCS entnehmen Sie dem LDAP-Abschnitt.

Admin umgehen

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. Lesen Sie hierzu auch „Konto für ‚Admin umgehen' konfigurieren“ in Kapitel 5.

Aktive Sitzungen

Auf dem Bildschirm „Aktive Sitzungen“ wird eine Liste aktiver Sitzungen und die folgenden zu jeder Sitzung gehörenden Informationen angezeigt: Zielgerät, Besitzer, Remote-Host, Dauer und Typ.

Schließen einer Sitzung

So schließen Sie eine Sitzung:

1 Klicken Sie in der seitlichen Navigationsleiste auf *Aktive Sitzungen*, um den Bildschirm für die aktiven RCS-Sitzungen anzuzeigen.

2 Aktivieren Sie die Kontrollkästchen neben den gewünschten Zielgeräten.

3 Klicken Sie auf *Trennen*.

HINWEIS: Gibt es eine zugehörige gesperrte Virtual Media-Sitzung, so wird diese getrennt.

So schließen Sie eine Sitzung (nur lokale Benutzer):

1 **Klicken Sie in der seitlichen Navigationsleiste auf Lokale Sitzung.**

2 Aktivieren Sie das Kontrollkästchen **Aktive Sitzung trennen**.

4

Video Viewer-Fenster

Über den Video Viewer werden KVM-Sitzungen mit den Zielgeräten durchgeführt, die an einen Switch angeschlossen sind und über die OBWI verwaltet werden. Wenn Sie mithilfe des Video Viewers eine Verbindung mit einem Gerät herstellen, wird der Desktop des Zielgeräts in einem separaten Video Viewer-Fenster angezeigt und enthält den lokalen als auch den Cursor des Zielgeräts.

Die Switch-OBWI-Software verwendet ein Java-basiertes Programm zum Anzeigen des Video Viewer-Fensters. Die Switch-OBWI lädt den Video Viewer automatisch herunter und installiert ihn, wenn der Video Viewer das erste Mal geöffnet wird.

HINWEIS: Java 1.6.0_11 oder höher wird benötigt, um eine Sitzung zu starten.

HINWEIS: Die Switch-OBWI installiert nicht die Java Resource Engine (JRE). Die JRE wird als kostenloser Download zur Verfügung gestellt unter http://www.sun.com.

HINWEIS: Die Switch-OBWI verwendet den Systemspeicher, um Bildanzeigen in Video Viewer-Fenstern zu speichern und anzuzeigen. Jedes separat geöffnete Video Viewer-Fenster erfordert zusätzlichen Systemspeicher. Eine 8-Bit-Farbeinstellung auf dem Server erfordert 1,4 MB, eine 16-Bit-Farbeinstellung erfordert 2,4 MB und eine 32-Bit-Farbeinstellung erfordert 6,8 MB Speicher pro Video Viewer-Fenster. Wenn Sie mehr Video Viewer-Fenster öffnen, als Ihr System zulässt (gewöhnlich sind es vier), erhalten Sie die Nachricht „Nicht genügend Arbeitsspeicher“ und das angeforderte Video Viewer-Fenster wird nicht geöffnet.

Wenn das Gerät, auf das Sie versuchen zuzugreifen, momentan von einem anderen Benutzer verwendet wird, werden Sie dazu aufgefordert, die Sitzung des anderen Benutzers zu unterbrechen, sofern Ihre Benutzerunterbrechungsstufe gleich oder höher als die des anderen Benutzers ist. Ein RCS-Administrator kann

auch einen aktiven Benutzer über die Seite „Aktive Sitzung“ unterbrechen. Weitere Informationen finden Sie unter RCS„Aktive Sitzungen“ auf Seite 86.

Abbildung 4.1. Video Viewer-Fenster (normaler Fenstermodus)

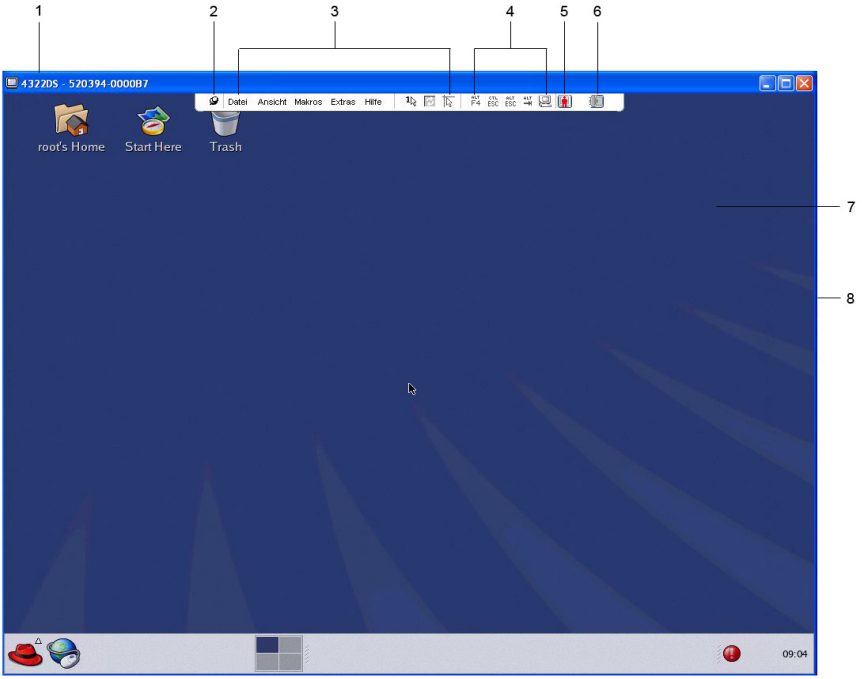


Tabelle 4.1: Beschreibungen Video Viewer

Nummer	Beschreibung
1	Titelleiste: Zeigt den Namen des angezeigten Zielgeräts an. Im Vollbildmodus wird die Titelleiste ausgeblendet und der Zielgerätename zwischen Menü und Symbolleiste angezeigt.

Nummer	Beschreibung
2	Pin-Symbol: Verankert die Menü- und Symbolleisten, sodass sie ständig sichtbar sind.
3	Menü- und Symbolleiste: Ermöglicht den Zugriff auf viele Funktionen im Video Viewer-Fenster. Die Menü- und Symbolleisten können ein- und ausgeblendet werden, wenn der Pin nicht verwendet wird. Platzieren Sie den Cursor auf der Symbolleiste, um die Menü- und Symbolleisten anzuzeigen. Bis zu zehn Befehle und/oder Makrogruppen-Schaltflächen können auf der Symbolleiste angezeigt werden. Standardmäßig werden die Schaltflächen für Einzelcursor-Modus, Aktualisieren, Automatische Monitoranpassung und Lokalen Cursor ausrichten auf der Symbolleiste angezeigt. Weitere Informationen finden Sie unter „Ändern der Symbolleiste“ auf Seite 90 und „Makros“ auf Seite 112.
4	Makro-Schaltflächen: Häufig verwendete Tastenfolgen, die an das Zielgerät gesendet werden können.
5	Verbindungsstatusanzeige: Zeigt den Status des Benutzers an, der mit dem RCS für diesen Server verbunden ist. Diese Modi lauten: Exklusiv, aktive Basis-Verbindung, primäre aktive Teilung, sekundäre aktive Teilung, passive Teilung, getarnte Verbindung und Scan-Verbindung.
6	Smart Card-Statusanzeigen: Diese zeigen an, ob sich eine Smart Card im Smart Card-Lesegerät befindet. Das Smart Card-Symbol im Video Viewer wird grau angezeigt und bedeutet somit, dass die Smart Card-Option nicht zur Verfügung steht oder deaktiviert wurde. Das Symbol ist grün, wenn die Smart Card zugeordnet wurde.
7	Anzeigebereich: Greift auf den Server-Desktop zu.
8	Rahmen: Ändert durch Klicken und Halten des Rahmens die Größe des Video Viewer-Fensters.

Ändern der Symbolleiste

Sie können eine Zeitspanne bestimmen, die verstreicht, bevor die Symbolleiste im Video Viewer-Fenster ausgeblendet wird, sofern diese frei beweglich ist, d. h. nicht mit einem Pin fixiert ist.

So legen Sie die Zeitspanne, die verstreicht, bis die Symbolleiste ausgeblendet wird:

1 Wählen Sie im Video Viewer-Menü Extras – Sitzungsoptionen aus.

- oder -

Klicken Sie auf die Schaltfläche Sitzungsoptionen.

Das Dialogfeld „Sitzungsoptionen“ wird angezeigt.

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

3 Verwenden Sie die Pfeiltasten, um die Anzahl der Sekunden festzulegen, die verstreichen sollen, bis die Symbolleiste ausgeblendet wird.

4 Klicken Sie auf OK, um die Änderungen zu speichern und schließen Sie das Dialogfeld.

Starten einer Sitzung

HINWEIS: Bei einer langsameren Netzwerkverbindung ohne Proxy-Server kann die Bildqualität ungenügend sein. Da bestimmte Farbeinstellungen (wie z. B. Grauskala) weniger Netzwerkbandbreite als andere (wie z. B. optimale Farbe) benötigen, kann das Ändern der Farbeinstellungen die Bildqualität verbessern. Die beste Bildqualität bei langsamen Netzwerkverbindungen erzielen Sie mit Einstellungen wie Grauskala/optimale Kompression oder Geringe Farbe/Hohe Kompression. Weitere Informationen finden Sie unter „Anpassen der Ansicht“ auf Seite 92.

HINWEIS: Wenn ein Benutzer eine Verbindung zu einem Zielgerät mit einer höheren Auflösung aufbaut als auf dem lokalen Computer, zeigt das Video Viewer-Fenster einen Teil des Zielgerätebildschirms mit Bildlaufleisten zur Anzeige der verdeckten Teile des Bildschirms an. Der Benutzer kann sich den gesamten Bildschirm anzeigen lassen, indem die Auflösung des Zielgeräts, des lokalen Computers oder beider Geräte angepasst wird.

So starten Sie eine KVM-Sitzung über das Switch-Explorer-Fenster:

1 Klicken Sie auf ein auf dem Bildschirm „Zielgeräte“ aufgeführtes Gerät, um das Fenster „Einheiten-Überblick“ aufzurufen.

2 Klicken Sie auf den Link *KVM-Sitzung*, um den Video Viewer in einem neuen Fenster zu öffnen.

Sitzungs-Zeitlimit

Bei einer Remote-Sitzung kann ein Timeout erfolgen, wenn im Sitzungsfenster in einer bestimmten Zeit keine Aktivität erkannt wird. Der Wert für das Sitzungs-Timeout kann im Fenster „RCS KVM-Sitzungseinstellungen“ konfiguriert werden. Dieser festgelegte Timeout-Wert wird dann beim nächsten Zugriff auf die OBWI des Switches verwendet.

So aktivieren, deaktivieren oder konfigurieren Sie das Sitzungs-Timeout:

1 Wählen Sie in der seitlichen Navigationsleiste *Einheiten-Ansicht – RCS – RCS-Einstellungen – Sitzungen – Allgemein* aus.

2 Wählen Sie gewünschte Einstellung für das Feld *Aktivitäts-Timeout aktivieren*.

3 Legen Sie, falls erforderlich, die Zeitbegrenzung für das Inaktivitäts-Timeout fest.

4 Klicken Sie auf *Speichern*.

Fenstergröße

HINWEIS: Der Befehl Ansicht – Skalierung steht nicht zur Verfügung, wenn das Video Viewer-Fenster im Vollbildmodus angezeigt wird. Benutzer, die nicht primäre Benutzer einer geteilten Sitzung sind, haben ebenfalls keinen Zugriff auf diesen Befehl.

Wenn Sie die Switch-OWBI zum ersten Mal verwenden, werden alle geöffneten Video Viewer-Fenster mit einer Auflösung von 1024 x 768 angezeigt, bis der Benutzer diesen Wert ändert. Jedes einzelne Video Viewer-Fenster kann auf eine andere Auflösung eingestellt werden.

Die Switch-OBWI passt die Anzeige automatisch an, wenn die Fenstergröße während einer Sitzung geändert wird und die automatische Skalierung aktiviert ist. Wenn sich die Auflösung des Zielgeräts während einer Sitzung verändert, wird die Anzeige automatisch angepasst.

So ändern Sie die Auflösung des Video Viewer-Fensters:

1 Wählen Sie den Befehl *Ansicht – Skalierung* aus.

2 Wählen Sie die gewünschte Auflösung aus.

Anpassen der Ansicht

Mithilfe der Menüs und Schaltflächen im Video Viewer-Fenster können Sie folgende Aktionen ausführen:

- Die Mauscursor ausrichten.
- Den Bildschirm aktualisieren.
- Den Vollbildmodus aktivieren oder deaktivieren. Bei aktiviertem Vollbildmodus passt sich das Bild an den Desktop mit einer Größe von 1600 x 1200 oder 1680 x 1050 (Breitbild) an.Wenn der Desktop auf eine höhere Auflösung eingestellt ist, geschieht Folgendes:
  - Das Vollbild wird in der Mitte des Bildschirms zentriert dargestellt. Die nicht ausgefüllten Bereiche bleiben schwarz.
  - Die Menü- und Symbolleisten sind verankert, sodass sie immer sichtbar sind.
- Die automatische, vollständige oder manuelle Skalierung der Sitzungsanzeige aktivieren:
  - Wenn die vollständige Skalierung ausgewählt wird, behält das Desktop-Fenster seine Größe bei und die Zielgeräte-Anzeige wird so angepasst, dass sie das Fenster ausfüllt.
  - Bei der automatischen Skalierung wird das Desktop-Fenster an die Auflösung des angezeigten Zielgeräts angepasst.

- Wenn die manuelle Skalierung ausgewählt wird, wird ein Dropdownmenü der unterstützten Auflösungen der Bildschirmskalierung angezeigt.

- Ändern Sie die Farbtiefe der Sitzungsanzeige.

So richten Sie die Mauszeiger aufeinander aus:

Klicken Sie in der Video Viewer-Symbolleiste auf die Schaltfläche *Lokalen Cursor ausrichte*n. Der lokale Cursor sollte auf den Cursor des Remote-Gerätes ausgerichtet werden.

HINWEIS: Deaktivieren Sie die Mausbeschleunigung des angeschlossenen Geräts, wenn der Cursor nicht einwandfrei ausgerichtet ist.

Klicken Sie zum Aktualisieren der Anzeige auf die Schaltfläche *Anzeige aktualisieren* im Video Viewer-Fenster oder wählen Sie *Ansicht – Aktualisieren* aus dem Video Viewer-Menü aus. Die digitalisierte Darstellung wird vollständig regeneriert.

Klicken Sie für den Vollbildmodus auf die Schaltfläche *Maximieren* oder wählen Sie *Ansicht – Vollbild* aus dem Video Viewer-Menü aus. Das Desktop-Fenster wird ausgeblendet und nur der aufgerufene Desktop des Zielgeräts wird angezeigt. Der Bildschirm ändert sich auf eine maximale Auflösung von 1600 x 1200 oder 1680 x 1050 (Breitbild). Wenn der Desktop eine höhere Auflösung besitzt, wird ein schwarzer Rahmen um das Vollbild angezeigt. Die unverankerte Symbolleiste wird angezeigt.

Klicken Sie auf der unverankerten Symbolleiste auf die Schaltfläche *Vollbildmodus*, um den Vollbildmodus zu deaktivieren und zum Desktop-Fenster zurückzukehren.

Zum Aktivieren der automatischen Skalierung gehen Sie im Video Viewer-Menü auf die Option *Ansicht – Skalierung* und wählen Sie **Vollbild**. Die Geräteanzeige skaliert sich automatisch auf die Auflösung des angezeigten Zielgeräts.

Zum Aktivieren der manuellen Skalierung wählen Sie im Video Viewer-Menü die Option *Ansicht – Skalierung*. Wählen Sie die Fenstergröße aus, auf die skaliert

werden soll. Die verfügbaren Größen für die manuelle Skalierung variieren je nach System.

Aktualisieren der Anzeige

Klicken Sie im Dialogfeld „Manuelle Monitoranpassung“ auf die Schaltfläche *Bildschirm aktualisieren*, um die digitalisierte Bildschirmdarstellung vollständig neu zu generieren.

HINWEIS: Sie können außerdem *Ansicht – Aktualisieren* im Video Viewer-Menü auswählen, um den Bildschirm zu aktualisieren.

Videoeinstellungen

Zusätzliche Monitoranpassung

Generell dienen die automatischen Anpassungsfunktionen des Video Viewer-Fensters dazu, das Bild für die bestmögliche Darstellung zu optimieren. Benutzer können die Bildanzeige jedoch mithilfe des Kundendienstes von Dell von feineinstellen, indem Sie im Video Viewer-Menü auf *Extras – Manuelle Monitoranpassung* oder auf die Schaltfläche *Manuelle Monitoranpassung* im Video Viewer-Fenster klicken. Das Dialogfeld „Manuelle Monitoranpassung“ wird angezeigt. Die Videoeinstellung richtet sich immer nach dem Zielgerät.

