CommandCenter Secure Gateway

Handbuch für Administratoren

Version 5.1

Copyright © 2011 Raritan, Inc.

CCA-0N-v5.1-G

Februar 2011

255-80-5140-00-0N

Dieses Dokument enthält urheberrechtlich geschützte Informationen. Alle Rechte vorbehalten. Ohne die vorherige ausdrückliche schriftliche Genehmigung von Raritan, Inc. darf kein Teil dieses Dokuments fotokopiert, vervielfältigt oder in eine andere Sprache übersetzt werden.

© Copyright 2011 Raritan, Inc. CommandCenter®, Dominion®, Paragon® und das Raritan-Firmenlogo sind Marken oder eingetragene Marken von Raritan, Inc. Alle Rechte vorbehalten. Java® ist eine eingetragene Marke von Sun Microsystems, Inc. Internet Explorer® ist eine eingetragene Marke der Microsoft Corporation. Netscape® und Netscape Navigator® sind eingetragene Marken der Netscape Communication Corporation. Alle anderen Marken oder eingetragenen Marken sind Eigentum der jeweiligen Rechteinhaber.

Einhaltung der FCC-Bestimmungen

In Tests wurde festgestellt, dass das Gerät die Grenzwerte für digitale Geräte der Klasse A gemäß Teil 15 der FCC-Bestimmungen einhält. Diese Grenzwerte sollen in kommerziell genutzten Umgebungen einen angemessenen Schutz vor Störungen bieten. Das in diesem Handbuch beschriebene Gerät erzeugt, verbraucht und gibt unter Umständen hochfrequente Strahlung ab und kann bei unsachgemäßer Installation und Verwendung zu Störungen des Rundfunk- und Fernsehempfangs führen. Der Betrieb dieses Geräts in Wohnumgebungen führt unter Umständen zu schädlichen Störungen.

VCCI-Informationen (Japan)

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Raritan ist nicht verantwortlich für Schäden an diesem Produkt, die durch einen Unfall, ein Missgeschick, durch Missbrauch, Fremdeingriffe am Produkt oder andere Ereignisse entstanden sind, die sich außerhalb der Kontrolle von Raritan befinden oder unter normalen Betriebsbedingungen nicht auftreten.

1F61
I.T.E.

Inhalt

Neuerungen im CC-SG Handbuch für Administratoren **xvi**

Kapitel 1 Einleitung **1**

Vorbereitungen 1
Terminologie/Abkürzungen 2
Clientbrowser-Anforderungen 4

Kapitel 2 Zugreifen auf CC-SG **5**

Browserbasierter Zugriff über CC-SG-Administrations-Client 5
JRE-Inkompatibilität 6
Thick-Client-Zugriff 6
Thick-Client installieren 7
Thick-Client verwenden 8
CC-SG-Administrations-Client 8

Kapitel 3 Erste Schritte **10**

Lizenzierung – Erste Schritte – Neue und bestehende Kunden 10
Lizenzierung – Grundlegende Lizenzinformationen 11
Verfügbare Lizenzen 11
Auffinden der Host-ID Ihrer physischen Appliance und Überprüfen der Anzahl der Knoten in der Datenbank 13
Lizenzierung – Neue Kunden – Physische Appliance 14
Lizenzierung – Cluster – Neue Kunden 17
Lizenzierung – Virtuelle Appliance mit Lizenzserver 18
Installationsvoraussetzungen für virtuelle Appliance 18
Installationsdateien herunterladen 19
Lizenserversoftware unter Linux- oder Windows-Server installieren 19
Erhalt Ihrer Lizenz 21
Lizenzdatei auf Lizenzserver kopieren 23
Lizenzserver starten 23
CommandCenter Secure Gateway unter VMware ESX Server 4.0 installieren 24
Anmelden bei Diagnosekonsole und Einstellen der IP-Adresse für CC-SG 25
Anmelden bei CC-SG 26
Installieren und Auschecken der Lizenz 26
Kommunikation mit Lizenzserver 27
Befehlszeilenprogramme zum Verwalten des Lizenzservers 28
VMware Tools installieren oder aktualisieren 30
Sicherungen und Schnappschüsse von virtueller Appliance und Speicherservern konfigurieren 31

Virtuelle Appliances mit Remote-Speicherservern 31
Lizenzierung – Beschränkter Betrieb vor der Lizenzinstallation 31
Lizenzierung – Bestehende Kunden 33
Lizenzierung – Rehosting 34
Lizenz hinzufügen 34
IP-Adresse bestätigen 35
CC-SG-Serverzeit festlegen 35
Kompatibilitätsmatrix überprüfen 36
Anwendungsversionen prüfen und aktualisieren 37

Kapitel 4 Konfigurieren von CC-SG mit dem Setup-Assistenten 39

Vor der Verwendung des Setup-Assistenten 40
Zuordnungen im Setup-Assistenten 40
Kategorien und Elemente erstellen 40
Geräte-Setup 41
Geräte erkennen und hinzufügen 41
Gruppen erstellen 43
Gerätegruppen und Knotengruppen hinzufügen 43
Benutzerverwaltung 46
Benutzergruppen und Benutzer hinzufügen 46

Kapitel 5 Zuordnungen, Kategorien und Elemente 49

Zuordnungen 49
Zuordnungsterminologie 49
Zuordnungsbestimmende Kategorien und Elemente 49
Zuordnungen erstellen 50
Kategorien und Elemente hinzufügen, bearbeiten und löschen 50
Kategorien hinzufügen 51
Kategorien löschen 51
Elemente hinzufügen 51
Kategorien und Elemente per CSV-Dateiimport hinzufügen 52
Anforderungen an CSV-Dateien – Kategorien und Elemente 52
Beispiel-CSV-Datei für Kategorien und Elemente 53
Kategorien und Elemente importieren 54
Kategorien und Elemente exportieren 54

Kapitel 6 Geräte, Gerätegruppen und Ports 56

Geräte anzeigen 57
Die Registerkarte "Geräte" 57
Geräte- und Portsymbole 57
Portsortieroptionen 58
Fenster "Geräteprofil" 60
Topologieansicht 61
Kontextmenüoptionen auf der Registerkarte Geräte 61
Geräte suchen 61
Platzhalter für die Suche 62
Beispiele mit Platzhaltern 62

Geräte erkennen 62
Geräte hinzufügen 63
KVM- oder serielle Geräte hinzufügen 64
PowerStrip-Geräte hinzufügen 66
Dominion PX-Geräte hinzufügen 66
Geräte bearbeiten 67
Ändern der HTTP- und HTTPS-Ports für ein KX2-Gerät 68
PowerStrip- oder Dominion PX-Geräte bearbeiten 68
Hinweise zu einem Geräteprofil hinzufügen 69
Einsatzort und Kontakte zu einem Geräteprofil hinzufügen 69
Geräte löschen 70
Ports konfigurieren 70
Seriellen Port konfigurieren 71
KVM-Port konfigurieren 71
Durch das Konfigurieren von Ports erstellte Knoten 72
Ports bearbeiten 73
Ports löschen 74
An KX2 angeschlossenes Blade-Chassis-Gerät konfigurieren 74
Übersicht über das Blade-Chassis 74
Blade-Chassis-Gerät hinzufügen 75
Blade-Chassis-Gerät bearbeiten 79
Blade-Chassis-Gerät löschen 80
Blade-Chassis-Gerät auf einen anderen Port verschieben 80
Blade-Server-Ports als normale KX2-Ports wiederherstellen 81
Massenkopieren für Gerätezuordnungen, Einsatzort und Kontakte 82
Konfigurieren der mit KX2 2.3 oder höher verbundenen analogen KVM-Switches 83
Hinzufügen eines mit KX2 verbundenen KVM-Switches 83
Konfigurieren von Ports auf einem mit KX2 verbundenen analogen KVM-Switch-Gerät . 84
Gerätegruppenmanager 85
Überblick über Gerätegruppen 86
Gerätegruppen hinzufügen 87
Gerätegruppen bearbeiten 91
Gerätegruppen löschen 91
Geräte per CSV-Dateiimport hinzufügen 92
Anforderungen an CSV-Dateien – Geräte 93
Beispiel-CSV-Datei für Geräte 98
Geräte importieren 98
Geräte exportieren 99
Gerät aktualisieren 99
Gerätekonfiguration sichern 100
Gerätekonfiguration wiederherstellen 101
Gerätekonfiguration wiederherstellen (KX, KSX, KX101, SX, IP-Reach) 101
Alle Konfigurationsdaten mit Ausnahme der Netzwerkeinstellungen auf einem KX2-, KSX2- oder KX2-101-Gerät wiederherstellen 102
Nur Geräteeinstellungen oder Benutzer- und Benutzergruppendaten auf einem KX2-, KSX2- oder KX2-101-Gerät wiederherstellen 102
Alle Konfigurationsdaten auf einem KX2-, KSX2- oder KX2-101-Gerät wiederherstellen 103
Sicherungsdateien von Geräten speichern, hochladen und löschen 103

Gerätekonfiguration kopieren 105
Gerät neu starten 106
Gerät anpingen 106
CC-SG-Verwaltung eines Geräts unterbrechen 106
Geräteverwaltung fortsetzen 107
Geräteverwaltung mit einer geplanten Aufgabe unterbrechen und fortsetzen 107
Gerätestrommanager 108
Verwaltungsseite eines Geräts aufrufen 109
Benutzerverbindung trennen 109
Sonderzugriff auf Paragon II-Systemgeräte 110
Paragon II-Systemcontroller (P2-SC) 110
IP-Reach- und UST-IP-Verwaltung 110

Kapitel 7 Verwaltete PowerStrips 111

PowerStrips konfigurieren, die von einem anderen Gerät in CC-SG verwaltet werden 113
PowerStrips, die an KX-, KX2-, KX2-101-, KSX2- und P2SC-Geräte angeschlossen sind, konfigurieren 114
PowerStrip-Gerät, das an ein KX-, KX2-, KX2-101-, KSX2- oder P2SC-Gerät angeschlossen ist, hinzufügen 114
PowerStrip eines KX-, KX2-, KX2-101-, KSX2- oder P2SC-Geräts an einen anderen Port bewegen 115
PowerStrip, der an ein KX-, KX2-, KX2-101-, KSX2- oder P2SC-Gerät angeschlossen ist, löschen 115
PowerStrips, die an SX 3.0- und KSX-Geräte angeschlossen sind, konfigurieren 115
PowerStrip, der an ein SX 3.0- oder KSX-Gerät angeschlossen ist, hinzufügen 116
PowerStrip, der an ein SX 3.0- oder KSX-Gerät angeschlossen ist, löschen 117
Geräte- oder Portzuordnung eines PowerStrips ändern (SX 3.0, KSX) 117
PowerStrips, die an SX 3.1-Geräte angeschlossen sind, konfigurieren 118
PowerStrip, der an ein SX 3.1-Gerät angeschlossen ist, hinzufügen 118
PowerStrip eines SX 3.1-Geräts an einen anderen Port bewegen 119
PowerStrip, der an ein SX 3.1-Gerät angeschlossen ist, löschen 119
Ausgänge auf einem PowerStrip konfigurieren 119