Benutzer können auch die Pakete pro Sekunde überprüfen, die für die Unterstützung eines statischen Bildschirms erforderlich sind, indem sie die Paketdurchsatzrate in der unteren linken Ecke des Dialogfelds beobachten.

So passen Sie die Videoqualität des Fensters manuell an:

HINWEIS: Die folgenden Einstellungen der Videoqualität sollten nur mit Unterstützung des Kundendienstes von Dell vorgenommen werden.

1 Wählen Sie im Video Viewer-Menü die Option *Extras – Manuelle Monitoranpassung*.

- oder -

Klicken Sie auf die Schaltfläche *Manuelle Monitoranpassung*.

Das Dialogfeld „Manuelle Monitoranpassung“ wird angezeigt.

Abbildung 4.2. Dialogfeld „Manuelle Monitoranpassung“

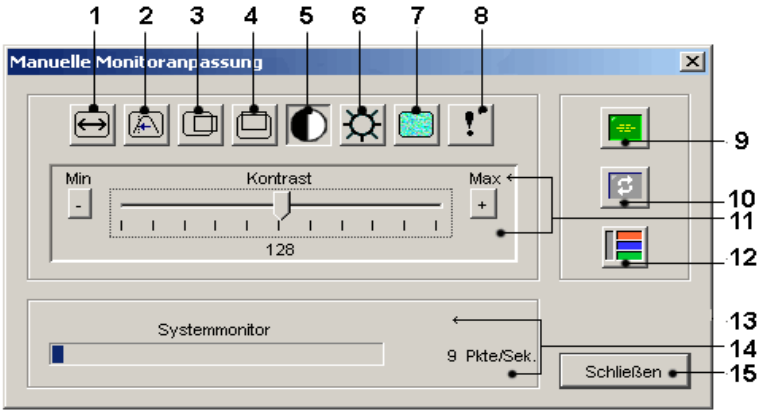


Tabelle 4.2: Abbildung 4.2

Nummer	Beschreibung	Nummer	Beschreibung
1	Bild-Aufnahmebreite	9	Automatische Monitoranpassung
2	Pixel-Sampling/Feineinstellung	10	Bild aktualisieren
3	Horizontale Bildaufnahme	11	Schieberegler
4	Vertikale Bildaufnahme	12	Testbild
5	Kontrast	13	Hilfe
6	Helligkeit	14	Systemmonitor

Nummer	Beschreibung	Nummer	Beschreibung
7	Rauschschwelle	15	Schaltfläche „Schließen“
8	Prioritätsschwelle		

2 Klicken Sie auf das Symbol für die anzupassende Funktion.

3 Bewegen Sie den Schieberegler und führen Sie dann eine Feinabstimmung durch Klicken auf die Schaltflächen *Min* (-) oder *Max* (+) durch, um die Parameter für das jeweils angeklickte Symbol anzupassen. Die Einstellungen werden sofort im Video Viewer-Fenster sichtbar.

4 Wenn Sie den Vorgang beendet haben, klicken Sie auf *Schließen*, um das Dialogfeld „Manuelle Monitoranpassung“ zu verlassen.

Monitoreinstellungen am Zielgerät

Die Einstellungen Bild-Aufnahmebreite, Feineinstellung für Pixel-Sampling, Horizontale Bild-Aufnahme und Vertikale Bild-Aufnahme beeinflussen die Aufnahme und Digitalisierung des Zielbildschirms und werden selten geändert.

Die Parameter für die Bild-Aufnahme werden automatisch von der automatischen Anpassungsfunktion geändert. Für das Zielbild sind spezielle Einstellungen nötig, damit genaue Anpassungen unabhängig durchgeführt werden können.

Automatische Monitoranpassung

In den meisten Fällen müssen die Standardeinstellungen für die Videoparameter nicht verändert werden. Das System stellt sich automatisch ein und verwendet die optimalen Videoparameter. Die Switch-OBWI arbeitet am Besten, wenn die Videoparameter so eingestellt sind, dass keine (0) Videopakete für einen Statikbildschirm übertragen werden.

Die Videoparameter können auf einfache Weise auf die bestmöglichen Einstellungen durch Klicken im Dialogfeld „Manuelle Monitoranpassung“ auf die Schaltfläche *Automatische Monitoranpassung* eingestellt werden.

HINWEIS: Sie können auch aus dem Video Viewer-Menü *Extras – Automatische Monitoranpassung* auswählen oder auf das Symbol für *Automatische Monitoranpassung* in der Toolbar klicken, um die Monitoreinstellungen anzupassen.

Testbild

Durch Klicken auf die Schaltfläche *Testbild* im Dialogfeld „Manuelle Monitoranpassung“ wird auf ein Testbild umgeschaltet. Klicken Sie erneut auf die Schaltfläche *Testbild*, um zur normalen Videoanzeige zurückzuschalten.

Anbieterspezifische Videoeinstellungen

Die Videoeinstellungen sind von Hersteller zu Hersteller unterschiedlich. Dell verfügt über eine Online-Datenbank mit optimierten Videoeinstellungen für eine Vielzahl von Grafikkarten, besonders für Sun-spezifische Sätze. Diese Informationen können Sie über die Online Knowledge Base oder vom Kundendienst von Dell erhalten.

Farbeinstellungen

Anpassen der Farbtiefe

Der Videokomprimierungsalgorithmus Dambrackas Video Compression® (DVC) ermöglicht es Benutzern, die Anzahl der sichtbaren Farben eines Remote-Sitzungsfensters 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 Video Viewer-Fensters sind folgende Optionen möglich: Optimale verfügbare Farbe (langsamere Aktualisierung), optimale Kompression (schnellste Aktualisierung), eine Kombination aus optimaler Farbe und optimaler Kompression oder Grauskala.

Die Farbtiefen von einzelnen Ports und Kanälen können durch Auswahl des Befehls *Farbe anzeigen* in einem Remote-Sitzungsfenster festgelegt werden. Diese Einstellungen werden individuell für jeden Kanal gespeichert.

Kontrast und Helligkeit

Falls das Bild im Video Viewer-Fenster zu dunkel oder zu hell ist, wählen Sie *Extras – Automatische Monitoranpassung* aus oder klicken Sie auf die Schaltfläche *Automatische Monitoranpassung*. Dieser Befehl ist auch im Dialogfeld „Monitoranpassung“ verfügbar. Dies korrigiert in den meisten Fällen Störungen bei der Bilddarstellung.

Wenn durch mehrmaliges Klicken auf *Automatische Anpassung* der Kontrast und die Helligkeit nicht wie gewünscht eingestellt werden, kann eventuell eine manuelle Anpassung hilfreich sein. Erhöhen Sie die Helligkeit. Erhöhen Sie die Helligkeit nicht um mehr als 10 Stufen, bevor Sie mit dem Kontrast fortfahren. Generell sollte der Kontrast nur gering geändert werden.

Rauschschwellen-Einstellungen

Schwellenwerte für die Bilderkennung

In einigen Fällen kann es vorkommen, dass das Rauschen bei der Bildübertragung die Übertragungsrate der Pakete hochhält, was durch kleine sich verändernde Punkte im Bereich des sich bewegenden Cursors zu erkennen ist. Das Ändern der Schwellenwerte kann dazu führen, dass die Bildschirme rauschfreier sind und das Mauszeiger-Tracking verbessert wird.

Sie können die Werte für Rausch- und Prioritätsschwelle verändern, wenn Sie die standardmäßige Videokomprimierung verwenden. Die Schwellenwerte können durch Klicken auf *Automatische Monitoranpassung* wiederhergestellt werden.

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: Zur Einstellung der Rauschschwelle für größere Änderungen wird der Schieberegler und zur Feinabstimmung werden die Schaltflächen Plus (+) und Minus (-) an den Enden des Schiebereglers verwendet.

Siehe „Anpassen der Ansicht“ auf Seite 92 für weitere Informationen zum Ändern der Farbtiefe.

Mauseinstellungen

Anpassen der Mausoptionen

Die Mausoptionen des Video Viewer-Fensters beeinflussen den Cursortyp, den Cursor-Modus, die Skalierung, die Ausrichtung und das Zurücksetzen. Die Mauseinstellungen sind gerätespezifisch und können für jedes Gerät unterschiedlich festgelegt werden.

HINWEIS: Wenn das Gerät das Trennen und den erneuten Anschluss der Maus nicht unterstützt (fast alle neueren Computer unterstützen dies), wird die Maus deaktiviert und das Gerät muss neu gestartet werden.

Cursor-Typ

Das Video Viewer-Fenster bietet fünf Anzeigemöglichkeiten für den lokalen Mauszeiger. Sie können auch den Standard-Cursor auswählen oder festlegen, dass kein Cursor angezeigt werden soll.

Im Einzelcursor-Modus wird der lokale (zweite) Cursor im Video Viewer-Fenster nicht angezeigt und nur der Cursor des Zielgeräts wird angezeigt. Die einzigen Mausbewegungen, die angezeigt werden, sind die des Remote-Cursors auf dem Zielgerät. Verwenden Sie den Einzelcursor-Modus, wenn der Einsatz eines lokalen Cursors nicht erforderlich ist.

Abbildung 4.3. Video Viewer-Fenster mit angezeigtem lokalen und Remote-Cursor

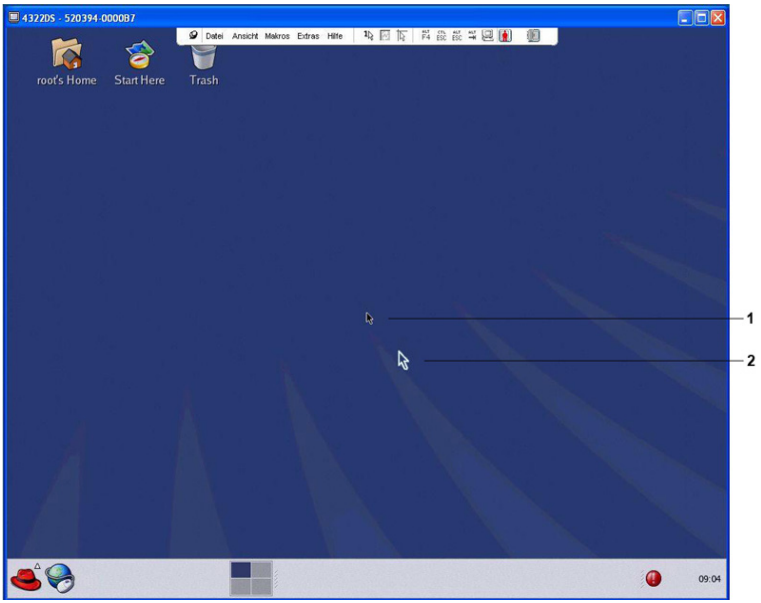


Tabelle 4.3: Abbildung 4.3

Nummer	Beschreibung
1	Remote-Cursor
2	Lokaler Cursor

Der Status des Cursormodus des Video Viewer-Fensters einschließlich des Tastenanschlags, der den Einzelcursormodus beendet, wird in der Titelleiste angezeigt. Sie können den Tastenanschlag, mit dem der Einzelcursormodus beendet wird, im Dialogfeld „Sitzungsoptionen“ festlegen.

HINWEIS: Wenn Sie ein Gerät verwenden, dass Tastenanschläge aufzeichnet, bevor diese den Client-Server erreichen, sollten Sie möglichst nicht diese Tastenanschläge verwenden, um den Mauszeiger wiederherzustellen.

Wählen Sie zum Aufrufen des Einzelcursormodus *Extras – Einzelcursormodus* aus dem Video Viewer-Menü aus, oder klicken Sie auf die Schaltfläche *Einzelcursormodus*. Der lokale Cursor wird nicht angezeigt und alle Bewegungen sind relativ zum Zielgerät.

So legen Sie eine Taste für das Beenden des Einzelcursormodus fest:

1 Wählen Sie im Video Viewer-Menü *Extras – Sitzungsoptionen* aus.

- oder -

Klicken Sie auf die Schaltfläche *Sitzungsoptionen*.

Das Dialogfeld „Sitzungsoptionen“ wird angezeigt.

2 Klicken Sie auf das Register *Maus*.

3 Wählen Sie im Bereich Einzelcursormodus den gewünschten Tastenanschlag zum Beenden des Modus aus dem Dropdownmenü aus.

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

Wenn der Einzelcursormodus aktiviert ist, können Sie die festgelegte Taste drücken, um zum normalen Desktop-Modus zurückzukehren.

Drücken Sie die Taste, die in der Titelleiste angezeigt wird, um den Einzelcursormodus zu beenden.

So ändern Sie die Mauszeigereinstellung:

1 Wählen Sie im Video Viewer-Menü *Extras – Sitzungsoptionen* aus.

- oder -

Klicken Sie auf die Schaltfläche *Sitzungsoptionen*.

Das Dialogfeld „Sitzungsoptionen“ wird angezeigt.

2 Klicken Sie auf das Register *Maus*.

3 Wählen Sie im Bereich „Lokaler Cursor“ einen Mauszeigertyp aus.

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

Maus-Skalierung

Einige ältere Linux Versionen unterstützten keine anpassbaren Mausbeschleunigungen. Bei Installationen, die diese älteren Versionen unterstützen müssen, können Sie zwischen drei vorkonfigurierten Mausskalierungsoptionen wählen oder Ihre eigene benutzerdefinierte Skalierung einstellen. Die vorkonfigurierten Einstellungen sind „Standard“ (1:1), „Hoch“ (2:1) oder „Niedrig“ (1:2):

- Bei einem Skalierverhältnis von 1:1 sendet jede Mausbewegung auf dem Desktop-Fenster die gleiche Mausbewegung an das Zielgerät.
- Bei einem Skalierverhältnis von 2:1 sendet die gleiche Mausbewegung eine doppelte Mausbewegung.
- Bei einem Skalierverhältnis von 1:2 bewirkt eine Halbierung des Wertes.

So stellen Sie die Mausskalierung ein:

1 Wählen Sie im Video Viewer-Menü *Extras – Sitzungsoptionen* aus.

- oder -

Klicken Sie auf die Schaltfläche *Sitzungsoptionen*.

Das Dialogfeld „Sitzungsoptionen“ wird angezeigt.

2 Klicken Sie auf das Register *Maus*.

3 Wählen Sie die entsprechende Optionsschaltfläche aus, um eine der vorkonfigurierten Einstellungen zu verwenden.

- oder -

So stellen Sie eine benutzerdefinierte Skalierung ein:

a. Klicken Sie auf die Optionsschaltfläche *Benutzerdefiniert*, um die X- und Y-Felder zu aktivieren.

b. Geben Sie die Skalierungswerte in die X- und Y-Felder ein. Jede Mausbewegung wird mit den entsprechenden X- und Y-Skalierungsfaktoren multipliziert. Der zulässige Eingabebereich liegt zwischen 0,25-3,00.

Maus-Ausrichtung und Synchronisation

Die OBWI des Switches kann nicht kontinuierlich Rückmeldungen von der Maus erhalten. Das kann dazu führen, dass die Maus am Switch nicht mehr mit der Maus am Host-System synchronisiert ist. Wenn Maus oder Tastatur nicht mehr ordnungsgemäß reagieren, kann die Maus neu ausgerichtet werden, um eine ordnungsgemäße Synchronisation wiederherzustellen.

Eine Ausrichtung bewirkt die Ausrichtung des lokalen Cursors auf den Cursor des Remote-Zielgeräts. Ein Zurücksetzen bewirkt eine Simulation eines erneuten Verbindungsaufbaus von Maus und Tastatur, genau wie bei einer hardwaremäßigen Trennung und darauffolgendem Neuanschluss.

Zum Ausrichten des Mauszeigers klicken Sie in der Video Viewer-Symbolleiste auf die Schaltfläche *Lokalen Cursor ausrichten*.

Virtual Media

Mithilfe der Virtual Media-Funktion können Sie ein physikalisches Laufwerk des Client-Computers als virtuelles Laufwerk auf dem Zielgerät zuweisen. Sie können auch eine ISO- oder Disk-Image-Datei des lokalen Clients als virtuelles Laufwerk auf dem Zielgerät hinzufügen und zuweisen. Sie können ein CD-ROM-Laufwerk und ein Massenspeichergerät gleichzeitig zuweisen.

- Ein CD-ROM-/DVD-Laufwerk oder eine Disk-Image-Datei (wie eine ISO- oder Disketten-Image-Datei) wird als virtuelles CD-/DVD-ROM-Laufwerk zugewiesen.
- Diskettenlaufwerke, USB-Speichergeräte oder andere Speichermedien werden als virtuelle Massenspeichergeräte zugewiesen.