Kapitel 8 Knoten, Knotengruppen und Schnittstellen 121

Überblick über Knoten und Schnittstellen 122
Knoten 122
Knotennamen 122
Schnittstellen 123
Knoten anzeigen 123
Registerkarte "Knoten" 123
Knotenprofil 124
Knoten- und Schnittstellensymbole 126
Dienstkonten 126
Überblick über Dienstkonten 126
Dienstkonten hinzufügen, bearbeiten und löschen 127
Kennwort für ein Dienstkonto ändern 128
Schnittstellen Dienstkonten zuweisen 129

Knoten hinzufügen, bearbeiten und löschen 130
Knoten hinzufügen 130
Durch das Konfigurieren von Ports erstellte Knoten 131
Knoten bearbeiten 131
Knoten löschen 131
Einsatzort und Kontakte zu einem Knotenprofil hinzufügen 132
Hinweise zu einem Knotenprofil hinzufügen 133
Virtuelle Infrastruktur in CC-SG konfigurieren 133
Terminologie zur virtuellen Infrastruktur 133
Überblick über virtuelle Knoten 135
Steuerungssystem mit virtuellen Hosts und virtuellen Geräten hinzufügen 135
Virtuellen Host mit virtuellen Geräten hinzufügen 138
Steuerungssysteme, virtuelle Hosts und virtuelle Geräte bearbeiten 141
Steuerungssysteme und virtuelle Hosts löschen 143
Virtuellen Geräteknoten löschen 143
Virtuelle Infrastruktur löschen 143
vSphere 4-Benutzer müssen ein neues Plug-In installieren 144
Virtuelle Infrastruktur mit CC-SG synchronisieren 145
Virtuelle Infrastruktur synchronisieren 145
Tägliche Synchronisierung der virtuellen Infrastruktur aktivieren oder deaktivieren 145
Virtuellen Host neu starten oder Neustart erzwingen 146
Zugriff auf die Ansicht für die virtuelle Topologie 147
Verbindung zu Knoten herstellen 147
Firefox-Benutzer des Zugriffs-Clients müssen JNLP-Datei herunterladen 148
Knoten anpingen 148
Schnittstellen hinzufügen, bearbeiten und löschen 148
Schnittstellen hinzufügen 148
Schnittstellen bearbeiten 160
Schnittstellen löschen 160
Lesezeichen für Schnittstelle 161
Direkten Portzugriff auf Knoten konfigurieren 162
Massenkopieren für Knotenzuordnungen, Einsatzort und Kontakte 162
Chat verwenden 163
Knoten per CSV-Dateiimport hinzufügen 164
Anforderungen an CSV-Dateien – Knoten 165
Beispiel-CSV-Datei für Knoten 176
Knoten importieren 177
Knoten exportieren 177
Bearbeiten von IP-Adressen mit CSV-Datei-Import 178
Knotengruppen hinzufügen, bearbeiten und löschen 179
Überblick über Knotengruppen 179
Knotengruppen hinzufügen 180
Knotengruppen bearbeiten 184
Knotengruppen löschen 184

Kapitel 9 Benutzer und Benutzergruppen 185

Registerkarte "Benutzer" 186
Standardbenutzergruppen 187
Die CC-Superuser-Gruppe 187
Systemadministratorgruppe 187

CC Users-Gruppe 188
Benutzergruppen hinzufügen, bearbeiten und löschen 188
Benutzergruppen hinzufügen 188
Benutzergruppen bearbeiten 190
Benutzergruppen löschen 191
Anzahl an KVM-Sitzungen pro Benutzer einschränken 192
Zugriffsüberwachung für Benutzergruppen konfigurieren 193
Benutzer hinzufügen, bearbeiten und löschen 194
Benutzer hinzufügen 194
Benutzer bearbeiten 195
Benutzer löschen 196
Benutzer einer Gruppe zuordnen 197
Benutzer aus einer Gruppe löschen 198
Benutzer per CSV-Dateiimport hinzufügen 198
Anforderungen an CSV-Dateien – Benutzer 199
Beispiel-CSV-Datei für Benutzer 204
Benutzer importieren 204
Benutzer exportieren 205
Ihr Benutzerprofil 206
Eigenes Kennwort ändern 206
Eigenen Namen ändern 206
Eigene Standardsucheinstellungen ändern 206
Standardschriftgrad für CC-SG ändern 207
Eigene E-Mail-Adresse ändern 207
Benutzernamen des CC-SG-Superusers ändern 207
Benutzer abmelden 207
Massenkopieren von Benutzern 208

Kapitel 10 Richtlinien für die Zugriffssteuerung 210

Richtlinien hinzufügen 211
Richtlinien bearbeiten 212
Richtlinien löschen 214
Unterstützung für virtuelle Medien 214
Richtlinien Benutzergruppen zuordnen 215

Kapitel 11 Benutzerdefinierte Ansichten für Geräte und Knoten 216

Typen von benutzerdefinierten Ansichten 216
Ansicht nach Kategorie 216
Filter nach Knotengruppe 216
Filter nach Gerätegruppe 217
Verwenden von benutzerdefinierten Ansichten im Administrations-Client 217
Benutzerdefinierte Ansichten für Knoten 217
Benutzerdefinierte Ansichten für Geräte 220

Kapitel 12 Remoteauthentifizierung 225

Überblick über Authentifizierung und Autorisierung (AA) 225
Authentifizierungsfluss 225

Benutzerkonten ... 226
Definierte Namen für LDAP und Active Directory ... 226
Definierte Namen für Active Directory festlegen ... 227
Definierte Namen für LDAP festlegen ... 227
Benutzernamen für Active Directory festlegen ... 227
Basis-DNs festlegen ... 227
Module für die Authentifizierung und Autorisierung festlegen ... 227
Reihenfolge für externe AA-Server festlegen ... 228
Überblick über AD und CC-SG ... 228
AD-Module zu CC-SG hinzufügen ... 229
Allgemeine AD-Einstellungen ... 229
Erweiterte AD-Einstellungen ... 231
AD-Gruppeneinstellungen ... 232
AD-Vertrauenseinstellungen ... 233
AD-Module bearbeiten ... 234
AD-Benutzergruppen importieren ... 235
Active Directory mit CC-SG synchronisieren ... 236
Alle Benutzergruppen mit Active Directory synchronisieren ... 237
Alle AD-Module synchronisieren ... 238
Tägliche Synchronisierung aller AD-Module aktivieren oder deaktivieren ... 239
Täglichen AD-Synchronisierungszeitpunkt ändern ... 239
Umbenennen und Verschieben von AD-Gruppen ... 240
LDAP und CC-SG ... 240
LDAP-Module (Netscape) zu CC-SG hinzufügen ... 240
Allgemeine LDAP-Einstellungen ... 241
Erweiterte LDAP-Einstellungen ... 242
Konfigurationseinstellungen für Sun One LDAP (iPlanet) ... 243
Konfigurationseinstellungen für OpenLDAP (eDirectory) ... 243
IBM LDAP-Konfigurationseinstellungen ... 244
TACACS+ und CC-SG ... 245
TACACS+-Module hinzufügen ... 245
Allgemeine TACACS+-Einstellungen ... 245
RADIUS und CC-SG ... 246
RADIUS-Module hinzufügen ... 246
Allgemeine RADIUS-Einstellungen ... 246
Zwei-Faktoren-Authentifizierung mit RADIUS ... 247

Kapitel 13 Berichte 248

Berichte verwenden ... 248
Berichtsdaten sortieren ... 248
Spaltenbreite in Berichten vergrößern/verkleinern ... 248
Berichtsdetails anzeigen ... 249
In mehrseitigen Berichten navigieren ... 249
Berichte drucken ... 249
Berichte in Dateien speichern ... 250
Berichtsdaten aus CC-SG leeren ... 250
Berichtsfilter ausblenden oder einblenden ... 250

Überwachungslistenbericht 251
Fehlerprotokollbericht 252
Zugriffsbericht 252
Verfügbarkeitsbericht 253
Bericht „Aktive Benutzer“ 254
Bericht "Gesperrte Benutzer" 254
Bericht "Alle Benutzerdaten" 254
Bericht "Benutzergruppendaten" 255
Geräteanlagenbericht 256
Bericht "Gerätegruppendaten" 256
Portabfragebericht 256
Knotenanlagebericht 258
Bericht „Aktive Knoten“ 259
Knotenerstellungsbericht 259
Bericht "Knotengruppendaten" 260
AD-Benutzergruppenbericht 260
Geplante Berichte 261
Bericht "Gerätefirmware aktualisieren" 262

Kapitel 14 Systemwartung 263

Wartungsmodus 263
Geplante Aufgaben und der Wartungsmodus 264
Wartungsmodus starten 264
Wartungsmodus beenden 264
CC-SG sichern 265
Worin besteht der Unterschied zwischen einer vollständigen und einer Standardsicherung? 267
Sicherungsdateien speichern und löschen 267
Sicherungsdateien speichern 267
Sicherungsdateien löschen 268
CC-SG wiederherstellen 268
CC-SG zurücksetzen 270
CC-SG neu starten 272
CC-SG aktualisieren 273
Browser-Cache löschen 275
Java-Cache löschen 275
Aktualisieren eines Clusters 276
Fehlgeschlagene Aktualisierung des primären Knotens 277
CC-SG-Datenbank migrieren 277
Migrationsvoraussetzungen 278
CC-SG-Datenbank migrieren 278
CC-SG herunterfahren (CC-SG Shutdown) 279
CC-SG nach dem Herunterfahren neu starten 279
CC-SG herunterfahren (Powering Down CC-SG) 280
CC-SG-Sitzung beenden 280
CC-SG verlassen 280
CC-SG beenden 281

Kapitel 15 Erweiterte Administration 282

Tipp des Tages konfigurieren 282
Anwendungen für den Zugriff auf Knoten konfigurieren 283
Anwendungen für den Zugriff auf Knoten 283
Anwendungsversionen prüfen und aktualisieren 283
Ältere Version der Anwendung öffnet sich nach Aktualisierung 284
Anwendungen hinzufügen 284
Anwendungen löschen 285
Voraussetzungen für die Verwendung des AKC 286
Standardanwendungen konfigurieren 286
Standardanwendungen 286
Zuordnungen der Standardanwendung anzeigen 286
Standardanwendung für Schnittstellen- oder Porttypen einstellen 287
Gerätefirmware verwalten 287
Upload 287
Firmware löschen 288
CC-SG-Netzwerk konfigurieren 288
Netzwerkeinrichtung 288
CC-SG-LAN-Ports 289
Was ist der IP-Ausfallsicherungsmodus? 290
Was ist der IP-Isolationsmodus? 292
Empfohlene DHCP-Konfigurationen für CC-SG 295
Protokollaktivitäten konfigurieren 295
Interne CC-SG-Protokolle leeren 296
CC-SG-Serverzeit und -datum konfigurieren 296
Verbindungsmodi: Direkt und Proxy 297
Verbindungsmodi 297
Direktmodus für alle Client-Verbindungen konfigurieren 298
Proxymodus für alle Client-Verbindungen konfigurieren 298
Kombination aus Direktmodus und Proxymodus konfigurieren 298
Geräteeinstellungen 299
Aktivieren der AKC-Download-Serverzertifikat-Validierung 300
Benutzerdefinierte JRE-Einstellungen konfigurieren 301
SNMP konfigurieren 303
MIB-Dateien 304
CC-SG-Cluster konfigurieren 304
Anforderungen für CC-SG-Cluster 305
Auf einen CC-SG-Cluster zugreifen 305
Cluster erstellen 305
Cluster-Einstellungen konfigurieren 307
Zwischen primärem und sekundärem Knotenstatus wechseln 307
Cluster wiederherstellen 308
Cluster löschen 309
Cluster aktualisieren 309
Clusterlizenzen 310
Netzwerkumgebung konfigurieren 311
Was ist eine Netzwerkumgebung? 311
Netzwerkumgebung erstellen 311
Netzwerkumgebung bearbeiten 313

Netzwerkumgebung aktualisieren 316
Netzwerkumgebung löschen 316
Sicherheitsmanager 316
Remoteauthentifizierung 316
AES-Verschlüsselung 316
Browser-Verbindungsprotokoll konfigurieren: HTTP oder HTTPS/SSL 318
Portnummer für SSH-Zugriff auf CC-SG einstellen 318
Anmeldeeinstellungen 319
Leerlaufzeitgeber konfigurieren 322
Portal 322
Zertifikate 324
Zugriffssteuerungsliste 327
Benachrichtigungsmanager 329
Externe SMTP-Server konfigurieren 329
Aufgabenmanager 330
Aufgabenarten 331
Aufeinander folgende Aufgaben planen 331
E-Mail-Benachrichtigungen für Aufgaben 331
Geplante Berichte 331
Aufgaben suchen und anzeigen 332
Aufgaben planen 332
Firmware-Aktualisierung für Geräte planen 335
Geplante Aufgaben ändern 337
Aufgaben neu planen 338
Aufgaben planen, die einer anderen Aufgabe ähneln 338
Aufgaben löschen 338
SSH-Zugriff auf CC-SG 339
Hilfe zu SSH-Befehlen erhalten 340
SSH-Befehle und Parameter 342
Tipps zu Befehlen 345
SSH-Verbindung zu einem seriellen Gerät herstellen 346
Verbindung zum Knoten mit SSH über serielle Out-of-Band-Schnittstelle herstellen 347
SSH-Verbindungen beenden 348
Serieller Administrationsport 349
Terminalemulationsprogramme 350
CC-SG-Seriennummer auffinden 350
Web Services-API 350
CC-NOC 352

Kapitel 16 Diagnosekonsole 353

Auf die Diagnosekonsole zugreifen 353
Auf die Diagnosekonsole über VGA-/Tastatur-/Mausport zugreifen 353
Über SSH auf die Diagnosekonsole zugreifen 353
Statuskonsole 354
Die Statuskonsole 354
Auf die Statuskonsole zugreifen 354
Statuskonsoleninformationen 356
Administratorkonsole 361
Die Administratorkonsole 361
Auf die Administratorkonsole zugreifen 361

Die Administratorkonsole navigieren 363
Konfiguration der Diagnosekonsole bearbeiten 364
Netzwerkschnittstellenkonfiguration bearbeiten (Network Interfaces) 365
IP-Adresse anpingen 367
Traceroute verwenden 368
Static Routes bearbeiten 369
Protokolldateien in der Diagnosekonsole anzeigen 371
CC-SG mit der Diagnosekonsole neu starten 375
CC-SG mit der Diagnosekonsole neu hochfahren 376
CC-SG-System über die Diagnosekonsole ausschalten 377
Kennwort des CC-Superusers mit der Diagnosekonsole zurücksetzen 378
Werksseitig eingestellte Konfiguration von CC-SG wiederherstellen 379
Kennworteinstellungen der Diagnosekonsole 381
Konfiguration des Diagnosekonsolen-Kontos 383
Überwachung des Remotesystems konfigurieren 385
Berichte zu Historical Data Trending (Trendermittlung für Datenhistorie) anzeigen 386
RAID-Status und Laufwerksauslastung anzeigen 387
Laufwerk- oder RAID-Tests ausführen 388
Laufwerktests planen 390
Repair (Reparieren) oder Rebuild (Wiederherstellen) von RAID-Laufwerken 392
Top Display mit der Diagnosekonsole anzeigen 393
NTP-Status anzeigen 394
Systemschnappschuss aufnehmen 396
Videoauflösung für Diagnosekonsole ändern 397

Kapitel 17 Integration von Power IQ 399

Stromversorgungssteuerung von Power IQ-IT-Geräten 399
Power IQ-Dienste konfigurieren 400
Stromversorgungssteuerung von Power IQ-IT-Geräten konfigurieren 402
Konfigurieren der Synchronisierung von Power IQ und CC-SG 403
Synchronisierung von Power IQ und CC-SG 404
Power IQ-Synchronisierungsrichtlinien 405
Dominion PX-Daten von Power IQ importieren und exportieren 406
Powerstrips aus Power IQ importieren 406
Dominion PX-Daten zur Verwendung in Power IQ exportieren 408

Anhang A Technische Daten für V1 und E1 409

V1-Modell 409
V1 – Allgemeine technische Daten 409
V1 – Umgebungsanforderungen 409
E1-Modell 410
E1 – Allgemeine technische Daten 410
E1 – Umgebungsanforderungen 410

Anhang B CC-SG und Netzwerkkonfiguration 412

Erforderliche geöffnete Ports für CC-SG-Netzwerke: Übersicht 412
CC-SG-Kommunikationskanäle 414
CC-SG und Raritan-Geräte 414
CC-SG Clustering 415
Zugriff auf Infrastrukturdienste 416
Verbindung von PC-Clients mit CC-SG 416
Verbindung von PC-Clients mit Knoten 417
CC-SG und Client für IPMI, iLO/RILOE, DRAC, RSA 418
CC-SG und SNMP 418
Interne CC-SG-Ports 419
CC-SG-Zugriff über NAT-fähige Firewall 419
RDP-Zugriff auf Knoten 420
VNC-Zugriff auf Knoten 420
SSH-Zugriff auf Knoten 420
Port für die Überwachung des Remotesystems 420

Anhang C Benutzergruppenberechtigungen 421

Anhang D SNMP-Traps 431

Anhang E CSV-Dateiimporte 433

Häufige Anforderungen für CSV-Dateien 434
Einträge in der Überwachungsliste für Importe 435
Problembehebung bei CSV-Dateien 436

Anhang F Problembehandlung 437

Anhang G Diagnoseprogramme 439

Speicherdiagnose 439
Debug-Modus 440
CC-SG-Laufwerksüberwachung 441

Anhang H Zwei-Faktoren-Authentifizierung 444

Unterstützte Umgebungen für die Zwei-Faktoren-Authentifizierung 444
Setupanforderungen für die Zwei-Faktoren-Authentifizierung 444
Bekannte Probleme bei der Zwei-Faktoren-Authentifizierung 445

Anhang I Häufig gestellte Fragen (FAQs) 446

Allgemeine häufig gestellte Fragen (FAQs) 446
Häufig gestellte Fragen (FAQs) zur Authentifizierung 449
Häufig gestellte Fragen (FAQs) zur Sicherheit 449
Häufig gestellte Fragen (FAQs) zu Konten 451
Häufig gestellte Fragen (FAQs) zur Leistung 451
Häufig gestellte Fragen (FAQs) zu Gruppen 452
Häufig gestellte Fragen (FAQs) zur Interoperabilität 453
Häufig gestellte Fragen (FAQs) zur Autorisierung 453
Häufig gestellte Fragen (FAQs) zur Benutzerfreundlichkeit 453
Häufig gestellte Fragen zur Lizenzierung 455

Anhang J Tastenkombinationen 456

Anhang K Benennungsregeln 457

Neuerungen im CC-SG Handbuch für Administratoren

Benutzerinformationen 457
Knoteninformationen 457
Standortinformationen 458
Kontaktinformationen 458
Dienstkonten 458
Geräteinformationen 458
Portinformationen 459
Zuordnungen 459
Administration 459

Anhang L Startmeldungen der Diagnosekonsole 461

Index 463

Die folgenden Abschnitte im CommandCenter Secure Gateway Handbuch für Administratoren wurden auf der Grundlage von Verbesserungen und Änderungen am Gerät und/oder an der Dokumentation geändert oder um Informationen erweitert.

- ***Lizenz hinzufügen*** (auf Seite 34)
- ***Geräteverwaltung mit einer geplanten Aufgabe unterbrechen und fortsetzen*** (auf Seite 107)
- ***Einzelheiten zur IBM IMM-Modulverbindung*** (auf Seite 156)
- ***Richtlinien Benutzergruppen zuordnen*** (auf Seite 215)
- ***Aktualisieren eines Clusters*** (auf Seite 276)
- ***Fehlgeschlagene Aktualisierung des primären Knotens*** (auf Seite 277)
- ***CC-SG-Datenbank migrieren*** (auf Seite 277)
- ***Migrationsvoraussetzungen*** (auf Seite 278)
- ***CC-SG-Datenbank migrieren*** (auf Seite 278)
- ***Clusterlizenzen*** (auf Seite 310)
- ***Häufig gestellte Fragen zur Lizenzierung*** (auf Seite 455)

Ausführlichere Informationen zu den Änderungen in dieser CommandCenter Secure Gateway-Version finden Sie in den Versionshinweisen.