Weitere Informationen zur Konfiguration der Virtual Media-Einstellungen über die OBWI finden Sie unter „Konfigurieren von lokalen Virtual Media-Sitzungen“ auf Seite 79.

Anforderungen

Das Zielgerät muss Virtual Media unterstützen und mit einem USB2- oder USB2+CAC-SIP an den KVM-Switch angeschlossen sein.

Das Zielgerät muss auf jeden Fall die Typen USB2-kompatibler Speichermedien unterstützen, die Sie virtuell zuweisen. Anders gesagt, wenn das Zielgerät tragbare USB-Speichergeräte nicht unterstützt, können Sie dieses Gerät nicht als Virtual Media-Laufwerk auf dem Zielgerät zuweisen.

Sie (oder die Benutzergruppe, zu der Sie gehören) müssen über die Berechtigung verfügen, Virtual Media-Sitzungen und/oder reservierte Virtual Media-Sitzungen auf dem Zielgerät öffnen zu können. Siehe „Einrichten von Benutzerkonten“ auf Seite 83.

Es kann immer jeweils nur eine Virtual Media-Sitzung zu einem Zielgerät aktiv sein.

Überlegungen zum Teilen und Trennen von Sitzungen

Die KVM- und Virtual Media-Sitzungen werden unabhängig voneinander ausgeführt. Daher stehen viele Möglichkeiten zum Teilen, Reservieren oder Trennen von Sitzungen zur Verfügung. Die Avocent-Managementsoftware bietet die Flexibilität, diese Systemanforderungen zu erfüllen.

Zum Beispiel können die KVM- und Virtual Media-Sitzungen zusammen gesperrt werden. Wenn in diesem Modus eine KVM-Sitzung getrennt wird, wird auch die zugehörige Virtual Media-Sitzung getrennt. Wenn die Sitzungen nicht zusammen gesperrt wurden, kann die KVM-Sitzung geschlossen werden, während die Virtual Media-Sitzung aktiv bleibt. Dies kann vorteilhaft sein, wenn ein Benutzer eine zeitintensive Aufgabe unter Verwendung der Virtual Media-Sitzung (wie z. B. das Laden eines Betriebssystems) ausführt und gleichzeitig eine KVM-Sitzung zu einem anderen Zielgerät aufbauen möchte, um andere Funktionen auszuführen, bis das Laden des Betriebssystems abgeschlossen ist.

Wenn auf dem Zielgerät eine aktive Virtual Media-Sitzung ohne eine zugehörige aktive KVM-Sitzung ausgeführt wird, kann entweder der erste Benutzer (Benutzer A) oder ein anderer Benutzer (Benutzer B) mit diesem Kanal eine

Verbindung herstellen. Sie können eine Option (Reserviert) im Dialogfeld „Virtual Media“ festlegen, sodass nur Benutzer A auf das entsprechende Zielgerät mit ausgeführter KVM-Sitzung zugreifen kann.

Wenn Benutzer B auf diese Sitzung zugreifen darf (die Option „Reserviert“ ist deaktiviert), kann er das Speichermedium steuern, das bei der Virtual Media-Sitzung verwendet wird. Durch Verwenden der Option „Reserviert“ in einer kaskadierten Umgebung kann nur Benutzer A auf den unteren Switch zugreifen. Der KVM-Kanal zwischen dem oberen und unteren Switch ist für Benutzer A reserviert.

Dialogfeld „Virtual Media“

Verwenden Sie das Dialogfeld „Virtual Media“, um das Zuweisen von Virtual Media bzw. das Aufheben der Zuweisung zu verwalten. Das Dialogfeld zeigt alle physischen Laufwerke des Client-Servers, die als Virtual Media zugewiesen werden können. Sie können auch ISO- und Disk-Image-Dateien hinzufügen und sie dann mithilfe des Dialogfelds „Virtual Media“ zuweisen.

Nach der Zuweisung eines Geräts werden in der Detailansicht im Dialogfeld „Virtual Media“ die Menge der übertragenen Daten und die seit der Zuweisung des Geräts verstrichene Zeit angezeigt.

Sie können angeben, ob die Virtual Media-Sitzung reserviert werden soll. Wenn eine Sitzung reserviert wurde und die zugehörige KVM-Sitzung geschlossen wird, kann kein anderer Benutzer eine KVM-Sitzung auf diesem Zielgerät öffnen. Wenn eine Sitzung nicht reserviert wurde, kann eine andere KVM-Sitzung geöffnet werden.

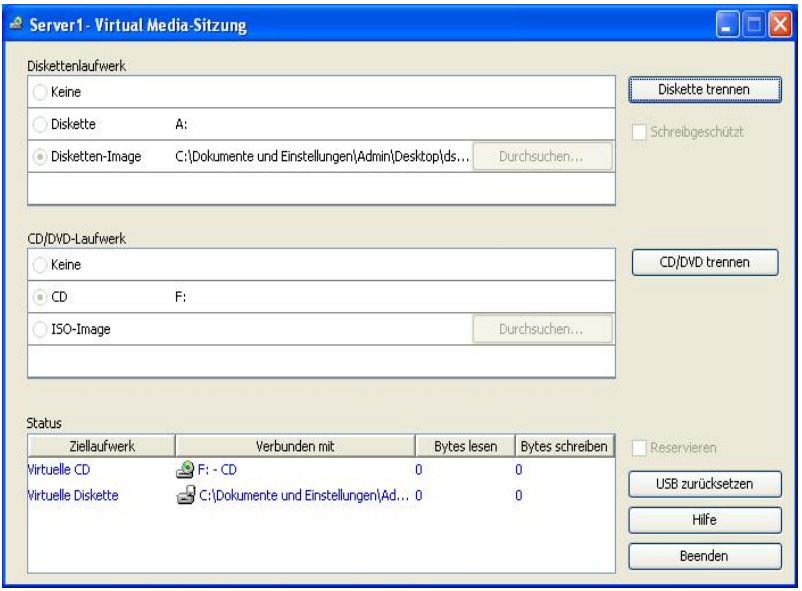
Über das Virtual Media-Dialogfeld können Sie den SIP auch zurücksetzen. Dieser Vorgang setzt alle Arten von USB-Medien am Zielgerät zurück. Er sollte daher nur verwendet werden, wenn das Zielgerät nicht reagiert.

Öffnen von Virtual Media-Sitzungen

So starten Sie eine Virtual Media-Sitzung:

Wählen Sie *Extras – Virtual Media* im Video Viewer-Menü aus. Das Dialogfeld „Virtual Media“ wird angezeigt. Wenn diese Sitzung als reservierte Sitzung festgelegt werden soll, klicken Sie auf *Details* und aktivieren Sie dann das Kontrollkästchen *Reserviert*.

Abbildung 4.4. Video Viewer-Dialogfeld „Virtual Media“



So weisen Sie ein Virtual Media-Laufwerk zu:

1 Öffnen Sie eine Virtual Media-Sitzung, indem Sie in der Video Viewer-Symbolleiste *Extras – Virtual Media* auswählen.

2 So weisen Sie ein physisches Laufwerk als Virtual Media-Laufwerk zu:

   a. Aktivieren Sie im Dialogfeld „Virtual Media“ das Kontrollkästchen *Zugewiesen* neben den Laufwerken, die Sie zuweisen möchten.

b. Wenn für das zugewiesene Laufwerk ein schreibgeschützter Zugriff festgelegt werden soll, aktivieren Sie neben dem Laufwerk das Kontrollkästchen *Schreibgeschützt*. Wenn die Einstellungen der Virtual Media-Sitzung so vorkonfiguriert wurden, dass alle zugewiesenen Laufwerke schreibgeschützt sein müssen, ist dieses Kontrollkästchen bereits aktiviert und kann nicht geändert werden.

   Sie können das Kontrollkästchen *Schreibgeschützt* aktivieren, wenn in den Sitzungseinstellungen Schreib-/Lesezugriff festgelegt wurde, Sie jedoch den Zugriff eines bestimmten Laufwerks auf schreibgeschützt einschränken möchten.

3 So fügen und weisen Sie ein ISO- oder Disk-Image als Virtual Media-Laufwerk hinzu:

a. Klicken Sie im Dialogfeld „Virtual Media“ auf *Image hinzufügen*.

b. Das Dialogfeld zum Auswählen der allgemeinen Datei wird geöffnet, wobei das Verzeichnis mit den Disk-Image-Dateien (Erweiterung .iso oder .img) angezeigt wird. Wählen Sie eine ISO- oder Disk-Image-Datei aus und klicken Sie auf *Öffnen*.

   - oder -

   Wenn das Betriebssystem des Client-Servers Drag & Drop unterstützt, wählen Sie die gewünschte ISO- oder Disk-Image-Datei im Dialogfeld für allgemeine Dateien aus und ziehen Sie diese in das Dialogfeld „Virtual Media“.

c. Der Datei-Header wird überprüft, um sicherzustellen, dass er korrekt ist. Wenn der Datei-Header korrekt ist, wird das Dialogfeld zum Auswählen der allgemeinen Datei geschlossen und die ausgewählte Image-Datei im Dialogfeld „Virtual Media“ geöffnet, wo sie durch Aktivieren des Kontrollkästchens *Zugewiesen* zugewiesen werden kann.

d. Wiederholen Sie Schritte a bis c für alle weiteren ISO- oder Disk-Images, die Sie hinzufügen möchten. Sie können eine beliebige Anzahl von Image-Dateien hinzufügen (bis zu der vom Speicher vorgegebenen

Beschränkung), Sie können jedoch nur ein virtuelles CD- oder DVD-Laufwerk oder ein virtuelles Massenspeichergerät gleichzeitig zuweisen.

Wenn Sie zu viele Laufwerke (ein CD- oder DVD-Laufwerk und ein Massenspeichergerät) oder zu viele Laufwerke eines bestimmten Typs (mehrere CD-/DVD-Laufwerke oder Massenspeichergeräte) zuweisen, wird eine Nachricht angezeigt. Wenn Sie trotzdem ein neues Laufwerk zuweisen möchten, müssen Sie zuerst die Zuweisung eines vorhandenen Laufwerks aufheben. Danach können Sie dann das neue Laufwerk zuweisen.

Nach der Zuweisung eines physikalischen Laufwerks oder Images kann es auf dem Zielgerät verwendet werden.

So heben Sie die Zuweisung eines Virtual Media-Laufwerks auf:

1 Deaktivieren Sie im Dialogfeld „Virtual Media“ das Kontrollkästchen *Zugeordnet* neben den Laufwerken, deren Zuweisung Sie aufheben möchten.

2 Eine Bestätigung ist erforderlich. Bestätigen Sie das Aufheben der Zuweisungen oder brechen Sie den Vorgang ab.

3 Wiederholen Sie diesen Vorgang für zusätzliche Virtual Media-Laufwerke, deren Zuweisung Sie aufheben möchten.

So zeigen Sie Details zu Virtual Media-Laufwerken an:

Klicken Sie im Dialogfeld „Virtual Media“ auf *Details*. Das Dialogfeld wird erweitert und die Details-Tabelle wird eingeblendet. Die Zeilen bedeuten Folgendes:

- Ziellaufwerk – Name für das zugewiesene Laufwerk, wie z. B. Virtual CD 1 oder Virtual CD 2.
- Zugeordnet zu – Identisch zu den Laufwerksinformationen, die in der Spalte „Client-Ansicht des Laufwerks“ angezeigt werden.
- Bytes lesen und Bytes schreiben – Datenmenge, die seit der Zuweisung übertragen wurde.
- Dauer – Zeit, die seit der Zuweisung des Laufwerks verstrichen ist

Klicken Sie zum Schließen der Detailansicht erneut auf *Details*.

So setzen Sie alle USB-Geräte auf dem Zielgerät zurück:

HINWEIS: 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.

1 Klicken Sie im Dialogfeld „Virtual Media“ auf *Details*.

2 Die Detailansicht wird angezeigt. Klicken Sie auf *USB zurücksetzen*.

3 Eine Warnmeldung weist auf die möglichen Auswirkungen des Zurücksetzens hin. Bestätigen Sie den Vorgang oder brechen Sie ihn ab.

4 Klicken Sie zum Schließen der Detailansicht erneut auf *Details*.

Schließen von Virtual Media-Sitzungen

So schließen Sie das Dialogfeld „Virtual Media“:

1 Klicken Sie auf *Beenden*.

2 Wenn Laufwerke zugewiesen wurden, wird eine Nachricht angezeigt, dass die Zuweisung aufgehoben wird. Bestätigen Sie den Vorgang oder brechen Sie ihn ab.

Wenn Sie versuchen, eine Virtual-Media-Sitzung oder eine aktive KVM-Sitzung zu trennen, die über eine zugehörige gesperrte Virtual Media-Sitzung verfügt, werden Sie in einer Bestätigungsnachricht darauf hingewiesen, dass alle Virtual Media-Zuweisungen verloren gehen.

Smart Cards

Sie können ein Smart Card-Lesegerät an einen verfügbaren USB-Port am Client-Server anschließen und auf angeschlossene Zielgeräte im Switch-System zugreifen. Starten Sie dann eine KVM-Sitzung, um den Video Viewer zu öffnen, und weisen Sie eine Smart Card zu.

HINWEIS: Für alle Smart Card-Lesegeräte müssen Sie ein Dell USB2+CAC-SIP oder ein Avocent VMC-IQ-Modul verwenden.

Der Smart Card-Status wird durch ein Smart Card-Symbol auf der äußerst rechten Seite der Video Viewer-Symbolleiste angezeigt. Die folgende Tabelle beschreibt die Smart Card-Statussymbole.

Tabelle 4.4: Smart Card-Symbole

Symbol	Beschreibung
	Es befindet sich keine Smart Card im Lesegerät oder es ist kein Smart Card-Lesegerät angeschlossen.
	Es befindet sich eine Smart Card im Lesegerät, diese wurde jedoch noch nicht zugewiesen.
	Es ist eine Smart Card zugewiesen (grünes Symbol).

So weisen Sie eine Smart Card zu:

1 Öffnen Sie eine KVM-Sitzung, um das Video Viewer-Menü anzuzeigen.

2 Setzen Sie eine Smart Card in das an Ihren Client-Server angeschlossene Smart Card-Lesegerät ein.

3 Wählen Sie im Video Viewer-Menü *Extras – Smart Card zuweisen* aus.

4 Wenn keine Smart Card zum Zielgerät zugewiesen ist, wird dies durch einen Punkt neben der Option „Keine Karte zugewiesen“ angezeigt. Wählen Sie Ihre Smart Card aus, die unter dieser Option angezeigt wird, um die Smart Card zuzuweisen.

Um die Zuweisung einer Smart Card aufzuheben, schließen Sie die KVM-Sitzung, indem Sie im Video Viewer-Fenster auf *X* klicken, *Extras – Keine Karte zugewiesen* auswählen, die Smart Card aus dem Smart Card-Lesegerät entfernen oder das Smart Card-Lesegerät vom Client-Server trennen.

Tastaturanschlag-Weitergabe

Tastenanschläge, die von einem Benutzer eingegeben werden, wenn dieser ein Video Viewer-Fenster verwendet, können je nach eingestelltem Bildschirmmodus des Video Viewers auf zwei verschiedene Arten interpretiert werden.

- Mit dem Video Viewer im Vollbildmodus werden alle Tastenanschläge und Tastenfolgen mit der Ausnahme von *Strg-Alt-Entf* zum angezeigten Remote-Zielgerät gesendet.
- Wenn sich das Video Viewer-Fenster im normalen Desktop-Modus befindet, kann die Tastenanschlag-Weitergabe dazu verwendet werden, zu steuern, ob das Remote-Zielgerät oder der lokale Computer bestimmte Tastenanschläge oder Tastenfolgen erkennt.

Die Tastenanschlag-Weitergabe muss im Dialogfeld „Sitzungsoptionen“ festgelegt werden. Wenn diese Option aktiviert ist, werden alle Tastenanschläge und Tastenfolgen mit der Ausnahme von *Strg-Alt-Entf* bei aktiviertem Video Viewer-Fenster zum angezeigten Remote-Zielgerät gesendet. Wenn der lokale Desktop aktiv ist, beziehen sich alle Tastenanschläge und Tastenfolgen, die durch den Benutzer eingegeben werden, auf den lokalen Computer.

HINWEIS: Die Tastenfolge Strg-Alt-Entf kann nur mittels Makro an das Remote-Zielgerät übertragen werden.

HINWEIS: Die japanische Tastenfolge ALT-Han/Zen wird immer an das Remote-Zielgerät übertragen, unabhängig vom Bildschirmmodus oder den Einstellungen der Tastenanschlag-Weitergabe.