Kapitel 1 Einleitung

Das CommandCenter Secure Gateway (CC-SG) Handbuch für Administratoren bietet Anleitungen für die Verwaltung und Wartung von CC-SG.

Dieses Handbuch richtet sich an Administratoren, die über alle verfügbaren Berechtigungen verfügen.

Benutzer, die keine Administratoren sind, finden weitere Informationen im **CommandCenter Secure Gateway-Benutzerhandbuch** von Raritan.

In diesem Kapitel

Vorbereitungen 1
Terminologie/Abkürzungen.....2
Clientbrowser-Anforderungen 4

Vorbereitungen

Bevor Sie CC-SG nach den Anweisungen in diesem Dokument konfigurieren können, lesen Sie das Handbuch **CommandCenter Secure Gateway – Implementierungshandbuch** von Raritan. Es enthält umfangreiche Anweisungen zur Implementierung von Raritan-Geräten, die von CC-SG verwaltet werden.

Terminologie/Abkürzungen

Im vorliegenden Handbuch werden folgende Begriffe und Abkürzungen verwendet:

Zugriffs-Client: Ein auf HTML basierender Client zur Verwendung durch Benutzer mit normalen Zugriffsrechten, die auf einen von CC-SG verwalteten Knoten zugreifen müssen. Der Zugriffs-Client bietet keine Verwaltungsfunktionen.

Administrations-Client: Ein auf Java basierender Client für CC-SG, der von Benutzern mit normalem Zugriff und Administratoren verwendet werden kann. Die Verwaltung ist nur mit diesem Client möglich.

Zuordnungen: Beziehungen zwischen Kategorien und Kategorieelementen zu Ports und/oder Geräten. Wenn beispielsweise einem Gerät die Kategorie "Standort"zugeordnet werden soll, erstellen Sie die Zuordnungen, bevor Sie in CC-SG Geräte und Ports hinzufügen.

Kategorie: Eine Variable, die bestimmte Werte oder Elemente enthält. "Standort" ist beispielsweise eine Kategorie, die Elemente wie "New York City", "Philadelphia" oder "Data Center 1" enthält. Wenn Sie in CC-SG Geräte und Ports hinzufügen, werden diese Informationen entsprechend zugewiesen. Es ist einfacher, zuerst die Zuordnungen richtig einzurichten und dann Geräte und Ports hinzuzufügen. "Betriebssystemtyp" ist eine weitere Kategorie, die Elemente wie "Windows", "Unix" oder "Linux" enthalten kann.

CIM (Computer Interface Module): Die Hardware, die zur Verbindung eines Zielservers mit einem Raritan-Gerät verwendet wird. Für jedes Ziel ist ein CIM erforderlich. Eine Ausnahme bildet dabei das Dominion KX101-Gerät, das direkt mit einem Ziel verbunden wird und daher kein CIM erfordert. VOR dem Hinzufügen des Gerätes und der Konfigurationsports in CC-SG sollten die Zielserver eingeschaltet und mit den CIMs verbunden worden sein, die ihrerseits mit dem Raritan-Gerät verbunden sein sollten. Andernfalls wird der Portname in CC-SG durch den leeren CIM-Namen überschrieben. Nach der Verbindung mit einem CIM müssen die Server neu hochgefahren werden.

Gerätegruppe: Definierte Gruppe von Geräten, auf die ein Benutzer zugreifen kann. Gerätegruppen werden beim Erstellen von Richtlinien für die Zugriffssteuerung für Geräte in der Gruppe verwendet.

Geräte: Raritan-Produkte wie Dominion KX, Dominion KX II, Dominion SX, Dominion KSX, IP-Reach, Paragon II Systemcontroller und Paragon II UMT832 mit USTIP usw., die von CC-SG verwaltet werden. Diese Geräte steuern die mit ihnen verbundenen Zielserver und -systeme oder „Knoten“. Überprüfen Sie die CC-SG-Kompatibilitätsmatrix auf der Support-Website von Raritan auf eine Liste der unterstützten Geräte.

Elemente: Werte einer Kategorie. Das Element "New York City" gehört beispielsweise zur Kategorie "Standort", und das Element "Windows" gehört zur Kategorie "Betriebssystemtyp".

Verwaiste Ports: Bei der Verwaltung von Paragon-Geräten kann ein verwaister Port bei Entfernung eines CIMs oder Zielservers aus dem System und bei der Abschaltung eines Zielservers (manuell oder unbeabsichtigt) entstehen. Siehe **Benutzerhandbuch für Paragon II-Geräte von Raritan**.

Hostname: Ein Hostname kann verwendet werden, wenn die DNS-Serverunterstützung aktiviert ist. Weitere Informationen finden Sie unter ***Netzwerkeinrichtung*** (auf Seite 288).

Der Hostname und der vollständig qualifizierte Domänenname (Hostname + Suffix) dürfen nicht mehr als 257 Zeichen umfassen. Er kann aus einer beliebigen Anzahl an Komponenten bestehen, solange diese durch einen Punkt (.) voneinander getrennt sind.

Die einzelnen Komponenten dürfen aus maximal 63 Zeichen bestehen, wobei das erste Zeichen ein Buchstabe sein muss. Die übrigen Zeichen können alphabetisch, numerisch oder das Trenn- bzw. Minuszeichen ("-") sein.

Trenn- bzw. Minuszeichen dürfen jedoch nicht an letzter Stelle einer Komponentenbezeichnung stehen.

Obwohl das System bei der Eingabe der Zeichen die Groß-/Kleinschreibung beibehält, spielt die Groß-/Kleinschreibung bei der Verwendung des vollständig qualifizierten Domänennamens keine Rolle.

iLO/RILOE und iLO2/RILOE2: Integrated Lights Out/Remote Insight Lights Out Edition von Hewlett Packard für Server, die von CC-SG verwaltet werden können. Ziele eines iLO/RILOE-Geräts werden direkt ein- und ausgeschaltet bzw. aktiviert und deaktiviert. iLO/RILOE-Geräte werden nicht von CC-SG erkannt, sondern müssen manuell als Knoten hinzugefügt werden. In diesem Handbuch bezieht sich der Begriff iLO/RILOE sowohl auf iLO/RILOE als auch auf iLO2/RILOE2.

In-Band-Zugriff: Korrekturen oder Problembehandlungen bei einem Ziel im Netzwerk erfolgen über das TCP/IP-Netzwerk. Über die folgenden In-Band-Anwendungen können Sie auf KVM- und serielle Geräte zugreifen: RemoteDesktop Viewer, SSH Client, RSA Client, VNC Viewer.

IPMI-Server (Intelligent Platform Management Interface): Server, die von CC-SG gesteuert werden können. IPMI werden automatisch erkannt, können jedoch auch manuell hinzugefügt werden.

Out-of-Band-Zugriff: Korrekturen oder Problembehebungen bei einem KVM- oder einem seriellen verwalteten Knoten im Netzwerk erfolgen über Anwendungen wie Raritan Remote Console (RRC), RaritanConsole (RC), Multi-Platform Client (MPC), Virtual KVM Client (VKC) oder Active KVM Client (AKC).

Richtlinien: Definieren den Zugriff einer Benutzergruppe innerhalb des CC-SG-Netzwerks. Richtlinien werden einer Benutzergruppe zugewiesen und enthalten verschiedene Parameter zur Festlegung der Steuerungsebene wie Datum und Uhrzeit des Zugriffs.

Knoten: Zielsysteme wie Server, Desktop-PCs und andere Netzwerkgeräte, auf die CC-SG-Benutzer zugreifen können.

Schnittstellen: Die verschiedenen Arten des Zugriffs auf Knoten, entweder über eine Out-of-Band-Lösung wie eine Dominion KX101-Verbindung oder eine In-Band-Lösung wie einen VNC-Server.

Knotengruppe: Definierte Gruppe von Knoten, auf die ein Benutzer zugreifen kann. Knotengruppen werden beim Erstellen von Richtlinien für die Zugriffssteuerung für Knoten in der Gruppe verwendet.

Ports: Verbindungspunkte zwischen einem Raritan-Gerät und einem Knoten. Ports bestehen nur für Raritan-Geräte und kennzeichnen einen Pfad von dem Gerät zu einem Knoten.

SASL (Simple Authentication and Security Layer): Methode zum Hinzufügen von Authentifizierungsunterstützung für verbindungsgestützte Protokolle.

SSH: Clients, wie beispielsweise PuTTY oder OpenSSH, stellen CC-SG eine Befehlszeilenschnittstelle zur Verfügung. Nur ein Teil der CC-SG-Befehle zur Verwaltung von Geräten und CC-SG wird über SSH ausgegeben.

Benutzergruppen**: Mehrere Benutzer mit der gleichen Zugriffsebene und den gleichen Berechtigungen.**

Clientbrowser-Anforderungen

Eine vollständige Liste der unterstützten Browser finden Sie in der Kompatibilitätsmatrix auf der Support-Website von Raritan.

Kapitel 2 Zugreifen auf CC-SG

Sie haben mehrere Möglichkeiten für den Zugriff auf CC-SG:

- Browser: CC-SG unterstützt verschiedene Webbrowser. (Eine vollständige Liste der unterstützten Browser finden Sie in der Kompatibilitätsmatrix auf der Support-Website von Raritan.)
- Thick-Client Sie können einen Java Web Start Thick-Client auf Ihrem Client-Computer installieren. Der Thick-Client funktioniert wie ein browserbasierter Client.
- SSH: Sie können auf Remotegeräte, die über den seriellen Port angeschlossen sind, über SSH zugreifen.
- Diagnosekonsole: Diese Konsole wird nur bei Problembehandlungen und für die Diagnose in Notfällen verwendet und stellt keinen Ersatz für die browserbasierte Benutzeroberfläche zum Konfigurieren und Betreiben der CC-SG-Einheit dar. Siehe ***Diagnosekonsole*** (auf Seite 353).

Hinweis: Die Benutzer können während des Zugriffs auf CC-SG mit dem Browser, Thick-Client und SSH gleichzeitig verbunden sein.

In diesem Kapitel

Browserbasierter Zugriff über CC-SG-Administrations-Client.....5
Thick-Client-Zugriff 6
CC-SG-Administrations-Client.....8

Browserbasierter Zugriff über CC-SG-Administrations-Client

Mit der Benutzeroberfläche des auf Java basierenden CC-SG-Administrations-Clients können Sie je nach Ihren Berechtigungen Administrations- und Zugriffsaufgaben ausführen.

1. Verwenden Sie einen unterstützten Internetbrowser, und geben Sie den URL des CC-SG und dann /admin ein: http(s)://*IP-Adresse*/admin, z. B. ***http://10.0.3.30/admin*** (***https://10.0.3.30/admin***) oder https://10.0.3.30/admin.

   Wenn das Fenster "Warnhinweis zur JRE-Inkompatibilität" angezeigt wird, wählen Sie die für Ihren Client-Computer geeignete JRE-Version aus und installieren sie. Nachdem JRE installiert wurde, führen Sie diesen Vorgang noch einmal aus. Siehe **JRE-Inkompatibilität** *(auf Seite 6).*

   Sie können auch fortfahren, ohne eine neue JRE-Version zu installieren.

2. Wenn vertragliche Einschränkungen der Serviceleistungen angezeigt werden, lesen Sie den Text, und aktivieren Sie das Kontrollkästchen "Ich stimme den Vertragsbedingungen zu".
3. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein, und klicken Sie auf "Anmelden".
4. Nach der Anmeldung wird der CC-SG-Administrations-Client angezeigt.

JRE-Inkompatibilität

Wenn nicht die erforderliche JRE-Mindestversion auf dem Client-Computer installiert ist, wird vor dem Zugriff auf den CC-SG-Administrations-Client eine Warnung angezeigt. Das Fenster "Warnhinweis zur JRE-Inkompatibilität" wird geöffnet, wenn CC-SG nicht die erforderliche JRE-Datei auf dem Client-Computer findet.

Wenn das Fenster "Warnhinweis zur JRE-Inkompatibilität" angezeigt wird, wählen Sie die für Ihren Client-Computer geeignete JRE-Version aus, und installieren Sie sie. Sie können auch fortfahren, ohne eine neue JRE-Version zu installieren.

Sie müssen CC-SG neu starten, nachdem JRE installiert wurde.

Administratoren können die empfohlene JRE-Mindestversion und die Meldung konfigurieren, die im Fenster "Warnhinweis zur JRE-Inkompatibilität" angezeigt wird. Siehe ***Benutzerdefinierte JRE-Einstellungen konfigurieren*** (auf Seite 301).

Thick-Client-Zugriff

Anstatt ein Applet über einen Webbrowser auszuführen, startet der CC-SG-Thick-Client eine Java Web Start-Anwendung, um eine Verbindung mit CC-SG herzustellen. Der Thick-Client kann schneller sein als ein Browser. Die erforderliche Java-Mindestversion für das Ausführen des Thick-Clients ist 1.6.0.10.

Thick-Client installieren

So laden Sie den Thick-Client von CC-SG herunter:

Hinweis: Wenn Sie JRE Version 1.6.0_20 verwenden, vergewissern Sie sich, dass "Keep temporary files on my computer" (Temporäre Dateien auf dem Computer behalten) auf der Registerkarte "Temporäre Internetdateien" unter "Java Control Panel" (Java-Systemsteuerung) aktiviert ist. Ohne diese Einstellung kann der Client nicht gestartet werden, und es wird die folgende Meldung angezeigt: "Unable to launch application" (Anwendung kann nicht gestartet werden).

1. Starten Sie einen Webbrowser, und geben Sie diesen URL ein: `http(s)://<IP-Adresse>/install` wobei `<IP-Adresse>` für die IP-Adresse von CC-SG steht.
   - Wenn eine Sicherheitswarnung angezeigt wird, klicken Sie auf "Start", um das Herunterladen fortzusetzen.
2. Nach dem Herunterladen wird ein neues Fenster angezeigt, in dem Sie die IP-Adresse von CC-SG angeben können.
3. Geben Sie im Feld "Zu verbindende IP-Adresse" die IP-Adresse der CC-SG-Einheit ein, auf die Sie zugreifen möchten. Nachdem eine Verbindung aufgebaut wurde, steht diese Adresse in der Dropdown-Liste "Zu verbindende IP-Adresse" zur Verfügung. Die IP-Adressen werden in einer Eigenschaftendatei auf Ihrem Desktop gespeichert.
4. Wenn CC-SG für sichere Browserverbindungen konfiguriert ist, müssen Sie das Kontrollkästchen "Secure Socket Layer (SSL)" aktivieren. Ist CC-SG nicht für sichere Browserverbindungen konfiguriert, müssen Sie das Kontrollkästchen "Secure Socket Layer (SSL)" deaktivieren. Diese Einstellung muss richtig sein, damit der Thick-Client eine Verbindung zu CC-SG herstellen kann.
   - So prüfen Sie die Einstellungen in CC-SG: Wählen Sie "Administration > Sicherheit". Sehen Sie sich auf der Registerkarte "Verschlüsselung" das Feld "Browser-Verbindungsprotokoll" an. Wenn die Option "HTTPS/SSL" ausgewählt ist, müssen Sie das Kontrollkästchen "Secure Socket Layer SSL" im Fenster zur Eingabe der IP-Adresse des Thick-Clients aktivieren. Wenn die Option "HTTP" ausgewählt ist, deaktivieren Sie das Kontrollkästchen "Secure Socket Layer SSL" im Fenster zur Eingabe der IP-Adresse des Thick-Clients.
5. Klicken Sie auf Start.
   - Wenn Sie eine nicht unterstützte Version der Java Runtime Environment auf Ihrem Computer verwenden, werden Sie durch eine Warnung darauf hingewiesen. Laden Sie entweder eine unterstützte Java-Version herunter, oder fahren Sie mit der installierten Version fort.

6. Das Anmeldefenster wird angezeigt.
7. Sind die vertraglichen Einschränkungen der Serviceleistungen aktiviert, lesen Sie den Text und markieren Sie das Kontrollkästchen "Ich stimme den Vertragsbedingungen zu".
8. Geben Sie Ihren Benutzernamen und Ihr Kennwort in die entsprechenden Felder ein, und klicken Sie zum Fortfahren auf Anmelden.

Thick-Client verwenden

Die erforderliche Java-Mindestversion für das Ausführen des Thick-Clients ist 1.6.0.10.

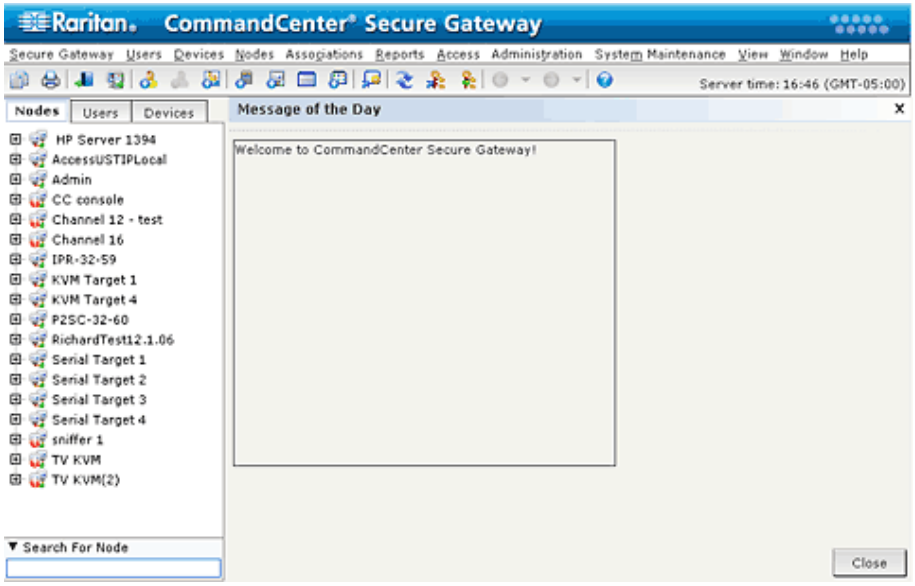
Nachdem der Thick-Client installiert wurde, haben Sie zwei Möglichkeiten, über Ihren Client-Computer darauf zuzugreifen.

So greifen Sie auf den Thick-Client zu:

- in der Java-Systemsteuerung den Thick-Client über Java Application Cache Viewer starten.
- in der Java-Systemsteuerung über Java Application Cache Viewer ein Desktop-Symbol für den Thick-Client installieren.

CC-SG-Administrations-Client

Nach der Anmeldung wird der CC-SG-Administrations-Client angezeigt.



- Registerkarte Knoten: Klicken Sie auf die Registerkarte Knoten, um alle bekannten Zielknoten in einer Strukturansicht anzuzeigen. Klicken Sie auf einen Knoten, um das Knotenprofil anzuzeigen. Schnittstellen sind unter den übergeordneten Knoten zusammengefasst. Klicken Sie auf das Plus- oder Minuszeichen (+ oder -), um die Struktur ein- oder auszublenden. Klicken Sie mit der rechten Maustaste auf eine Schnittstelle, und wählen Sie Verbinden aus, um eine Verbindung mit dieser Schnittstelle herzustellen. Sie können die Knoten nach Knotennamen (alphabetisch) oder Knotenstatus (Verfügbar, Beschäftigt, Nicht verfügbar) sortieren. Klicken Sie mit der rechten Maustaste auf die Strukturansicht, klicken Sie auf "Knotensortieroptionen" und dann auf "Nach Knotenname" oder "Nach Knotenstatus".
- Registerkarte Benutzer: Klicken Sie auf die Registerkarte "Benutzer", um eine Strukturansicht aller registrierten Benutzer und Gruppen anzuzeigen. Klicken Sie auf das Plus- oder Minuszeichen (+ oder -), um die Struktur ein- oder auszublenden.
- Registerkarte Geräte: Klicken Sie auf die Registerkarte "Geräte", um eine Strukturansicht aller bekannten Raritan-Geräte anzuzeigen. Die einzelnen Gerätetypen sind durch unterschiedliche Symbole dargestellt. Ports sind unter den übergeordneten Geräten zusammengefasst. Klicken Sie auf das Plus- oder Minuszeichen (+ oder -), um die Struktur ein- oder auszublenden. Klicken Sie auf einen Port, um das Portprofil anzuzeigen. Klicken Sie mit der rechten Maustaste auf einen Port, und wählen Sie Verbinden aus, um eine Verbindung mit diesem Port herzustellen. Sie können die Ports nach Portnamen (alphabetisch), Portstatus (Verfügbar, Beschäftigt, Nicht verfügbar) oder nach Portnummer (numerisch) sortieren. Klicken Sie mit der rechten Maustaste auf die Strukturansicht, klicken Sie auf "Portsortieroptionen" und dann auf "Nach Portname" oder "Nach Portstatus".
- Symbolleiste mit Kurzbefehlen: Diese Symbolleiste enthält Schaltflächen zum Ausführen der am häufigsten benötigten Befehle.
- Menüleiste für den Betrieb und zur Konfiguration: Diese Menüs enthalten Befehle zum Bedienen und Konfigurieren von CC-SG. Sie können einige dieser Befehle ausführen, indem Sie mit der rechten Maustaste auf die Symbole auf den Registerkarten "Knoten", "Benutzer" und "Geräte" klicken. Die angezeigten Menüs und Menüelemente basieren auf Ihren Benutzerzugriffsberechtigungen.
- Serverzeit: Aktuelle Uhrzeit und Zeitzone, die für CC-SG im Konfigurationsmanager konfiguriert wurde. Diese Uhrzeit wird zum Planen von Aufgaben im Aufgabenmanager verwendet. Weitere Informationen finden Sie unter ***Aufgabenmanager*** (auf Seite 330). Diese Uhrzeit unterscheidet sich eventuell von der auf Ihrem Client-PC verwendeten Uhrzeit.