So legen Sie die Tastenanschlag-Weitergabe fest:

1 Wählen Sie im Video Viewer-Menü *Extras – Sitzungsoptionen* aus.

- oder -

Klicken Sie auf die Schaltfläche *Sitzungsoptionen*.

Das Dialogfeld „Sitzungsoptionen“ wird angezeigt.

2 Klicken Sie auf das Register *Allgemein*.

3 Wählen Sie *Alle Tastenanschläge im normalen Fenster-Modus weitergeben*.

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

Makros

Die Switch-OBWI ist mit vorkonfigurierten Makros für Windows, Linux und Sun ausgestattet.

Wählen Sie *Makros – <gewünschtes Makro>* aus dem Video Viewer-Menü aus oder wählen Sie das gewünschte Makro über die Schaltflächen im Video Viewer-Menü aus.

Speichern der Ansicht

Der Bildschirm des Video Viewers kann entweder in eine Datei gespeichert oder in die Zwischenablage kopiert werden und von dort in ein Textverarbeitungs- oder anderes Programm eingefügt werden.

So speichern Sie das Video Viewer-Fenster in einer Datei:

1 Wählen Sie im Video Viewer-Menü *Datei – In Datei speichern*.

- oder -

Klicken Sie auf die Schaltfläche *In Datei speichern*.

Das Dialogfeld „Speichern unter“ wird geöffnet.

2 Geben Sie einen Dateinamen ein und legen Sie einen Speicherort für die Datei fest.

3 Klicken Sie auf *Speichern*, um den Bildschirm in einer Datei zu speichern.

Um das Video Viewer-Fenster in der Zwischenablage zu speichern, wählen Sie *Datei – In Zwischenablage speichern* aus dem Video Viewer-Menü aus oder klicken Sie auf die Schaltfläche *In Zwischenablage speichern*. Die Bilddatei wird in die Zwischenablage kopiert.

Schließen einer Sitzung

So beenden Sie eine Video Viewer-Sitzung:

Wählen Sie im Video Viewer-Menü *Datei – Beenden*.

5

LDAP-Funktion für den RCS

LDAP ist ein Protokollstandard, der den Zugriff auf ein Verzeichnis und dessen Aktualisierung über TCP/IP ermöglicht. Die Dell RCS-Software und OBWI 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: Die Verwendung von Active Directory zur Erkennung von RCS-Benutzern wird von den Betriebssystemen 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. Dell RCSs sind darauf ausgelegt, einen einfachen Domain Tree zu unterstützen, der 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 RCSs ist darauf ausgelegt, diese beiden Aspekte von AD zu unterstützen. DNS wird dazu verwendet, die Netzwerkkoordinaten eines jeden Domänencontrollers zu bestimmen, sodass die Dell RCSs 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 RCSs 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 RCSs ist darauf ausgelegt, sämtliche für AD definierten Schachtelungsregeln 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 wird einer Benutzer-Objektklasse beispielsweise ein Attributtyp namens SAM ACCOUNT NAME und weitere Attribute, wie FIRSTNAME, SURNAME, PASSWORD usw., zugewiesen. Die Produktreihe der Dell Remote Console Switches nutzt die Attribute SAM ACCOUNT NAME und PASSWORD, um einen Benutzer zu authentifizieren (die formellen AD-Namen dieser beiden Attribute lauten sAMAccountName bzw. 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 liefern individuelle Objektklassen zur Repräsentation von Dell RCSs, Zugriffssteuerungsinformationen und einem

speziellen Container, über den spezifische Zugriffssteuerungsinformationen spezifischen Instanzen von Dell RCSs und Benutzern zugewiesen werden können. 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

Darüber hinaus ist die Produktreihe der Dell RCSs auf eine Funktion ausgelegt, für die ausschließlich die Objektklassen verwendet werden, die innerhalb der in AD enthaltenen Klassen vorkommen. Diese Option wird auch als Standardschema bezeichnet. Im Rahmen dieser Option wird die Computer-Objektklasse zur Repräsentation von Dell RCSs genutzt und über die Standard-Gruppenobjekte werden spezifischen Instanzen von Dell RCSs und Benutzern spezifische Zugriffssteuerungsinformationen zugewiesen. 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. DNS wird dazu verwendet, die Netzwerkkoordinaten eines jeden Domänencontrollers zu bestimmen, sodass die Dell RCSs 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 RCSs 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 individuellen RCS 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 RCS ist jedoch kein Computer. Aus diesem Grund können nicht alle Schemafunktionen angewendet werden. Bei der Konfiguration eines RCS, der entsprechend zugewiesen wurde, muss mit besonderer Vorsicht 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 RCS kann mithilfe jedes Schemas gleich gut authentifizieren, und bei keiner dieser Methoden ist mit Funktionalitätseinbußen zu rechnen. 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

Bevor ein Dell RCS Active Directory zur Authentifizierung nutzen kann, führen Sie folgende Schritte aus:

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

1 Klicken Sie auf *Benutzerkonten* und dann auf *Admin umgehen*.

2 Geben Sie den Benutzernamen und das Kennwort für den Benutzer ein und bestätigen Sie das Kennwort, indem Sie es im Feld „Kennwort bestätigen“ noch einmal eingeben.

3 Klicken Sie auf **Speichern**.

HINWEIS: Für diese Option müssen Sie als Administrator angemeldet sein.

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 RCS an und ermöglicht die Änderung von Netzwerkeinstellungen wie IP-Adresse, Subnetzmaske, Gateway, LAN-Geschwindigkeit und DHCP/BootP-Einstellung. Der für den RCS angezeigte Name entspricht dem im Feld „Systemname“ innerhalb der SNMP-Kategorie angegebenen Namen.

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. Jedes Mal wenn ein primärer Server nicht verfügbar ist, führt die RCS-Software automatisch ein Backup der DNS-Server durch, wie hier angegeben.

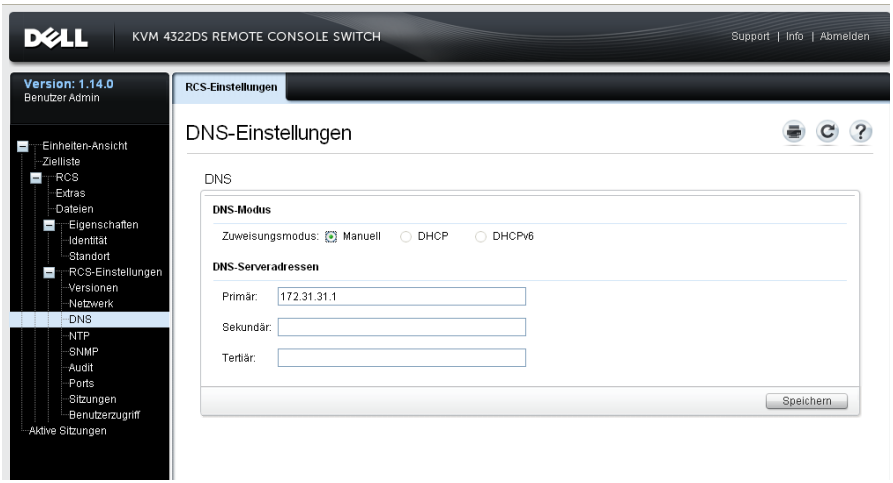
HINWEIS: Sie können die DNS-Serveradressen auch über die serielle Verwaltungsoberfläche des RCS einrichten. Weitere Informationen zur Verwendung der seriellen Verwaltungsschnittstelle finden Sie in der Produktdokumentation zu Ihrem RCS.

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

1 Klicken Sie auf *DNS*, um den Bildschirm „DNS-Einstellungen“ zu öffnen.

2 Geben Sie den DNS-Modus an und geben Sie die Serveradresse an. Klicken Sie danach auf **Speichern**.

Abbildung 5.1. OBWI - DNS-Einstellungen



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 über das NTP abgefragt wird. So konfigurieren Sie die NTP-Einstellungen über die integrierte Weboberfläche:

1 Klicken Sie auf *NTP*, um den Bildschirm „NTP“ zu öffnen.

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. Ist das Intervall auf 0 eingestellt, werden Abfragen nur während des RCS-Starts durchgeführt oder wenn Änderungen im Menü Global – NTP vorgenommen werden.

4 Klicken Sie auf **Speichern**.

Konfigurieren der LDAP-Authentifizierungsparameter

Die Authentifizierungsanzeige gestattet RCS-Administratoren die Konfiguration der Parameter, die für den Zugriff auf die LDAP-Verzeichnisdienste erforderlich sind. Wenn Zugriffsanfragen von Benutzern eingehen, können die RCSs LDAP-Protokolle verwenden, um den Benutzernamen, das Kennwort sowie weitere Informationen an die Verzeichnisdienste zu senden, um die Autorisierungsberechtigungen für diesen Benutzer zu ermitteln.

HINWEIS: Die Berechtigungsstufen zum Einrichten einer LDAP-Konfiguration sind „KVM-Benutzer“, „KVM-Benutzeradministrator“ und „KVM-Einheitenadministrator“. Diese Berechtigungsstufen gelten entsprechend für Benutzer, Benutzeradministratoren und RCS-Administratoren. Die Zugriffsebenen haben sich nicht geändert. Verwenden Sie dennoch die neuen Berechtigungsstufen.

LDAP-Authentifizierung aktivieren

Der Bereich „Betriebsmodi“ auf dem Bildschirm „LDAP-Konfigurationsoptionen“ ermöglicht Ihnen die Wahl des geeigneten LDAP-Dienstes, der zur Benutzerauthentifizierung verwendet werden soll. Folgende Modi stehen zur Verfügung:

- Standardmäßige LDAP-Verzeichnisdienste (nicht von Microsoft)
- Microsoft Active Directory-Dienste
- LDAP-Authentifizierung deaktivieren

Falls bereits eine andere Authentifizierungsmethode als LDAP ausgewählt wurde, wird die LDAP-Authentifizierung automatisch deaktiviert. Diese Methode muss deaktiviert werden, um LDAP-Verzeichnisdienste verwenden zu können.

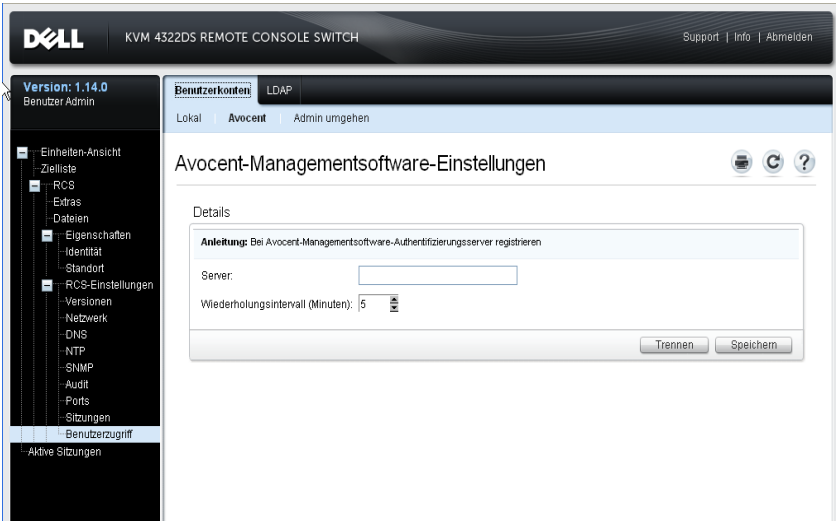
Die Möglichkeit zur Verwendung der LDAP-Authentifizierung wiederherstellen.

1 Wählen Sie unter „Benutzerzugriff“ das Register *Avocent* (siehe Abbildung 5.2).

2 Klicken Sie auf *Trennen*, um die Verwendung des Avocent Management-Authentifizierungsservers zu beenden.

3 Klicken Sie auf *Speichern*.

Abbildung 5.2. Der Bildschirm „Avocent Authentifizierung“

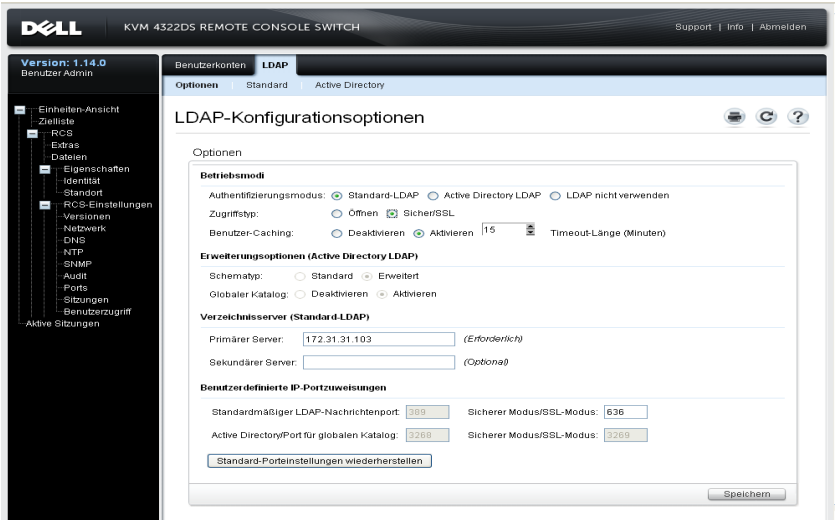


HINWEIS: Es ist möglich, die Avocent Authentifizierungszuweisung extern zu trennen, ohne diese Schritte durchzuführen. Falls eine Avocent Serverzuweisung zur Benutzerauthentifizierung erstellt wurde, muss diese dennoch ausdrücklich mit diesem Verfahren entfernt werden, damit die Konfiguration der LDAP-Authentifizierung fortgesetzt werden kann.

So aktivieren Sie die LDAP-Authentifizierung:

1 Wählen Sie unter „Benutzerzugriff“ das Register „LDAP“ (siehe Abbildung 5.3).

Abbildung 5.3. Der Bildschirm „LDAP-Konfigurationsoptionen“



2 Wählen Sie im Bereich „Betriebsmodi“ einen der verfügbaren LDAP-Authentifizierungsmodi aus.

3 Es müssen alle Konfigurationsoptionen eingestellt sein, um die LDAP-Authentifizierung vollständig zu aktivieren. In diesem Kapitel werden alle Funktionen detailliert beschrieben.

4 Klicken Sie auf *Speichern*.

Aktivieren Sie das Kontrollkästchen *LDAP nicht verwenden* und klicken Sie auf *Speichern*, um die LDAP-Authentifizierung zu deaktivieren. Alle anderen Optionen auf dem Bildschirm werden deaktiviert und eine Bearbeitung dieser weiteren Felder ist nicht möglich. Außerdem werden die zusätzlichen Konfigurationsbildschirme auf den Registern „Standard“ und „Active Directory“ ebenfalls deaktiviert.

Wenn die LDAP-Authentifizierung deaktiviert ist, wird der Benutzerzugriff entweder durch lokal definierte Zugriffslisten oder die Avocent Managementsoftware geregelt (siehe den Abschnitt zum Benutzerzugriff).

Wenn die LDAP-Authentifizierung aktiviert ist, haben lokal definierte Zugriffslisten Vorrang vor Anfragen an LDAP-Verzeichnisserver. Benutzerzugriffsanfragen, die zuerst auf über den RCS definierte Benutzer überprüft werden. Wenn keine Übereinstimmung gefunden wird, werden Anfragen gemäß Konfiguration an die LDAP-Verzeichnisserver gesendet.

Authentifizierungsparameter eingeben - Betriebsmodi

Zugriffsart

LDAP-Verzeichnisserver können so eingerichtet werden, dass sie entweder im offenen oder im sicheren Modus (mit SSL - Secure Socket Layer-Verschlüsselung) arbeiten. Der ausgewählte Modus muss mit dem des Host-Verzeichnisservers übereinstimmen. Bei Auswahl des Modus „Sicher/SSL“ lesen Sie bitte außerdem den Abschnitt „SSL-Zertifikate für LDAP“ zu den Anforderungen für den verschlüsselten Betrieb.

Zwischenspeichern

Bei jedem Abschluss einer erfolgreichen Benutzerauthentifizierung über LDAP kann der RCS die vom LDAP-Verzeichnisserver erhaltenen Ergebnisse für eine bestimmte Zeit speichern. Wenn in diesem Zeitfenster eine weitere Zugriffsanfrage generiert wird, die normalerweise erneut zu einer Anfrage beim Verzeichnisserver führen würde, werden solche Anfragen lokal vom RCS erledigt. Dies ermöglicht eine fast umgehende Antwort, die dem Benutzer das Weiterarbeiten mit minimalen Verzögerungen ermöglicht.

Die drei für diese Konfiguration möglichen Einstellungen sind „Aktivieren“, „Deaktivieren“ und „Timeout-Länge“.