Kapitel 3 Erste Schritte

Bevor Sie mit der Konfiguration und Arbeit in CC-SG beginnen können, müssen gültige Lizenzen installiert sein. Nach der ersten Anmeldung sollten Sie die IP-Adresse bestätigen, die CC-SG-Serverzeit einstellen und die installierten Firmware- und Anwendungsversionen überprüfen. Sie müssen die Firmware und Anwendungen ggf. aktualisieren.

Nach Abschluss der Erstkonfigurationen fahren Sie mit dem Setup-Assistenten fort. Siehe ***Konfigurieren von CC-SG mit dem Setup-Assistenten*** (auf Seite 39).

In diesem Kapitel

Lizenzierung – Erste Schritte – Neue und bestehende Kunden 10
Lizenzierung – Grundlegende Lizenzinformationen 11
Lizenzierung – Neue Kunden – Physische Appliance 14
Lizenzierung – Virtuelle Appliance mit Lizenzserver 18
Lizenzierung – Beschränkter Betrieb vor der Lizenzinstallation.....31
Lizenzierung – Bestehende Kunden 33
Lizenzierung – Rehosting 34
Lizenz hinzufügen.....34
IP-Adresse bestätigen 35
CC-SG-Serverzeit festlegen 35
Kompatibilitätsmatrix überprüfen 36
Anwendungsversionen prüfen und aktualisieren 37

Lizenzierung – Erste Schritte – Neue und bestehende Kunden

Raritan führt mit CC-SG 5.0 eine neue Lizenzierungstechnologie ein.

Sie müssen gültige Lizenzen installiert haben, bevor Sie CC-SG 5.0 nutzen können. Sind noch keine Lizenzen installiert, erlaubt CC-SG nur den Zugriff auf beschränkte Funktionen. Siehe ***Lizenzierung – Beschränkter Betrieb vor der Lizenzinstallation*** (auf Seite 31).

So beginnen Sie mit der Lizenzierung:

Wenn Sie ein neuer CC-SG-Kunde mit einer physischen Appliance sind, lesen Sie ***Lizenzierung – Neue Kunden – Physische Appliance*** (auf Seite 14).

Wenn Sie ein neuer CC-SG-Kunde mit einer virtuellen Appliance sind, lesen Sie ***Lizenzierung – Virtuelle Appliance mit Lizenzserver*** (auf Seite 18).

Wenn Sie ein bestehender Kunde sind, der eine Aktualisierung auf CC-SG 5.0 durchführt, lesen Sie ***Lizenzierung – Bestehende Kunden*** (auf Seite 33).

Lizenzierung – Grundlegende Lizenzinformationen

Die Lizenzen basieren auf der Anzahl der Knoten, die in CC-SG konfiguriert sind.

Mit dem Kauf einer physischen oder virtuellen Appliance erhalten Sie eine Lizenz für die Nutzung einer bestimmten Anzahl von Knoten. Diese "Basislizenz" aktiviert die CC-SG-Funktionen und beinhaltet eine Lizenzierung für die entsprechende Anzahl an Knoten. Wenn Sie mehr Knoten benötigen, müssen Sie auch eine Add-On-Lizenz für zusätzliche Knoten erwerben. Wenn Sie die WS-API-Funktion nutzen möchten, müssen Sie auch eine Add-On-Lizenz für den WS-API-Zugriff erwerben.

Lizenzdateien für physische Appliances sind mit einer Host-ID für eine bestimmte CC-SG-Einheit verknüpft.

Lizenzdateien für virtuelle Appliances sind mit einer Host-ID für einen bestimmten Lizenzserver verknüpft.

Das bedeutet, dass Lizenzdateien nicht übertragbar sind.

- Wenn Sie ein neuer Kunde mit einer physischen Appliance sind, laden Sie Ihre Lizenzdateien von der Raritan-Lizenzierungs-Website herunter. Siehe ***Lizenzierung – Neue Kunden – Physische Appliance*** (auf Seite 14).
- Wenn Sie bereits im Besitz einer älteren Version als Version 5.0 sind, brauchen Sie keine Lizenzdateien herunterzuladen. Wenn eine ältere CC-SG-Einheit auf Version 5.0 oder höher aktualisiert wird, werden die Lizenzen in das neue Format konvertiert. Eine neue Basislizenz und zugehörige Add-On-Lizenzen werden erstellt, automatisch installiert und ggf. ausgecheckt, um Ihrer aktuellen Konfiguration zu entsprechen. Siehe ***Lizenzierung – Bestehende Kunden*** (auf Seite 33).
- Wenn Sie Kunde mit einer virtuellen Appliance sind, müssen Sie einen Lizenzserver implementieren. Siehe ***Lizenzierung – Virtuelle Appliance mit Lizenzserver*** (auf Seite 18).

Verfügbare Lizenzen

CC-SG-Produkt	Beschreibung	Benötigte Informationen für das erstmalige Erstellen einer Lizenz
CC-E1-128	CC-SG E1-Appliance, enthält Lizenz für 128 Knoten	Host-ID der CC-SG-Einheit
CC-E1-256	CC-SG E1-Appliance, enthält Lizenz für 256 Knoten	Host-ID der CC-SG-Einheit
CC-E1-512	CC-SG E1-Appliance, enthält Lizenz für 512 Knoten	Host-ID der CC-SG-Einheit

CC-SG-Produkt	Beschreibung	Benötigte Informationen für das erstmalige Erstellen einer Lizenz
CC-V1-128	CC-SG V1-Appliance, enthält Lizenz für 128 Knoten	Host-ID der CC-SG-Einheit
CC-V1-256	CC-SG V1-Appliance, enthält Lizenz für 256 Knoten	Host-ID der CC-SG-Einheit
CCSG128-VA	Virtuelle CC-SG-Appliance enthält Lizenz für 128 Knoten	▪ Host-ID des Windows- oder Linux-Lizenzservers ▪ Hostname oder IP-Adresse des Windows- oder Linux-Lizenzservers
CC-2XE1-512	Cluster-Kit: 2 CC-SG E1-Appliances, enthält Lizenz für 512 Knoten	Host-IDs jeder CC-SG-Einheit im Cluster
CC-2XE1-1024	Cluster-Kit: 2 CC-SG E1-Appliances, enthält Lizenz für 1024 Knoten	Host-IDs jeder CC-SG-Einheit im Cluster
CC-2XV1-256	Cluster-Kit: 2 CC-SG V1-Appliances, enthält Lizenz für 256 Knoten	Host-IDs jeder CC-SG-Einheit im Cluster
Add-On-Lizenzen	Lizenzen für zusätzliche Knoten und Mehrwertdienste, wie z. B. WS-API.	Host-ID der CC-SG-Einheit

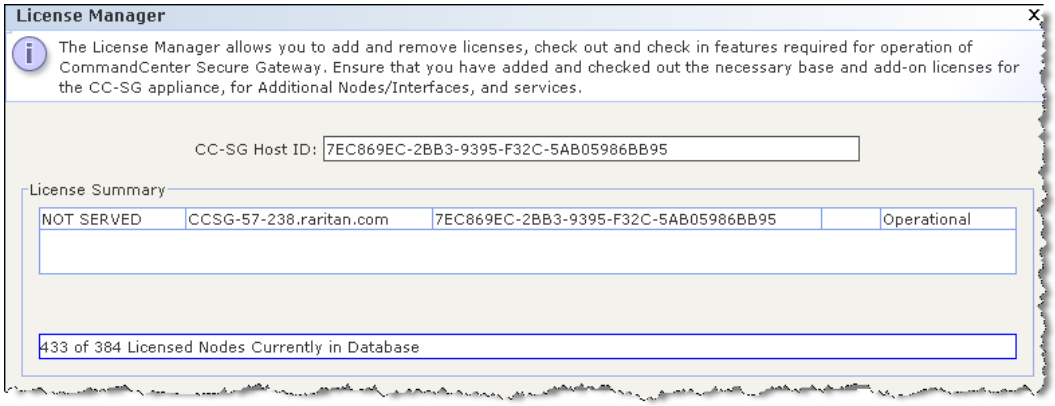
Auffinden der Host-ID Ihrer physischen Appliance und Überprüfen der Anzahl der Knoten in der Datenbank

Die Seite "Lizenzmanager" enthält Informationen über Ihre Lizenzen, einschließlich der Anzahl der derzeit in Ihrer Datenbank vorhandenen lizenzierten Knoten. Sie können die Host-ID der physischen Appliance von der Seite "License Management" (Lizenzverwaltung) abrufen. Sie müssen die Host-ID vom <Produktname> eingeben, wenn Sie eine Lizenzdatei im Raritan Licensing Portal (Raritan-Lizenzierungsportal) erstellen. Im Abschnitt ***Lizenzierung – Neue Kunden – Physische Appliance*** (auf Seite 14) erhalten Sie Informationen zum Erhalt der neuen Lizenzdateien.

Wenn Sie ein virtuelle Appliance besitzen, finden Sie im Abschnitt ***Erhalt Ihrer Lizenz*** (auf Seite 21) Informationen zum Abrufen der Host-ID für Ihren Lizenzserver.