Deaktivieren: Eine Zwischenspeicherung ist nicht zulässig. Vom LDAP-Verzeichnisserver müssen für jeden Benutzer und immer, wenn es erforderlich ist, Informationen zum Authentifizierungsstatus eingeholt werden. Die Standardeinstellung ist „deaktiviert“.

Aktivieren: Die vom LDAP-Verzeichnisserver ermittelten Ergebnisse der letzten Anfrage zur Benutzerautorisierung werden gespeichert. Wenn innerhalb einer

zuvor festgelegten Zeitspanne identische Autorisierungsanfragen eingehen, werden diese vorherigen Ergebnisse für die neue Anfrage verwendet.

Timeout-Länge: Diese Option legt die Länge des Zeitfensters fest. Werte werden in Minuten angegeben. Sie können die entsprechende Zahl in das Feld eingeben oder die Pfeilsteuerelemente verwenden.

- Timeout-Standardwert: 15 Minuten
- Timeout minimal: 1 Minute
- Timeout maximal: 1.000 Minuten

HINWEIS: Wie bei allen Konfigurationsaktualisierungen müssen Sie auf *Speichern* klicken, um die Änderungen zu übernehmen. Änderungen an der LDAP-Konfiguration sind im RCS im Allgemeinen sofort verfügbar, ohne einen Neustart durchführen zu müssen.

Erweiterungsoptionen eingeben - Active Directory LDAP

Wenn der Modus „Active Directory“ ausgewählt wird, muss der Administrator festlegen, ob das Standardschema oder das erweiterte Schema verwendet wird. Des Weiteren sollte der Administrator angeben, ob der globale Katalog von Microsoft verwendet wird.

Authentifizierungsparameter eingeben - Standard LDAP

Bei Verwendung des Standard-LDAP (nicht des Microsoft Active Directory-LDAP) ist die direkte Eingabe von mindestens einer relevanten Verzeichnisserveradresse erforderlich. Geben Sie die Adressen in die Felder „Primärer Server“ und „Sekundärer Server“ ein. Der Eintrag für den primären Server ist zwingend erforderlich.

Serveradressen können in einem der folgenden Formate eingegeben werden:

- DNS-Adresse (Beispiel: myldapserver.com)
- IPv4-Adresse (Beispiel: 10.20.255.255)
- IPv6-Adresse (Beispiel: fe80::200:f8af:fe20:76ce)

Authentifizierungsparameter eingeben - Benutzerdefinierte IP-Portzuweisungen

Dieser Bereich ermöglicht Änderungen an den gemäß Industrienorm üblicherweise für das LDAP verwendeten IP-Portnummern. In den meisten Fällen müssen diese Werte nicht geändert werden. Wenn der Administrator des von Ihnen verwendeten LDAP-Verzeichnisservers jedoch andere Portzuweisungen verwendet, können diese hier eingegeben werden.

Abhängig von der exakten Konfiguration kann das LDAP bis zu vier verschiedene IP-Ports nutzen, wobei immer zwei gleichzeitig verwendet werden können. Slots für jeden dieser vier Ports sind im Bildschirm „LDAP-Konfigurationsoptionen“ zu sehen. Andere Einstellungen im selben Bildschirm werden verwendet, um die Ports zu kennzeichnen, die geändert werden können. Das folgende Diagramm definiert Bedingungen, unter denen die verfügbaren Port-Slots aktiviert sind und geändert werden können.

Tabelle 5.1: IP-Portzuweisungen bearbeiten

Liste mit Port-Slots, die aktiviert sind und angepasst werden können	Offener Modus	Sicherer Modus/SSL-Modus
Globaler Katalog wird nicht verwendet	Standardmäßiger LDAP-Nachrichtenport	Standardmäßiger LDAP-Nachrichtenport - Modus „Sicher/SSL“
Globaler Katalog wird verwendet	Standardmäßiger LDAP-Nachrichtenport und Active Directory/Port für globalen Katalog	Standardmäßiger LDAP-Nachrichtenport - Modus „Sicher/SSL“ und Active Directory/Port für globalen Katalog - Modus „Sicher/SSL“

Wenn die ursprünglichen IP-Portzuweisungen gemäß Industrienorm wieder hergestellt werden müssen, klicken Sie einfach auf „Standard-Porteinstellungen

wiederherstellen“. Die Werte für alle vier Ports werden daraufhin wieder auf die ursprünglichen Werte zurückgesetzt. Diese lauten:

Standardmäßiger LDAP-Nachrichtenport - 389

Standardmäßiger LDAP-Nachrichtenport über SSL - 636

Active Directory über globalen Katalogserver - 3268

Active Directory über globalen Katalogserver/SSL - 3269

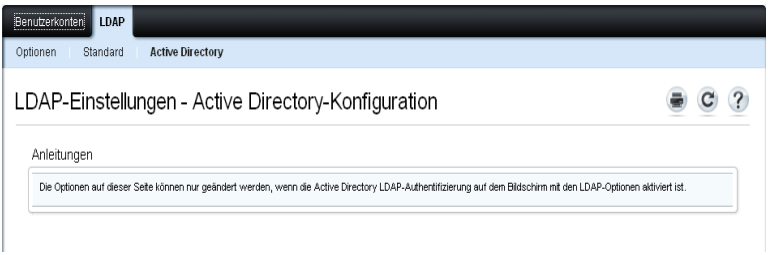
IP-Portnummern können im Bereich von 1 bis 65535 liegen. Wenn die Portnummern nicht mit den vom LDAP-Verzeichnisserver verwendeten Portnummern übereinstimmen, ist eine Kommunikation mit diesem Server nicht möglich

Fertigstellen der LDAP-Konfiguration

Sowohl für den Modus „Standard LDAP“ als auch für den Modus „Active Directory LDAP“ sind zusätzliche Parameter erforderlich, um die einwandfreie Konnektivität zu den LDAP-Verzeichnisservern sicherstellen zu können. Im folgenden Abschnitt werden diese Parameter erklärt. Sie sollten sich jedoch darüber im Klaren sein, dass auf den Seiten der OBWI „Sperren“ eingerichtet sind, die den Administrator bei seiner Arbeit unterstützen, indem sie dafür sorgen, dass Parameteraktualisierungen stets auf der richtigen Seite vorgenommen werden.

Wenn Sie beispielswiese das Register „Active Directory LDAP“ auswählen, sehen Sie auf Ihrem Bildschirm eventuell folgende Anzeige (siehe Abbildung 5.4).

Abbildung 5.4. Benachrichtigung - LDAP-Modus nicht aktiviert



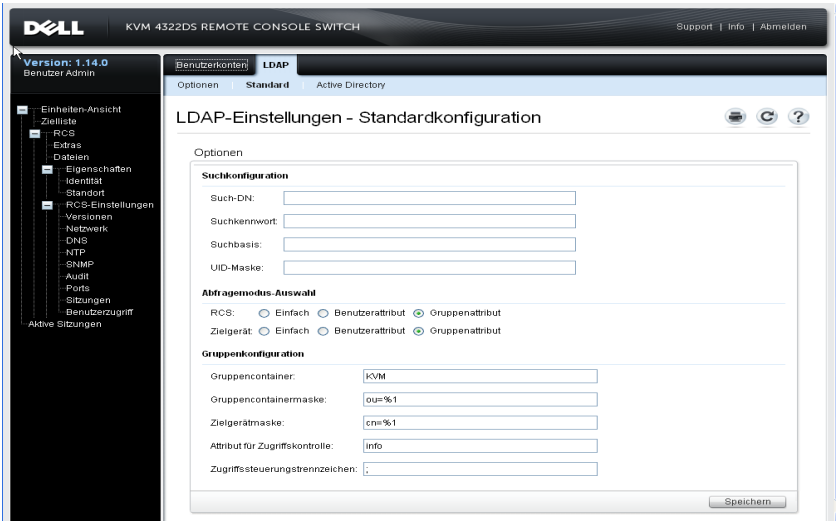
Falls das geschieht, ist das ein Anzeichen dafür, dass der Active Directory-Modus nicht aktiviert wurde oder dass er zwar aktiviert, aber nicht gespeichert wurde. Sie sollten erneut den Bildschirm mit den LDAP-Optionen aufrufen, dort *Active Directory LDAP* auswählen, sich die auf dieser Seite angegebenen sekundären Parameter für diesen Modus notieren und anschließend auf *Speichern* klicken, bevor Sie wieder diesen Bildschirm aufrufen.

Für den Modus „Standard LDAP“ gibt es eine entsprechende Anzeige, die immer dann angezeigt wird, wenn dieser Modus nicht aktiviert ist.

Sekundäre LDAP-Einstellungen - Standardkonfiguration

Wie für LDAP Active Directory-Konfigurationen auch werden die Parameter für die Standard LDAP-Authentifizierung, für die Suche und für Abfragen über die Remote-OBWI konfiguriert. Die Einstellungen in diesem Abschnitt werden über die Register „Benutzerzugriff“, „LDAP“ und „Standard“ im OBWI-Fenster aufgerufen (siehe Abbildung 5.5).

Abbildung 5.5. Sekundäre LDAP-Einstellungen - Standardkonfiguration



HINWEIS: Obwohl in diesem Abschnitt die Parameter für das Einrichten von Verbindungen zu standardmäßigen LDAP-Verzeichnisservern beschrieben werden, kann dieser Abschnitt auch verwendet werden, um Verbindungen zu generischeren Versionen von Active Directory-Diensten herzustellen.

Den RCS für das Durchführen von LDSP-Standardabfragen einrichten

HINWEIS: Bevor Sie die Abfragemodi mit Active Directory verwenden können, müssen Sie zunächst Änderungen am Active Directory vornehmen, damit der ausgewählte Abfragemodus die entsprechende Autorisierungsebene für den Benutzer zuordnen kann.

So stellen Sie Gruppenabfragen ein:

1 Melden Sie sich mit Administratorberechtigungen bei der Software Ihres LDAP-Verzeichnisservers an.

2 Erstellen Sie eine Organisationseinheit (OU), die als Gruppencontainer verwendet werden soll.

3 Zum Abfragen von Einheiten erstellen Sie ein Computerobjekt in Active Directory, dessen Name mit dem Switching-System identisch ist, oder dessen Name mit den verbundenen Zielgeräten identisch ist, um Zielgeräte abzufragen. Die Namen müssen genau übereinstimmen und die Groß- und Kleinschreibung muss beachtet werden.

4 Die Einheiten- und Zielgerätenamen für die Gruppenabfragen sind in der Einheit gespeichert. Der im Bildschirm „Einheit-Übersicht“ der Remote-OBWI angegebene Gerätename und die Namen der Zielgeräte müssen aus einer beliebigen Kombination von Groß- und Kleinbuchstaben, Zahlen und Bindestrichen bestehen und sie müssen den Objektnamen auf dem LDAP-Server entsprechen.

5 Es können mehrere Gruppen unter einer Gruppencontainer-Organisationseinheit erstellt werden.

6 Fügen Sie den in Schritt vier (4) erstellten Gruppen die Benutzernamen sowie die Zielgeräte- und Einheitenobjekte hinzu.

7 Geben Sie den Wert eines Attributs an, das zur Implementierung des Attributs für die Zugriffskontrolle verwendet wird.

Konfigurationseinstellungen für die Suche

Für erfolgreiche LDAP-Verbindungen sind vier Einstellungen erforderlich. Diese Einstellungen sind Such-DN, Suchkennwort, Suchbasis und UID-Maske.

Such-DN

Über das Feld „Such-DN“ können Sie einen Benutzer auf Administratorebene festlegen, unter dem sich die Einheit beim Verzeichnisdienst anmeldet. Nachdem das Zielgerät authentifiziert wurde, gewährt ihm der Verzeichnisdienst Zugriff auf das Verzeichnis, um die auf der LDAP-Abfrageseite angegebenen Abfragen zur Benutzerauthentifizierung durchzuführen. Die Suchwerte müssen durch Kommata voneinander getrennt werden. Ein typischer Eintrag kann wie folgt aussehen:

```
cn=Administrator,cn=Users,dc=MyDomainName,dc=com
```

Suchkennwort

Ein Suchkennwort wird verwendet, wenn für Suchoptionen ein Kennwort erforderlich ist. Dieses Kennwort authentifiziert den im Feld „Such-DN“ angegebenen Administrator oder Benutzer. Alle druckbaren ASCII-Zeichen sind zulässig.

Suchbasis

Im Feld „Suchbasis“ wird ein Anfangspunkt für die LDAP-Suche angegeben. Die Standardwerte sind dc=yourDomainName und dc=com. Die einzelnen Suchkomponenten müssen durch Kommata voneinander getrennt werden. Wenn zum Beispiel die Suchbasis auf test.com eingestellt werden soll, geben Sie dc=test, dc=com ein.

UID-Maske

Das Feld „UID-Maske“ gibt die Suchkriterien für die Benutzer-ID-Suche auf LDAP-Zielgeräten an. Das Format lautet <name>=<%1>. Der Standardwert ist sAMAccountName=%1. Dieser Wert entspricht dem Standard für Microsoft Active Directory-Dienste.

Abfragemodus-Auswahleinstellungen

Konfigurieren Sie die Parameter für den Abfragemodus für die Einheit und das Zielgerät. Die Einheit wird zur Authentifizierung von Administratoren und Benutzern verwendet, die auf den Console Switch selbst zugreifen. Das Zielgerät wird zur Authentifizierung von Benutzern verwendet, die versuchen, auf angeschlossene Zielgeräte zuzugreifen.

Es stehen drei Abfragemodi zur Verfügung. Diese Modi sind „Einfach“, „Benutzerattribut“ und „Gruppenattribut“.

Einfach

Ein Abfrage des Benutzernamens und des Kennworts wird an den Verzeichnisdienst gesendet. Nach der Authentifizierung als gültiger Benutzer erhält dieser Zugriff auf die Einheit und alle verbundenen Zielgeräte.

Benutzerattribut

Ein Abfrage des Benutzernamens, des Kennworts und des Attributs für die Zugriffskontrolle wird an den Verzeichnisdienst gesendet. Das Attribut für die Zugriffskontrolle wird aus dem Benutzerobjekt im Active Directory gelesen. Falls keine Werte gefunden werden, erhält der Benutzer keinen Zugriff auf die Einheit oder die Zielgeräte.

Gruppenattribut

Im Abfragemodus (Einheit) wird eine Abfrage des Benutzernamens, des Kennworts und der Gruppe für eine Einheit und die verbundenen Zielgeräte an den Verzeichnisdienst gesendet. Im Abfragemodus (Gerät) wird diese Abfrage für das ausgewählte Zielgerät durchgeführt. Wenn eine Gruppe gefunden wird, welche die Namen des Benutzers und der Einheit enthält, wird dem Benutzer im Abfragemodus (Einheit) der Zugriff auf die Einheit oder die verbundenen Zielgeräte gewährt. Wenn eine Gruppe gefunden wird, welche die IDs des Benutzers und des Zielgeräts enthält, wird dem Benutzer im Abfragemodus (Gerät) der Zugriff auf das ausgewählte Zielgerät gewährt.

HINWEIS: Abhängig vom ausgewählten Abfragemodus sind einige der Konfigurationsobjekte auf diesem Bildschirm je nach ihrer Anwendbarkeit aktiviert bzw. deaktiviert.

Gruppenkonfiguration

Es stehen verschiedene Gruppenkonfigurationsparameter zur Verfügung.

Gruppencontainer

Der Gruppen-Container gibt die OU an, die vom Administrator als Speicherort für Gruppenobjekte im Active Directory erstellt wurde. Gruppenobjekte können Benutzer, Computer, Kontakte sowie weitere Gruppen enthalten, von denen jeder eine bestimmte Zugriffsebene zugewiesen ist.

Maske des Gruppen-Containers

Die Gruppen-Containermaske definiert den Objekttyp des Gruppen-Containers (üblicherweise ein OU-Container). Der Standardwert ist ou=%1.

Maske des Zielgeräts

Die Maske des Zielgeräts legt einen Suchfilter für das Zielgerät fest. Der Standardwert ist cn=%1.

Attribut für Zugriffskontrolle

Das Attribut für die Zugriffskontrolle legt den Namen des Attributs fest, das verwendet wird, wenn die Abfragemodi auf „Benutzerattribut“ oder „Gruppenattribut“ eingestellt sind. Der Standardname für das Attribut lautet **„info“**.

Trennzeichen für die Zugriffskontrolle

Die LDAP-Standards legen fest, dass der Strichpunkt (;) verwendet wird, um mehrere Eigenschaften in einem einzelnen benannten Attribut voneinander zu trennen. Unter normalen Umständen ist hier keine Änderung erforderlich. Nehmen wir beispielsweise an, dass im LDAP-Verzeichnis ein Marker für eine Trockenlöschtafel vorhanden ist und das Attribut „Color“ verwendet wird, um mögliche Farben dieses Markers zu identifizieren.

Color: red;blue;green;black;purple

„Color“ ist der Name des Attributs. Der Rest stellt den Wert des Attributs dar (hier ein zusammengesetzter Wert). Bei zusammengesetzten Werten kennzeichnet der Strichpunkt das Ende der einen Komponente und den Anfang der nächsten.

In seltenen Fällen wird der Strichpunkt von einem LDAP-Administrator eventuell als Teil des Werts selbst verwendet. Wenn das der Fall ist, muss ein anderes Trennzeichen als der Strichpunkt verwendet werden. Verwenden Sie hierfür dieses Feld, um alle Zeichen anzugeben (mindestens ein Zeichen; mehrere sind möglich), die angeben sollen, wie das Attribut für die Zugriffskontrolle unterteilt werden soll. Beispielsweise können Sie **#$;** (drei Zeichen) in das Feld für das Trennzeichen eingeben.

Color: red#blue$green;black#purple

Mit diesen Trennzeichen finden Sie dieselben fünf Wertkomponenten wie im ersten Beispiel oben. LDAP-Administratoren sollten sicherstellen, dass die als Trennzeichen für die Zugriffskontrolle definierten Zeichen nirgends sonst als Wert für ein Attribut und ausschließlich in der Funktion als Trennzeichen verwendet werden.

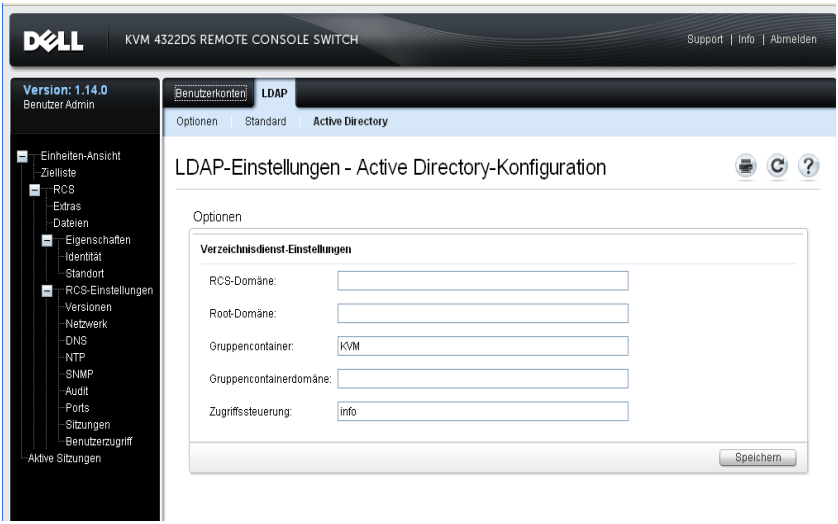
Wie oben gezeigt besteht das Attribut für die Zugriffskontrolle (ACA; Access Control Attribute) aus der Kombination eines Namens und eines Werts. Standardmäßig suchen wir nach LDAP-Verzeichniseinträgen, die dem Benutzer und dem Zielgerät entsprechen, indem wir nach Attributen mit der Bezeichnung „info“ suchen. Der Wert solcher Attribute sollte uns Auskunft über die Autorisierungsebene des Benutzers für dieses Gerät geben. Wenn der Administrator der LDAP-Dienste ein anderes Attribut als „info“ verwenden möchte, kann er über das oben angegebene Feld die entsprechende Anpassung vornehmen.

Da Benutzer mehreren Gruppen angehören können und jede Gruppe über unterschiedliche Autorisierungsebenen für verschiedene Geräte verfügen kann, werden die Ergebnisse laufend festgehalten. Gemäß LDAP-Standards handelt es sich bei der zuletzt gemeldeten Autorisierungsebene um die höchste Ebene (mit den meisten Berechtigungen) unter allen positiven Ergebnissen für den jeweiligen Benutzer und das Gerät, die einer Überprüfung unterzogen werden.

Sekundäre LDAP-Einstellungen - Active Directory-Konfiguration

Die Einstellungen in diesem Abschnitt werden über die Register „Benutzerzugriff“, „LDAP“ und „Standard“ im OBWI-Fenster aufgerufen (siehe Abbildung 5.6).

Abbildung 5.6. Sekundäre LDAP-Einstellungen - Active Directory-Konfiguration



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 RCSs sowie 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 OBWI-Fenster eingeben.

Eine detaillierte Beschreibung der in Abbildung 5.6 gezeigten Felder finden Sie in Tabelle 5.2.

Tabelle 5.2: Beschreibung der Felder in der Active Directory-Konfiguration

Feld	Beschreibung
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.

Feld	Beschreibung
Gruppen-Container (nur Standardschema-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, In diesem Fall sollte für das Feld „Gruppen-Container“ die Option „KVM-AccessControls“ ausgewählt werden. Der in das Feld „Gruppen-Container“ eingegebene Name muss unter allen OU-Objekten in der Domain des Gruppen-Containers 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 Standardschema-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.

Feld	Beschreibung
Attribut für Zugriffskontrolle (nur Standardschema-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 die Zugriffskontrolle wird aus den Attributen in dem LDAP-Verzeichnisobjekt ausgewählt, das die Gruppe repräsentiert, deren Mitgliederliste sowohl den Benutzer als auch den RCS bzw. den angeschlossenen Computer enthält, auf 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

Alle LDAP-Protokollaustausche (zwischen einem RCS und Active Directory-Servern) sind 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 RCS veranlasst. Nach Eingang überprüft der RCS das Zertifikat. Um das Zertifikat überprüfen zu können, muss dem RCS eine Kopie des Root-

Zertifikats der Zertifikatsautorität (CA) zur Verfügung gestellt 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.

HINWEIS: Wenn in den nachstehenden Anweisungen Text in <anglebrackets> 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 drücken 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 ist 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.

Ländername (2-Buchstaben-Code) [GB]:<US>

Bundesland oder Provinz (vollständiger Name) [Berkshire]:<Texas>

Örtlichkeit (z. B. Stadt) [Newbury]:<Austin>

Organisation (z. B. Unternehmen) [Mein Unternehmen Ltd]:<Dell, Inc.>

Einheit der Organisation (z. B. Abteilung) []:<Round Rock>

Allgemeiner Name (z. B. Ihr Name oder der Hostname Ihres Servers) []:<RCS

DNS Name or IP>

E-Mail-Adresse []:<support@dell.com>

OpenSSL> quit

3 Geben Sie an der Linux-Eingabeaufforderung **cat certificate.pem privatekey.pem > webserver.pem** ein und konvertieren Sie die Datei dann vom UNIX-Zeilenvorschub in den DOS-Zeilenumbruch/-Zeilenvorschub, indem Sie **unix2dos webserver.pem** eingeben.

So exportieren Sie das CA-Zertifikat:

1 Um das Managementtool der Zertifikatsautorität über das Windows-Betriebssystem zu öffnen, klicken Sie auf **Start – Programme – Verwaltung – Zertifikatsautorität**.

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 am Bildschirm „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**.

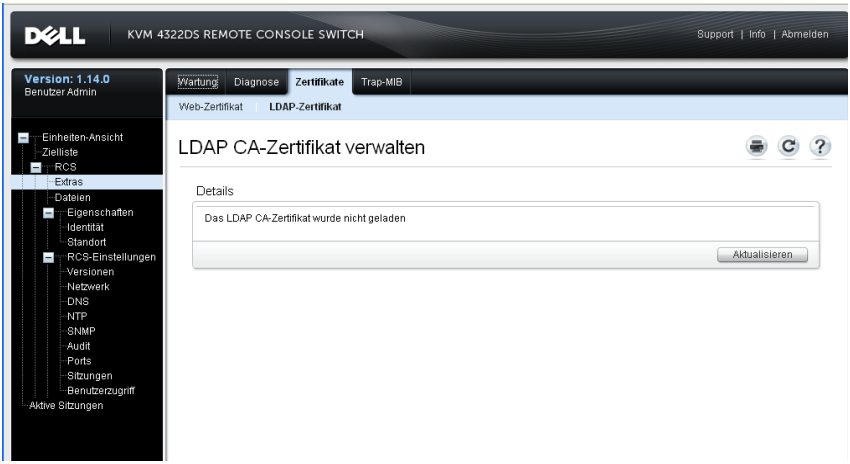
Die aus diesem Vorgang resultierende Zertifikatsdatei ist ordnungsgemäß formatiert und kann von OpenSSL gelesen werden.

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.

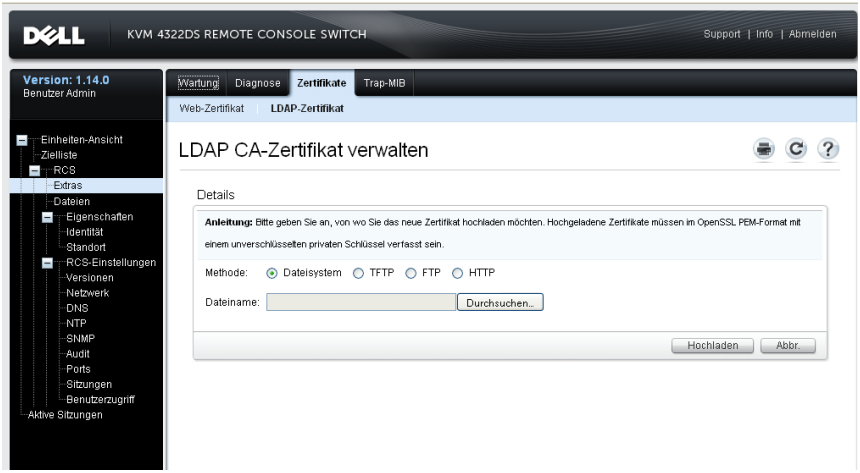
HINWEIS: Das Network Time Protocol (NTP) muss aktiviert sein, damit LDAPS funktionieren kann.

Abbildung 5.7. OBWI – LDAP-Zertifikat



Nach dem Klicken auf „Aktualisieren“ wird der folgende Bildschirm angezeigt:

Abbildung 5.8. OBWI – LDAP-Zertifikat aktualisieren



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 den RCS senden.

Anmeldungs-Timeout

Falls eine derart umfangreiche Verzeichnisstruktur vorhanden ist, dass die LDAP-Authentifizierung nur langsam durchgeführt werden kann, stellt das Fenster „Sitzungen“ eine Anmeldungs-Timeout-Funktion mit einem Standard-Timeout von 30 Sekunden zur Verfügung. Das Anmeldungs-Timeout ist der Zeitraum zwischen dem Betätigen des Schaltfläche **OK** im Anmeldedialogfenster durch den Benutzer und dem Zeitpunkt, bis zu dem der RCS reagiert haben muss. Der RCS verwendet diesen Wert außerdem dazu, das Timeout für eine LDAP-Authentifizierungsanforderung zu bestimmen.

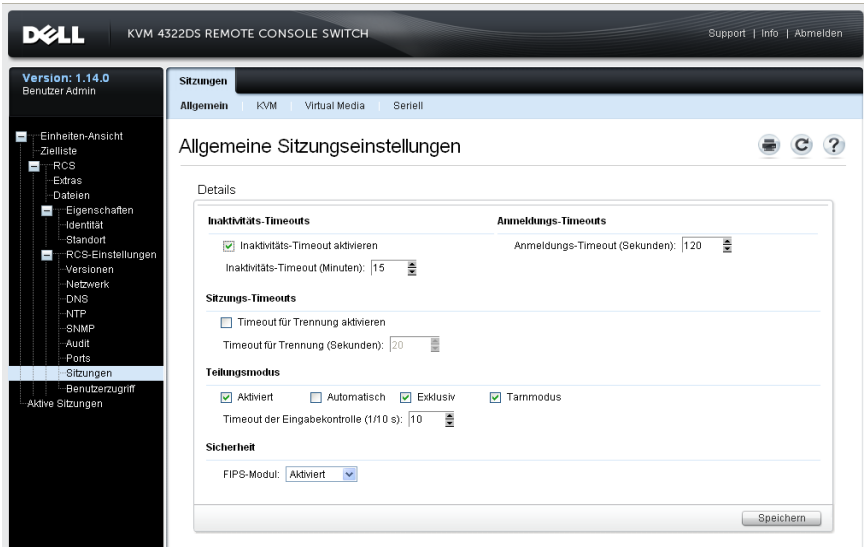
So legen Sie das Anmeldungs-Timeout über die integrierte Weboberfläche fest:

1 Klicken Sie auf **Sitzungen**, um die Bildschirmanzeige „Allgemeine Sitzungseinstellungen“ aufzurufen.

2 Geben Sie die Anzahl von Sekunden im Menü „Anmeldungs-Timeout“ ein.

3 Klicken Sie auf **Speichern**.

Abbildung 5.9. OBWI – Anmeldungs-Timeout



HINWEIS: Der Anmeldungs-Timeout unterscheidet sich von der Zwischenspeicherungsfunktion für die Benutzeranmeldung. Letztere greift nach einer abgeschlossenen Anmeldung, indem das Autorisierungsergebnis für einen gewissen Zeitraum zwischengespeichert wird. Auf diese Weise werden wiederholte LDAP-Kommunikationsanfragen vermieden.

Anzeigen von CA-Zertifikatsinformationen

Die RCS-Software kann nur vollständige CA-Zertifikatsinformationen in diesem Fenster anzeigen, wenn der öffentliche Schlüssel kleiner oder gleich 2048 Bits ist. Wenn der Schlüssel mehr als 2048 Bit umfasst, werden die Daten zu Betreff, Aussteller und Gültigkeitsdauer unvollständig dargestellt.[1]

Die folgende Anzeige ist ein Beispiel für CA-Zertifikatsinformationen:

1 Laden Sie das CA-Zertifikat vom Client auf den RCS.

2 Geben Sie im Hauptmenü der seriellen Konsole **Option** 8 ein, um das LDAP CA-Zertifikat anzuzeigen.

Der RCS 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 **Startmenü**.

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: In aufsteigender Reihenfolge sind dies „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 5.3: Zulässige Aktionen nach jeweiliger Zugriffsstufe

Vorgang	KVM-Einheiten-administrator	KVM-Benutzer-administrator	KVM-Benutzer
Trennen	Darf einen anderen KVM-Einheitenadministrator oder einen KVM-Benutzeradministrator 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
Netzwerkparameter und globale Einstellungen konfigurieren	Ja. – Die Berechtigung muss für jeden RCS konfiguriert werden, indem der RCS in das entsprechende Gruppenobjekt im Verzeichnis aufgenommen wird.	Nein	Nein

Vorgang	KVM-Einheiten-administrator	KVM-Benutzer-administrator	KVM-Benutzer
Neustart durchführen	Ja. – Die Berechtigung muss für jede RCS konfiguriert werden, indem der RCS in das entsprechende Gruppenobjekt im Verzeichnis aufgenommen wird.	Nein	Nein
FLASH-Aktualisierung	Ja. – Die Berechtigung muss für jeden RCS konfiguriert werden, indem der RCS in das entsprechende Gruppenobjekt im Verzeichnis aufgenommen wird.	Nein	Nein
Benutzerkonten verwalten	Ja. – Die Berechtigung muss für jeden RCS konfiguriert werden, indem der RCS in das entsprechende Gruppenobjekt im Verzeichnis aufgenommen wird.	Ja. – Die Berechtigung muss für jeden RCS konfiguriert werden, indem der RCS in das entsprechende Gruppenobjekt im Verzeichnis aufgenommen wird.	Nein

Vorgang	KVM-Einheiten-administrator	KVM-Benutzer-administrator	KVM-Benutzer
Port-Einstellungen konfigurieren	Ja. – Die Berechtigung muss für jeden RCS konfiguriert werden, indem der RCS in das entsprechende Gruppenobjekt im Verzeichnis aufgenommen wird.	Nein	Nein
Auf Zielgerät zugreifen	Ja. – Die Berechtigung muss für jeden RCS konfiguriert werden, indem der RCS in das entsprechende Gruppenobjekt im Verzeichnis aufgenommen wird.	Ja. – Die Berechtigung muss für jeden RCS konfiguriert werden, indem der RCS in das entsprechende Gruppenobjekt im Verzeichnis aufgenommen wird.	Ja, wenn vom Administrator entsprechend konfiguriert. Die Berechtigung muss für jedes Zielgerät (Target Device, TD) konfiguriert werden, indem das TD in das entsprechende Gruppenobjekt im Verzeichnis aufgenommen wird.

Ein AD-Benutzerkonto muss entsprechend konfiguriert werden, um die Berechtigung vom RCS-Administrator (KVM-Einheitenadministrator) zu erhalten, Felder in der Authentifizierungsanzeige zu ändern. Insbesondere die Authentifizierungseinstellungen dürfen nur von einem RCS-Administrator 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 Berechtigungsebene „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.