So zeigen Sie die Host-ID an und überprüfen die Anzahl der Knoten in der Datenbank:

1. Wählen Sie "Administration > License Management (Lizenzverwaltung)".
2. Die Host-ID der <Produktname>-Einheit, bei der Sie angemeldet sind, wird auf der Seite "License Management" (Lizenzverwaltung) angezeigt. Sie können die Host-ID kopieren und einfügen. Für virtuelle CC-SG-Einheiten wird die Host-ID nach Installation des Lizenzservers im Abschnitt "License Summary" (Lizenzübersicht) angezeigt. Zwischen der Seite "Lizenzmanager" für physische Appliances und der entsprechenden Seite für virtuelle Appliances bestehen geringfügige Unterschiede.
3. Überprüfen Sie auf dieser Seite die Anzahl der Knoten in Ihrer Datenbank. Sie können feststellen, wie viele weitere Knoten Sie noch hinzufügen können, bis das lizenzierte Limit erreicht ist.

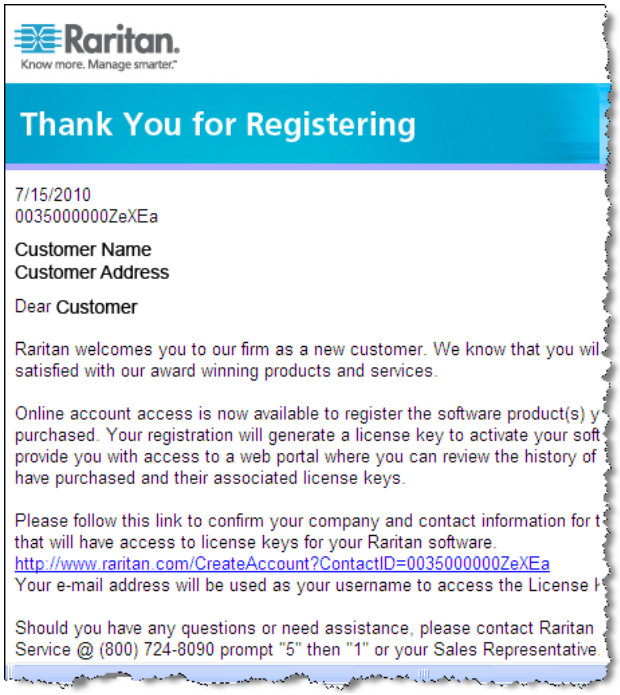


Lizenzierung – Neue Kunden – Physische Appliance

Wenn Sie ein neuer Kunde sind und gerade eine physische CC-SG 5.0-Appliance erworben haben, stellen Sie anhand der folgenden Anweisungen sicher, dass Sie gültige Lizenzen installiert und aktiviert haben.

Schritt 1 – Erhalt der Lizenz:

1. Der beim Kauf angegebene Lizenzadministrator erhält eine E-Mail vom Raritan Licensing Portal (Raritan-Lizenzierungsportal) mit dem Absender "licensing@raritan.com" und dem Betreff "Thank You for Registering" (Vielen Dank für Ihre Registrierung).


Raritan.
Know more. Manage smarter.

Thank You for Registering

7/15/2010
0035000000ZeXEa

Customer Name
Customer Address

Dear Customer

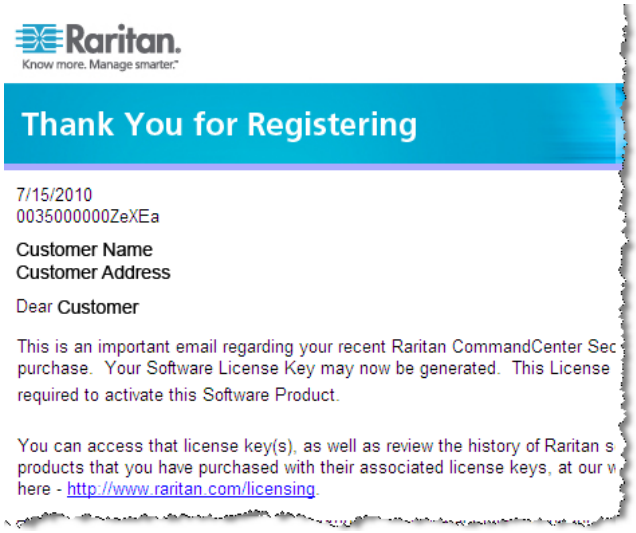
Raritan welcomes you to our firm as a new customer. We know that you wil
satisfied with our award winning products and services.

Online account access is now available to register the software product(s) y
purchased. Your registration will generate a license key to activate your soft
provide you with access to a web portal where you can review the history of
have purchased and their associated license keys.

Please follow this link to confirm your company and contact information for t
that will have access to license keys for your Raritan software.
http://www.raritan.com/CreateAccount?ContactID=0035000000ZeXEa
Your e-mail address will be used as your username to access the License I

Should you have any questions or need assistance, please contact Raritan
Service @ (800) 724-8090 prompt "5" then "1" or your Sales Representative.

2. Über den in der E-Mail enthaltenen Link gelangen Sie zur Anmeldeseite für den Software-Lizenzschlüssel auf der Raritan-Website. Erstellen Sie ein Benutzerkonto, und melden Sie sich an. Der Benutzername ist Ihre E-Mail-Adresse. Die Seite mit den Daten des Lizenzkontos wird angezeigt. Ihre Lizenzdateien sind in Kürze verfügbar.
3. Überprüfen Sie, ob Sie eine weitere E-Mail vom Raritan Licensing Portal (Raritan-Lizenzierungsportal) mit dem Absender "licensing@raritan.com" und dem Betreff "Your Raritan Commandcenter SG Software License Key is Available" (Ihr Lizenzschlüssel für die Raritan Commandcenter SG-Software ist verfügbar) erhalten haben.



Raritan.
Know more. Manage smarter.

Thank You for Registering

7/15/2010
0035000000ZeXEa

Customer Name
Customer Address

Dear Customer

This is an important email regarding your recent Raritan CommandCenter Sec
purchase. Your Software License Key may now be generated. This License
required to activate this Software Product.

You can access that license key(s), as well as review the history of Raritan s
products that you have purchased with their associated license keys, at our w
here - http://www.raritan.com/licensing.

4. Über den in der E-Mail enthaltenen Link gelangen Sie zur Anmeldeseite für den Software-Lizenzschlüssel auf der Raritan-Website und können sich über Ihr gerade erstelltes Benutzerkonto anmelden.
5. Klicken Sie auf die Registerkarte "Product License" (Produktlizenz). Die von Ihnen erworbenen Lizenzen werden in einer Liste angezeigt. Sie können über eine oder mehrere Lizenzen verfügen. Siehe ***Verfügbare Lizenzen*** (auf Seite 11).
6. Zum Erhalt jeder Lizenz klicken Sie neben dem Element in der Liste auf "Create" (Erstellen), und geben dann die <Produktname>-Host-ID ein. Sie können die Host-ID von der Seite "License Management" (Lizenzverwaltung) kopieren und einfügen. Siehe ***Auffinden der Host-ID und Überprüfen der Anzahl der Knoten in der Datenbank*** (siehe "***Auffinden der Host-ID Ihrer physischen Appliance und Überprüfen der Anzahl der Knoten in der Datenbank***" auf Seite 13).
7. Klicken Sie auf "Create License" (Lizenz erstellen). Die von Ihnen eingegebenen Details werden in einem Popup-Fenster angezeigt. Überprüfen Sie, dass die Host-ID korrekt ist.

   Warnhinweis: Vergewissern Sie sich, dass die Host-ID korrekt ist! Eine mit einer falschen Host-ID erstellte Lizenz ist ungültig, und zur Behebung des Problems ist die Unterstützung des technischen Supports von Raritan erforderlich.

8. Klicken Sie auf OK. Die Lizenzdatei wird erstellt.
9. Klicken Sie auf "Download Now" (Jetzt herunterladen), und speichern Sie die Lizenzdatei.

Schritt 2: Installieren der Lizenz

1. Wählen Sie "Administration > License Management (Lizenzverwaltung)".
2. Klicken Sie auf "Add License" (Lizenz hinzufügen).
3. Lesen Sie die gesamte Lizenzvereinbarung, und aktivieren Sie anschließend das Kontrollkästchen "I Agree" (Ich stimme den Lizenzbedingungen zu).

Schritt 3: Checken Sie die zu aktivierenden Lizenzen aus:

Sie müssen Lizenzen auschecken, um die Funktionen zu aktivieren.

- Wählen Sie eine Lizenz aus der Liste, und klicken Sie auf "Check Out" (Auschecken). Checken Sie alle Lizenzen aus, die Sie aktivieren möchten.

Lizenzierung – Cluster – Neue Kunden

Eine Cluster-Kit-Lizenz ermöglicht den Betrieb von 2 physischen CC-SG-Einheiten als Cluster zur gemeinsamen Nutzung von Lizenzen. Das System ermöglicht einen eingeschränkten Betrieb, bis der Cluster erstellt ist und aktiv betrieben wird und die Lizenz auf dem primären Clusterknoten installiert und ausgecheckt wurde. Die CC-SG-Einheiten im Cluster können vorübergehend als eigenständige Einheiten betrieben werden, um eine unabhängige Wartung jeder Einheit zu erlauben. Die 2 CC-SG-Einheiten müssen für die weitere vollständige Funktionalität wieder zusammengefügt werden. Clustering wird bei virtuellen Appliances nicht unterstützt.

Hinweis: Wenn die Gnadenfrist für den eigenständigen Betrieb abgelaufen ist, ist der CC-SG-Betrieb eingeschränkt, bis das Cluster wieder zusammengefügt wurde. Siehe **Lizenzierung – Beschränkter Betrieb vor der Lizenzinstallation** *(auf Seite 31).*

Bei der Erstellung der Cluster-Lizenzdatei im Raritan Licensing Portal (Raritan-Lizenzierungsportal) müssen Sie die Host-IDs jeder CC-SG-Einheit eingeben. Sie finden diese Nummern auf der Seite "Administration > License Management (Lizenzverwaltung)" jeder CC-SG-Einheit.

So implementieren Sie ein CC-SG-Cluster mit einer Cluster-Kit-Lizenz:

Siehe ***Konfigurieren von CC-SG-Clustern*** (siehe "***CC-SG-Cluster konfigurieren***" auf Seite 304), um weitere Informationen zu CC-SG-Clustern zu erhalten.