Um die Gruppenobjekte für einen RCS festzulegen:

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>]"

Wobei: <Berechtigungsstufe> : = „KVM-Benutzer“ oder „KVM-Benutzeradministrator“ oder „KVM-Einheitenadministrator“

<Begrenzungszeichen> ::= ein oder mehr der folgenden Zeichen: <neue Zeile> oder <c/r> oder <Komma> oder <Semikolon> oder <Tab>

<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 zur Kennzeichnung des RCS.

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.

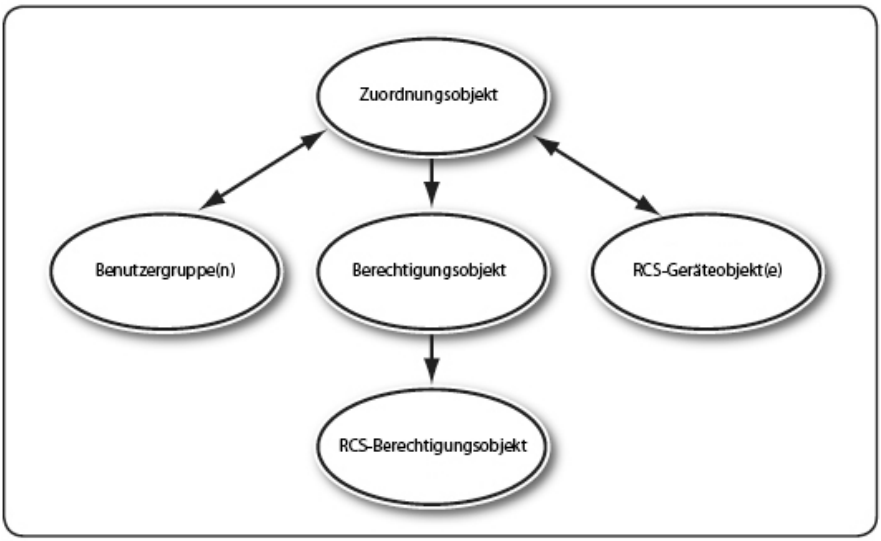
Das RCS-Geräteobjekt stellt die Verknüpfung zum RCS für die Abfrage des Active Directory zum Zweck der Authentifizierung und Autorisierung dar. Wenn ein RCS zum Netzwerk hinzugefügt wird, muss der Administrator den RCS und sein Geräteobjekt mit dem entsprechenden Active Directory-Namen konfigurieren, damit Benutzer die Authentifizierung und Autorisierung über das 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 der folgenden Abbildung wird veranschaulicht, dass das Zuordnungsobjekt die Verbindung bereitstellt, die für sämtliche Authentifizierungs- und Autorisierungsvorgänge erforderlich ist.

Abbildung 5.10. Typisches Setup für Active Directory-Objekte

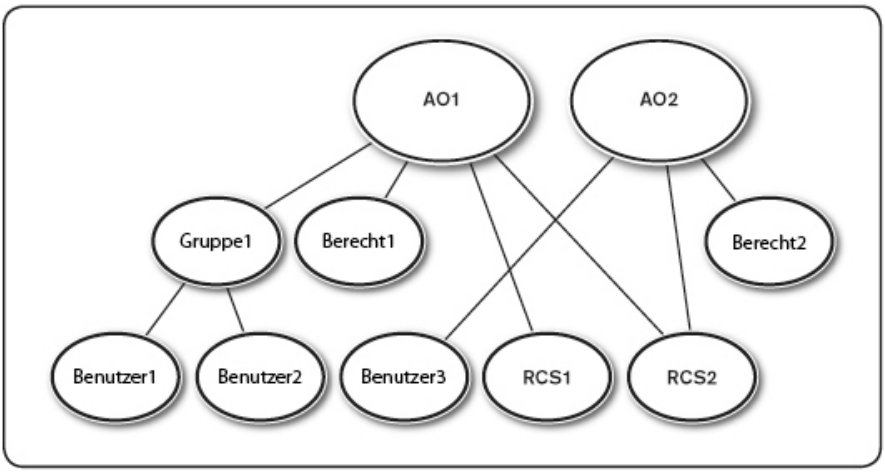


Sie können beliebig viele Zuordnungsobjekte erstellen. Es muss allerdings mindestens ein Zuordnungsobjekt erstellt werden und für jeden RCS im Netzwerk, der mit Active Directory zum Zweck der Authentifizierung und Autorisierung integriert werden soll, muss mindestens ein RCS-Geräteobjekt vorhanden sein. 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 Administratorberechtigungen für beide Remote Console Switches und Benutzer3 die Anmeldeberechtigung für den RCS2 erteilen.

Anhand der folgenden Abbildung sehen Sie, wie im Rahmen dieses Szenarios die entsprechenden Active Directory-Objekte eingerichtet werden:

Abbildung 5.11. 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 RCSs darzustellen.

3 Erstellen Sie zwei Berechtigungsobjekte, Berecht1 und Berecht2, wobei Berecht1 über alle Berechtigungen (Administrator) und Berecht2 über eine Anmeldeberechtigung verfügt.

4 Gruppieren Sie Benutzer1 und Benutzer2 in Gruppe1.

5 Fügen Sie Gruppe1 als Mitglieder im Zuordnungsobjekt1 (AO1), Berecht1 als Berechtigungsobjekte in AO1 und RCS1 und RCS2 als RCS-Geräte in AO1 hinzu.

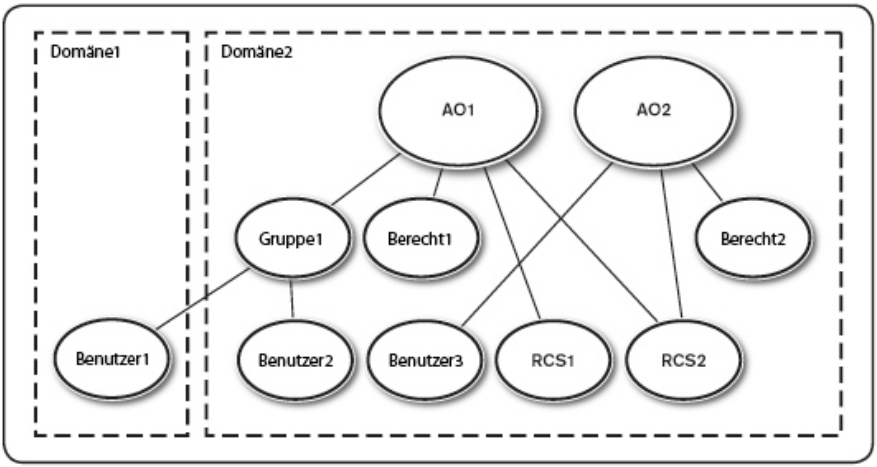
6 Fügen Sie Benutzer3 als Mitglied im Zuordnungsobjekt2 (AO2), Berecht2 als Berechtigungsobjekt in AO2 und RCS2 als RCS-Gerät in AO2 hinzu.

Detaillierte Anweisungen finden Sie im Abschnitt „Hinzufügen von Remote Console Switch-Benutzern und -Berechtigungen zu Active Directory mithilfe von Dell Schemata-Erweiterungen“.

Die folgende Abbildung verdeutlicht, wie Sie Active Directory-Objekte in mehreren Domänen einrichten können. In diesem Szenario 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 Administratorberechtigungen für beide RCSs und Benutzer3 die Anmeldeberechtigung für den RCS2 erteilen.

Abbildung 5.12. 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 RCSs darzustellen.

4 Erstellen Sie zwei Berechtigungsobjekte, Berecht1 und Berecht2, wobei Berecht1 über alle Berechtigungen (Administrator) und Berecht2 über eine Anmeldeberechtigung verfügt.

5 Gruppieren Sie Benutzer1 und Benutzer2 in Gruppe1. 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 den RCS

Bevor Sie Active Directory für den Zugriff auf Ihren RCS 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 RCS-Geräte, Benutzer und Benutzergruppen, RCS-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 RCS-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**.

– oder –

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 Remote Console Switch-Benutzer und -Berechtigungen zu Active Directory mithilfe von Dell Schemata-Erweiterungen

Mit dem von Dell erweiterten Snap-In „Active Directory-Benutzer und -Computer“ können Sie RCS-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 mit dem Namen des RCS übereinstimmen, den Sie in Schritt 4 des Abschnitts „Konfiguration des Remote Console Switches“ auf Seite 40 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 RCS-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-RCS-Objekte
- 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 entsprechend dem Typ der hinzuzufügenden Objekte auswählen. Wenn Sie beispielsweise „Universal“ auswählen, sind Zuordnungsobjekte nur dann verfügbar, wenn die Active Directory Domain im Native Mode oder höher ausgeführt 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 Windows2000-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 zum Zuordnungsobjekt eines 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 eines RCS kann mit jeder Benutzerberechtigung die integrierte Weboberfläche aufzurufen. Die Funktionalität der integrierten Weboberfläche für einen Benutzer wird durch die Benutzer-Berechtigungsstufe eingeschränkt, die im RCS festgelegt ist. LDAP mit erweitertem Dell Schema 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-RCS-Berechtigungen“. Aktivieren Sie das Kontrollkästchen für den Zugriff über die Konsolenumleitung in der Registerkarte „KVM-SIP-Berechtigungen“.

HINWEIS: Wenn Sie eines der Kontrollkästchen für die KVM-RCS-Berechtigungen und das Kontrollkästchen für den Zugriff über die Konsolenumleitung aktivieren, erhalten die in den KVM-RCS-Berechtigungen festgelegten Benutzerberechtigungen Vorrecht gegenüber dem 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.

Verwendung von Active Directory zur Anmeldung am RCS

Sie können Active Directory nutzen, um sich über die RCS Software oder OBWI am RCS anzumelden.

Die Anmeldesyntax ist für alle drei Methoden die gleiche:

<username@domain> domain> oder <domain>\<username>oder <domain>\<username> (wobei es sich beim Benutzernamen [username] um einen ASCII-String mit 1 - 256 Byte handelt). 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 OSCAR 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 SIPs sollte über OSCAR am Console Switch erfolgen. Danach muss über die RCS-Software eine Resynchronisation durchgeführt werden. Hierbei ist zu beachten, dass SIP-Namen unter OSCAR 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 (FAQ)

In der nachfolgenden Tabelle werden häufig gestellte Fragen und Antworten aufgeführt.

Tabelle 5.4: Häufig gestellte Fragen

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.

	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.
Was kann ich tun, wenn ich mich nicht über die Active Directory-Authentifizierung am Remote Console Switch anmelden kann?	• 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 RCS 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 Benutzerdomänennamen und nicht den NetBIOS-Namen verwenden.

A

Anhang A: Terminalbetrieb

Jeder RCS kann auf Switch-Ebene über das Konsolenmenü konfiguriert werden, auf das über den SETUP-Port zugegriffen werden kann. Auf alle Terminalbefehle kann über ein Terminal oder einen PC, auf dem die Terminal-Emulationssoftware ausgeführt wird, zugegriffen werden.

HINWEIS: Die bevorzugte Methode ist das Einstellen sämtlicher Konfigurationseinstellungen mit der lokalen Benutzeroberfläche.

So schließen Sie einen Terminal an einen Switch an:

1 Schließen Sie mit dem im Lieferumfang enthaltenen RJ-45-auf-DB-9-Adapter (Buchse) und einem flachen RJ-45-Kabel ein Terminal oder einen PC, auf dem Terminal-Emulationssoftware (z. B. HyperTerminal) läuft, an den SETUP-Port auf der Gehäuserückseite des Switches an. Das Terminal muss wie folgt eingestellt sein: 9600 bps, 8 bits, 1 stop bit, no parity und no flow control.

2 Schalten Sie alle Zielgeräte und danach den Switch ein. Wenn der Switch die Initialisierung abgeschlossen hat, wird auf dem Konsolenmenü folgende Nachricht angezeigt: **Press any key to continue.**

Menüoptionen im Boot-Menü der Konsole

Während der Switch hochgefahren wird, können Sie durch Tastendruck das Boot-Menü aufrufen. In diesem Menü können Sie eine der vier Optionen auswählen.

- Boot Normal
- Boot Alternate Firmware
- Reset Factory Defaults

- Full-Factory Reset

Optionen im Konsolenhauptmenü

Sobald das Gerät eingeschaltet ist, wird im Hauptmenü der Produktname und die Version angezeigt. In diesem Menü können Sie eine der vier Optionen auswählen.

- Network configuration: Mit dieser Menüoption können Sie die Netzwerkeinstellungen des RCS konfigurieren.
- Debug messages: Diese Menüoption aktiviert die Statusmeldungen der Konsole. Sie sollten Debug-Meldungen nur aktivieren, wenn Sie vom technischen Kundendienst von Dell™ dazu angewiesen wurden, da diese Funktion die Leistung deutlich mindern kann. Dieser Modus kann durch Betätigen einer beliebigen Taste beendet werden, wenn Sie sich die Meldungen durchgelesen haben.
- Reset RCS: Mit dieser Menüoption können Sie einen Warmstart des Switches ausführen.
- Exit: Mit dieser Menüauswahl kehren Sie wieder zur Eingabeaufforderung zurück. Wenn das Konsolenmenü durch ein Kennwort geschützt ist, müssen Sie das Hauptmenü der Konsole verlassen, sodass der nächste Benutzer wieder zur Eingabe von Benutzernamen und Kennwort aufgefordert wird.

B

Anhang B: Verwenden von SIPs

Ein Administrator kann für jeden seriellen SIP-Port über die lokale Benutzeroberfläche oder das Remote-OBWI zwischen den Pinbelegungen für den Avocent ACS-Konsolenserver und für Cisco wählen. ACS ist der Standardwert.

So ändern Sie die Pinbelegung auf den Cisco Modus:

1 Wählen Sie *Einheiten-Ansicht – RCS – RCS-Einstellungen – Ports – SIPs* aus.

2 Klicken Sie auf den gewünschten SIP.

3 Wählen Sie *Einstellungen – Pinbelegung*.

HINWEIS: Wenn ein DB-9-Adapter verwendet wird, wählen Sie die ACS Konsolenserver-Pinbelegung aus.

Portpinbelegung des ACS-Konsolenservers

Die folgende Tabelle listet die Pinbelegungen des seriellen Ports des ACS-Konsolenservers für den SIP auf.

Tabelle B.1: Pinbelegung des seriellen Ports des ACS-Konsolenservers

Pin-Nr.	Signalname	Eingang/Ausgang
1	RTS –Request to Send	AUSGANG
2	DTR –Data Terminal Ready	AUSGANG
3	TXD –Transmit Data	AUSGANG
4	GND –Signal Ground	-

Pin-Nr.	Signalname	Eingang/Ausgang
5	CTS –Clear to Send	EINGANG
6	RXD –Receive Data	EINGANG
7	DCD/DSR –Data Set Ready	EINGANG
8	N/C –Not Connected	-

Cisco Portpinbelegung

Die folgende Tabelle listet die Cisco-Pinbelegungen des seriellen Ports für die SIPs auf.

Tabelle B.2: Cisco-Port Pinbelegung

Pin-Nr.	Signalname	Eingang/Ausgang
1	CTS –Clear to Send	EINGANG
2	DCD/DSR –Data Set Ready	EINGANG
3	RXD –Receive Data	EINGANG
4	GND –Signal Ground	-
5	N/C –Not Connected	-
6	TXD –Transmit Data	AUSGANG
7	DTR –Data Terminal Ready	AUSGANG
8	RTS –Request to Send	AUSGANG

C

Anhang C: MIB und SNMP-Traps

Der Dell RCS ist in der Lage, Audit-Ereignisse an einen SNMP-Manager zu senden. Die SNMP-Traps sind in einer SNMP-Trap-MIB definiert.

Mithilfe der Funktion „Trap-MIB speichern“ kann die Trap-MIB-Datei über den RCS hochgeladen werden. Die hochgeladene Trap-MIB-Datei kann anschließend in eine SNMP-Trap-Receiver-Anwendung geladen werden.

Audit-Ereignisse können auch an „Syslog“-Ziele weitergeleitet werden. Das Format jeder Syslog-Nachricht wird im jeweiligen „--#SUMMARY“-Kommentar aller innerhalb der Trap-MIB-Datei definierten Traps angezeigt.

In diesem Anhang finden Sie eine Beschreibung der eventuell über den RCS erzeugten Trap-Ereignisse. Obwohl versucht wurde, die Informationen innerhalb dieses Anhangs auf dem neuesten Stand zu halten, enthält die Trap-MIB-Datei jedoch die genauesten Trap-Informationen.

Ein SNMP-Manager kann über IPv4- oder IPv6-Protokolle auf die MIB-II-Objekte des RCS zugreifen.

Standardmäßig kann auf die unternehmensspezifischen MIB-Objekte innerhalb des RCS nicht über SNMP zugegriffen werden.

Die RCS-Trap-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 über jeden TRAP gemeldeten spezifischen Objekte sind in der über den RCS hochgeladenen Trap-MIB-Datei definiert. In der nachfolgenden Tabelle finden Sie eine Auflistung der erzeugten Trap-Ereignisse.

Tabelle C.1: Erzeugte Trap-Ereignisse

Trap-Ereignis	Trap-Nummer
Neustart wurde eingeleitet	1
Benutzeranmeldung	2
Benutzerabmeldung	3
Zielgeräte-Sitzung gestartet	4
Zielgeräte-Sitzung angehalten	5
Zielgeräte-Sitzung abgebrochen	6
Traps 7 bis 9 abgelehnt	7-9
Image-Datei-Aktualisierung gestartet	10
Image-Datei-Aktualisierungsergebnisse	11
Benutzer hinzugefügt	12

Trap-Ereignis	Trap-Nummer
Benutzer gelöscht	13
Benutzer geändert	14
Benutzer gesperrt	15
Benutzer freigegeben	16
Benutzer-Authentifizierungsfehler	17
SIP hinzugefügt	18
SIP entfernt	19
SIP verschoben	20
Zielgerätename geändert	21
Gestufter Switch hinzugefügt.	22
Gestufter Switch entfernt.	23
Name des gestuften Switches geändert	24
Konfigurationsdatei geladen	25
Benutzerdatenbank-Datei geladen	26
CA-Zertifikat geladen	27
SIP-Image-Aktualisierung wurde gestartet	28
SIP-Image-Aktualisierungsergebnisse	29
SIP-Adapter neu gestartet	30
Virtual Media-Sitzung gestartet	31

Trap-Ereignis	Trap-Nummer
Virtual Media-Sitzung angehalten	32
Virtual Media Sitzung beendet	33
Virtual Media-Sitzung reserviert	34
Virtual Media-Sitzung nicht reserviert	35
Virtual Media-Laufwerk zugewiesen	36
Zuweisung des Virtual Media-Laufwerks aufgehoben	37
Traps 38 bis 44 abgelehnt	38-44
Bildschirmauflösung geändert	45
Statuszusammenfassung des Zielgeräts geändert	46
Werkseinstellungen eingestellt	47
Stromversorgungsfehler	48
Stromversorgung wiederhergestellt	49
PDU-Gerät online	50
PDU-Gerät offline	51
PDU-Ausgang Einschaltbefehl	52
PDU-Ausgang Ausschaltbefehl	53
PDU-Ausgang Neustartbefehl	54
PDU-Ausgang Ein-Erkennungsfehler	55
PDU-Ausgang Aus-Erkennungsfehler	56

Trap-Ereignis	Trap-Nummer
PDU-Status „Ausgang ein“	57
PDU-Status „Ausgang aus“	58
PDU-Portname geändert	59
PDU-Ausgangsname geändert	60
PDU-Eingang Gesamtlast hoch	61
PDU-Eingang Gesamtlast gering	62
PDU-Gerätename geändert	63
PDU-Eingangsname geändert	64
PDU-Ausgang Sperrbefehl	65
PDU-Ausgang Entsperrbefehl	66
PDU-Status „Ausgang sperren“	67
PDU-Status „Ausgangssperre aufheben“	68
PDU Image-Datei-Aktualisierung gestartet	69
PDU Image-Datei-Aktualisierungsergebnisse	70
PDU-Stromkreisname geändert	71
PDU-Gerät Gesamtlast hoch	72
PDU-Stromkreis Gesamtlast hoch	73
PDU-Ausgang Gesamtlast hoch	74
Gebläsefehler	75

Trap-Ereignis	Trap-Nummer
Temperaturbereich	76
Smart Card eingesetzt	77
Smart Card entfernt	78

D

Anhang D: Informationen zur Kabel-Pinbelegung

HINWEIS: Alle Switches verfügen über eine 8-polige Modularsteckerbuchse und Konsolen-/Setup-Ports.

Pinbelegung des Modems

Die Port-Pinbelegung des Modems und die entsprechenden Beschreibungen entnehmen Sie der nachfolgenden Abbildung und Tabelle.

Abbildung D.1. Pinbelegung des Modems

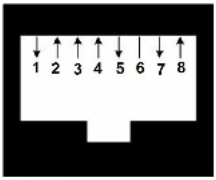


Tabelle D.1: Beschreibung der Pinbelegung des Modems

Stiftnummer	Beschreibung	Stiftnummer	Beschreibung
1	Request to Send (RTS)	5	Transmit Data (TXD)
2	Data Set Ready (DSR)	6	Signal Ground (SG)
3	Data Carrier Detect (DCD)	7	Data Terminal Ready (DTR)
4	Receive Data (RXD)	8	Clear to Send (CTS)

Konsolen-/Setup-Pinbelegung

Die Konsolen-/Setup-Pinbelegung und die entsprechenden Beschreibungen entnehmen Sie der nachfolgenden Abbildung und Tabelle.

Abbildung D.2. Konsolen-/Setup-Pinbelegung

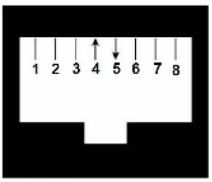


Tabelle D.2: Beschreibung der Konsolen-/Setup-Pinbelegung

Stiftnummer	Beschreibung	Stiftnummer	Beschreibung
1	Keine Verbindung	5	Transmit Data (TXD)
2	Keine Verbindung	6	Signal Ground (SG)
3	Keine Verbindung	7	Keine Verbindung
4	Receive Data (RXD)	8	Keine Verbindung

E

Anhang E: UTP-Verkabelung

In diesem Anhang werden die unterschiedlichen Anschlussmöglichkeiten beschrieben. Das RCS-System verwendet UTP-Kabel. Die Leistungsfähigkeit Ihres Switch-Systems hängt von der Qualität der Verkabelungen ab. Schlechte Kabelqualität oder schlecht verlegte bzw. gewartete Kabel können die Systemleistung des Switches verringern.

HINWEIS: Dieser Anhang ist nur für Informationszwecke gedacht. Sprechen Sie vor der Installation mit Ihrem Elektriker und/oder Kabelfachmann vor Ort.

UTP-Kupferkabel

Im Folgenden werden die drei UTP-Arten, die die RCS unterstützt, allgemein beschrieben:

- CAT 5-Hochleistungskabel (4-paarig), bestehend aus verdrillten Leiterpaaren. Diese Kabelart wird in erster Linie für die Datenübermittlung verwendet. Durch das Verdrillen von Leitungspaaren wird das Kabel widerstandsfähiger gegen das Eindringen von Störungen. CAT 5-Kabel werden allgemein für Netzwerke mit 10 oder 100 MBit/s verwendet.
- CAT 5E-Kabel (verbessert) haben die gleichen Merkmale wie CAT 5-Kabel, werden jedoch unter strengeren Vorschriften hergestellt.
- CAT 6-Kabel werden unter höheren Ansprüchen als CAT 5E-Kabel hergestellt. CAT 6-Kabel verfügen über höhere messbare Frequenzbereiche und bessere Leistungsansprüche als CAT 5E-Kabel bei gleichen Frequenzen.

Kabelnormen

Es bestehen zwei unterstützte Kabelnormen für UTP-Kabel mit 8 Leitern (4-paarig) und RJ-45-Stecker: EIA/TIA 568A und B. Diese Normen werden für Anlagen mit UTP-Kabeln angewendet. Das RCS-System unterstützt alle diese Kabelnormen. In der folgenden Tabelle wird die Pinbelegung beschrieben.

Tabelle E.1: UTP-Kabelnormen

Stift	EIA/TIA 568A	EIA/TIA 568B
1	weiß/grün	weiß/orange
2	grün	orange
3	weiß/orange	weiß/grün
4	blau	blau
5	weiß/blau	weiß/blau
6	orange	grün
7	weiß/braun	weiß/braun
8	braun	braun

Kabelverlegung, Kabelwartung und Sicherheitshinweise

Im Folgenden werden wichtige Sicherheitshinweise aufgelistet, die vor der Installation oder Wartung von Kabeln beachtet werden müssen:

- Verlegen Sie UTP-Kabel mit einer maximalen Länge von 10 Metern.

- Behalten Sie die Verdrillung der Paare bis zum endgültigen Anschluss bei oder lösen Sie die Verdrillung um höchstens 1,25 cm. Entfernen Sie am Kabelende nicht mehr als 2,54 cm der Ummantelung.
- Wenn das Kabel gebogen werden muss, sollte eine leichte Biegung mit nicht mehr als 2,54 cm Radius verlegt werden. Durch harte Biegungen oder Knicke des Kabels kann das Kabelinnere permanent beschädigt werden.
- Fassen Sie die Kabel unter geringem oder mittlerem Druck mit Kabelbindern zusammen. Binden Sie die Kabelbinder nicht zu fest.
- Kabel ggf. mithilfe von Kontaktblöcken, Patch-Panels und Komponenten querverbinden. Kabel dürfen nicht überbrückt oder gespleißt werden.
- UTP-Kabel so weit wie möglich von potenziellen elektromagnetischen Störquellen (zum Beispiel Stromkabel, Transformatoren oder Lampenfassungen) entfernt verlegen. Befestigen Sie die Kabel nicht an elektrischen Leitungsführungen und verlegen Sie die Kabel nicht auf elektrischen Vorrichtungen.
- Überprüfen Sie jedes installierte Segment mit einem Kabelprüfer. „Toning" ist keine akzeptable Prüfung.
- Installieren Sie die Anschlussbuchsen stets so, dass kein Staub oder andere Verschmutzungen auf die Kontakte gelangen können. Die Kontakte der Anschlussbuchse sollten nach oben auf die Einbauplatten zeigen oder sich links/rechts/unterhalb der Aufputzdosen befinden.
- Lassen Sie immer etwas zusätzlichen Durchhang für die Kabel, rollen Sie diese sauber in die Decke oder in eine unauffällige Stelle auf. Lassen Sie eine Extra-Kabellänge von mindestens 1,5 m am Arbeitsende und 5 m am Patch-Panel.
- Entscheiden Sie sich vor Arbeitsbeginn für die Kabelnorm 568A oder 568B. Verkabeln Sie alle Anschlussbuchsen und Patch-Panels nach dem gleichen Verkabelungsschema. Kombinieren Sie 568A- und 568B-Verkabelung nicht in derselben Installation.

- Befolgen Sie stets die örtlichen und gesetzlichen Feuer- und Gebäudevorschriften. Stellen Sie sicher, dass alle Kabel, die durch eine Brandschutzmauer verlegt werden, die Feuerschutzbedingungen erfüllen. Verwenden Sie ggf. Plenumkabel.

F

Anhang F: Sun Tastenemulation für Zusatztasten

Einige Tasten auf einer herkömmlichen Sun 5 Tastatur Typ 5 (US) können durch Tastenfolgen auf einer am lokalen Port angeschlossenen USB-Tastatur emuliert werden. Um die Tastenemulation für Sun-Zusatztasten zu aktivieren und diese Tasten zu verwenden, halten Sie <Strg+Umschalt+Alt>gedrückt und drücken Sie die Die Rollen-Tasten-LED blinkt. Verwenden Sie die entsprechenden Tasten in der folgenden Tabelle so, als würden Sie die Zusatztasten einer Sun Tastatur bedienen. Beispiel: Für <Stopp + A> drücken und halten Sie <Strg+Umschalt+Alt>. Drücken Sie anschließend <Rollen> und dann <F1 + A>.

Diese Tastenkombinationen funktionieren bei Dell USB-, USB2- und USB2+CAC-SIPs sowie Avocent USB-, USB2- und VMC-IQ-Modulen. Diese Tastenkombinationen werden mit Ausnahme von <F12> von Microsoft Windows nicht erkannt. Wird <F12> verwendet, dann wird eine Windows-Tastenfolge ausgeführt. Um die Tastenemulation für Sun-Zusatztasten zu deaktivieren, halten Sie <Strg+Umschalt+Alt> gedrückt und drücken Sie die <Rollen>-Taste.

Tabelle F.1: Sun Tastenemulation

Compose	Anwendung[1]
Compose	Zehnertastatur
Strom	F11
Öffnen	F7

Hilfe	Num-Taste
Props	F3
Vorderseite	F5
Stop	F1
Again	F2
Rückgängig	F4
Ausschneiden	F10
Kopieren	F6
Einfügen	F8
Find	F9
Mute	Zehnertastatur /
Vol.+	Zehnertastatur +
Vol.-	Zehnertastatur -
Command (links)[2]	F12
Command (links)[2]	Win (GUI) links[1]
Command (rechts)[2]	Win (GUI) rechts [1]

WEITERE HINWEISE:

(1) Tastatur mit 104 Tasten für Windows 95.

(2) Die Command-Taste ist die Sun Meta- (Diamant-) Taste.

G

Anhang G: Technische Daten

Tabelle G.1: Technische Daten RCS

Port-Anzahl	1082DS: 8 2162DS: 16 4322DS: 32
Typ	Dell PS/2-, USB-, USB2-, USB2+CAC- und seriellel SIPs. Avocent PS/2-, PS2M-, USB-, Sun-, USB2-, VMC- und serielle Module.
Anschlüsse	8-polig modular (RJ-45)
Sync-Arten	Unabhängig horizontal und vertikal
Eingangsvideoauflösung	Standard 640 x 480 bei 60 Hz 800 x 600 bei 75 Hz 960 x 700 bei 75 Hz 1024 x 768 bei 75 Hz 1280 x 1024 bei 75 Hz 1600 x 1200 bei 60 Hz Breitbild 800 x 500 bei 60 Hz 1024 x 640 bei 60 Hz 1280 x 800 bei 60 Hz 1440 x 900 bei 60 Hz 1680 x 1050 bei 60 Hz

Unterstützte Verkabelung	UTP 4-paarig, maximale Länge 45 Meter
Abmessungen	
Formfaktor	1-HE- oder 0-HE-Rackbefestigung
Abmessungen	1,72 x 17,00 x 9,20 (Höhe x Breite x Tiefe)
Gewicht (ohne Kabel)	1082DS: 6,6 lb (3,0 kg) 2162DS: 7,0 lb (3,2 kg) 4322DS: 7,6 lb (3,4 kg)
SETUP-Port	
Nummer	1
Protokoll	RS-232 seriell
Stecker	8-polig modular (RJ-45)
Lokaler Port	
Anzahl/Typ	1 VGA/4 USB
Netzwerkverbindung	
Nummer	2
Protokoll	10/100/1000 Ethernet
Stecker	8-polig modular (RJ-45)
USB-Geräte-Port	
Nummer	4
Protokoll	USB 2.0

MODEM-Port	
Nummer	1
Protokoll	RS-232 seriell
Anschlüsse	8-polig modular (RJ-45)
PDU-Port	
Nummer	2
Protokoll	RS-232 seriell
Stecker	8-polig modular (RJ-45)
Leistungsdaten	
Anschlüsse	1082DS: 1 IEC C14 2162DS: 2 IEC C14 4322DS: 2 IEC C14
Typ	Intern
Strom	18 W
Wärmeabstrahlung	47 BTU/hr
Wechselstrom-Eingangsleistungsbereich	100 - 240 V Wechselstrom
Wechselstromfrequenz	50/60 Hz Autosensing
Wechselstrom-Eingangsspannungswert	1,25 A

Wechselstrom-Eingangsleistung (max.)	40 W
Umgebungsbedingungen	
Temperatur	0 bis 50 °C Betriebstemperatur; -20 bis 70 °C bei abgeschaltetem Gerät
Luftfeuchtigkeit	Betrieb: Relative Luftfeuchtigkeit (nicht kondensierend): 20 % bis 80 % bei abgeschaltetem Gerät: Relative Luftfeuchtigkeit: 5 % bis 95 %, Feuchttemperatur: 38,7 °C (max.)
Sicherheits- und EMV-Zulassungen und -Kennzeichnungen	UL / cUL, CE - EU, N (Nemko), GOST, C-Tick, NOM / NYCE, MIC (KCC), SASO, TUV-GS, IRAM, FCC, ICES, VCCI, SoNCAP, SABS, Bellis, FIS/ Kvalitet, Koncar, INSM, Ukrtest, STZ, KUCAS 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.

H

Anhang H: Technischer Kundendienst

Unser technischer Kundendienst steht Ihnen jederzeit bei Fragen hinsichtlich Installations- oder Betriebsproblemen mit Ihrem Produkt von Dell zur Verfügung. Verfahren Sie zur schnellstmöglichen Problemlösung wie folgt.

So verfahren Sie zur Problemlösung:

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.