1. Implementieren Sie beide CC-SG-Einheiten, die zu einem Cluster zusammengefügt werden sollen. Weitere Informationen zur Implementierung finden Sie in der CC-SG Kurzanleitung für die Einrichtung.
2. Suchen Sie die Host-IDs für jede CC-SG-Einheit. Siehe ***Auffinden der Host-ID und Überprüfen der Anzahl der Knoten in der Datenbank*** (siehe "***Auffinden der Host-ID Ihrer physischen Appliance und Überprüfen der Anzahl der Knoten in der Datenbank***" auf Seite 13).
3. Erhalten Sie die Cluster-Kit-Lizenzdatei. Siehe ***Lizenzierung – Neue Kunden – Physische Appliance*** (auf Seite 14).
4. Erstellen Sie das Cluster. Siehe ***Cluster erstellen*** (auf Seite 305).
5. Installieren Sie die Lizenzdatei auf dem primären Knoten im Cluster. Die Datei wird bei der Cluster-Erstellung auf den sekundären Knoten kopiert. Siehe ***Lizenzierung – Neue Kunden – Physische Appliance*** (auf Seite 14), um weitere Informationen zum Installieren einer Lizenzdatei zu erhalten.

6. Checken Sie die zu aktivierenden Lizenzen aus. Stellen Sie sicher, dass Sie die Cluster-Kit-Lizenz auschecken. Siehe ***Lizenzierung – Neue Kunden – Physische Appliance*** (auf Seite 14).

Lizenzierung – Virtuelle Appliance mit Lizenzserver

Für die virtuelle CC-SG-Appliance müssen Sie einen Lizenzserver für Ihre Lizenz installieren. Raritan stellt die Lizenzserversoftware, die Tools und den Daemon eines Drittanbieters zur Installation auf einem physischen Server bereit. Siehe ***Installationsvoraussetzungen für virtuelle Appliance*** (auf Seite 18).

Wenn Sie ein neuer Kunde sind und gerade eine virtuelle CC-SG-Appliance erworben haben, stellen Sie anhand der folgenden Anweisungen sicher, dass Sie einen Lizenzserver installiert und gültige Lizenzen aktiviert haben.

Installationsvoraussetzungen für virtuelle Appliance

- ESX 4.0 zum Implementieren der virtuellen CommandCenter Secure Gateway-Appliance
  - Muss über einen Datenspeicher mit mindestens 40 GB verfügbarem Speicherplatz verfügen
  - Muss über 2 GB verfügbaren Speicher verfügen
  - 2 virtuelle Netzwerkkarten
  - Ein hoch verfügbares Cluster mit gemeinsam genutztem Speicher wird empfohlen
- Client-Computer mit vSphere Client 4.0
- Ein physischer Windows- oder Linux-Server für den Flexera™ FlexNet Publisher®-Lizenzserver und ein unterstütztes Betriebssystem

  Das Programm lmgrd von Flexera wird von den folgenden Betriebssystemen unterstützt:
  - Windows 32-Bit, x86 unter Windows Server 2008, Windows Server 2003, Windows XP Professional mit SP3, Windows Vista (Ultimate), Windows 7 (Ultimate)
  - Linux 32-Bit Linux Standard Base (LSB) 3.0-zertifiziert, x86 unter Red Hat Enterprise Linux 4.0 und 5.0
- Die folgenden Dateien, die unter "http://www.raritan.com/support/commandcenter-secure-gateway" verfügbar sind. Weitere Informationen finden Sie unter ***Installationsdateien herunterladen*** (auf Seite 19).
  - .OVF-Datei der virtuellen CommandCenter Secure Gateway-Appliance

- Von Raritan bereitgestellte Datei für den Daemon eines Drittanbieters
- Flexera FlexNet Publisher-Lizenzserver

Installationsdateien herunterladen

Der komplette Satz Installationsdateien ist unter "http://www.raritan.com/support/CommandCenter-Secure-Gateway/" verfügbar.

Sie müssen sich am Raritan Licensing Portal (Raritan-Lizenzierungsportal) anmelden, um unter diesem Link auf die Dateien zugreifen zu können. Siehe ***Erhalt Ihrer Lizenz*** (auf Seite 21).

Die OVF-Datei wird auch auf der Produkt-DVD an Kunden ausgeliefert, wenn Sie sie aufgrund ihrer Größe nicht herunterladen möchten. Die Flexera-Dateien oder die Dateien für den Daemon eines Drittanbieters sind nicht auf der DVD enthalten. Sie müssen sie daher von der Website herunterladen.

Die Installationsdateien sind in zwei .ZIP-Dateien gepackt. Der Teil mit der <Versionsnummer> des Dateinamens enthält die tatsächliche CC-SG-Versionsnummer.

Die Datei "vccsg_rel_<Versionsnummer>_ovf.ZIP" enthält Folgendes:

- .OVF-Datei zum Implementieren der virtuellen Appliance

Die Datei "flexserver-11.8-raritan.ZIP" enthält Folgendes:

- Von Raritan bereitgestellte Daemons von Drittanbietern für Linux und Windows
- Flexera™ FlexNet Publisher®-Lizenzserver-Toolkit für Linux und Windows

Lizenserversoftware unter Linux- oder Windows-Server installieren

Der Flexera™ FlexNet Publisher®-Lizenzserver muss für die virtuelle CommandCenter Secure Gateway-Appliance auf einem physischen Server installiert sein. Informationen zu den unterstützten Servern finden Sie unter Anforderungen.

Linux-Server

1. Melden Sie sich am Linux-Server an.
2. Fügen Sie einen Benutzer mit dem Namen *flex* zum System hinzu.
3. Melden Sie sich als *flex* an, und öffnen Sie das Terminal.
4. Kopieren Sie die heruntergeladene Datei "flexserverv11.8-linux.tar.gz" in das Verzeichnis "home/flex". Entpacken Sie den Inhalt im selben Verzeichnis.
5. Geben Sie den folgenden Befehl ein:

```
tar -xvzf flexserverv11.8.tar.gz
```

Die Dateien werden entpackt. Die folgenden Verzeichnisse werden erstellt:

- flexserverv11.8
- i86_lsb wird unter flexserverv11.8 erstellt.

6. Entpacken Sie die Datei "5-1-0-raritan-daemon/raritan-linux32-1.1.zip" in das Verzeichnis "home/flex".
7. Verschieben Sie die von Raritan bereitgestellte Datei für den Daemon eines Drittanbieters mit dem folgenden Befehl:

   ```
   cp raritan /home/flex/flexserverv11.8/i86_lsb/
   ```

8. Geben Sie den folgenden Befehl ein:

   ```
   chmod +x raritan
   ```

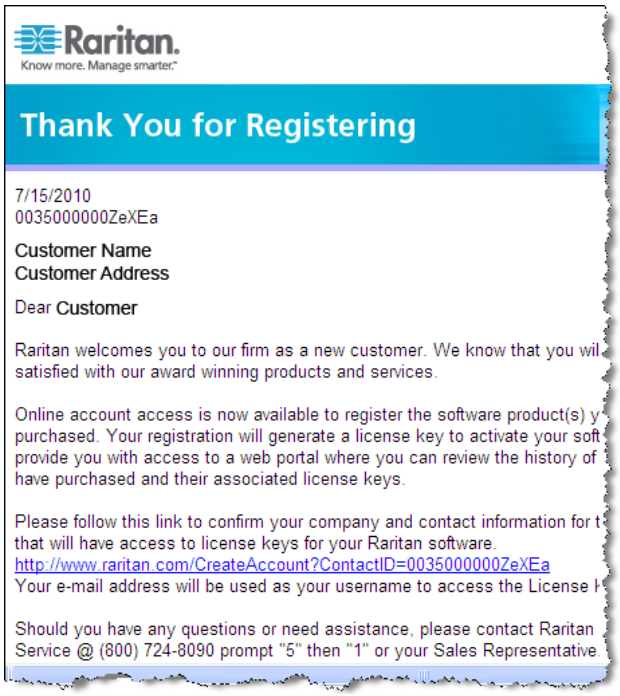
9. Stellen Sie sicher, dass das Paket "redhat-lsb" installiert ist. Führen Sie `yum install redhat-lsb` als Root aus.

Windows-Server

1. Entpacken Sie die Datei "flexserverv11.8-win.zip" unter C:\ auf dem Windows-Server. Damit wird ein Ordner mit dem Namen "flexnet-win" erstellt.
2. Entpacken Sie die Datei "raritan-win32-1.0.zip" im Verzeichnis "C:\flexnet-win\i86_n3\".

Erhalt Ihrer Lizenz

1. Der beim Kauf angegebene Lizenzadministrator erhält eine E-Mail vom Raritan Licensing Portal (Raritan-Lizenzierungsportal) mit dem Absender "licensing@raritan.com" und dem Betreff "Thank You for Registering" (Vielen Dank für Ihre Registrierung).



Raritan.
Know more. Manage smarter.

Thank You for Registering

7/15/2010
0035000000ZeXEa

Customer Name
Customer Address

Dear **Customer**

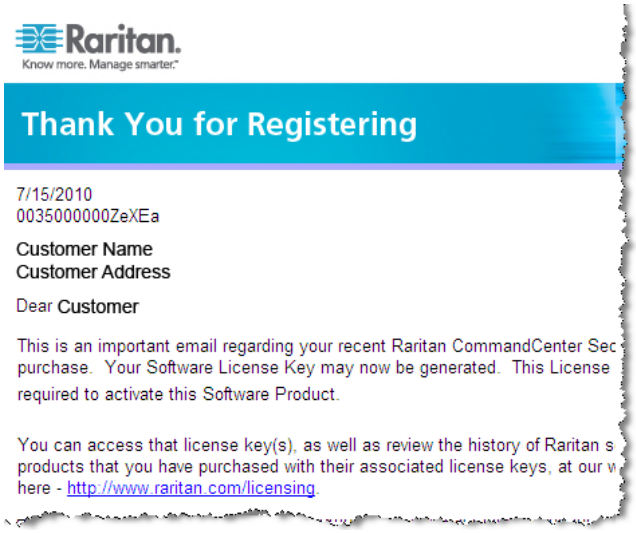
Raritan welcomes you to our firm as a new customer. We know that you wil
satisfied with our award winning products and services.

Online account access is now available to register the software product(s) y
purchased. Your registration will generate a license key to activate your soft
provide you with access to a web portal where you can review the history of
have purchased and their associated license keys.

Please follow this link to confirm your company and contact information for t
that will have access to license keys for your Raritan software.
http://www.raritan.com/CreateAccount?ContactID=0035000000ZeXEa
Your e-mail address will be used as your username to access the License I

Should you have any questions or need assistance, please contact Raritan
Service @ (800) 724-8090 prompt "5" then "1" or your Sales Representative

2. Über den in der E-Mail enthaltenen Link gelangen Sie zur Anmeldeseite für den Software-Lizenzschlüssel auf der Raritan-Website. Erstellen Sie ein Benutzerkonto, und melden Sie sich an. Der Benutzername ist Ihre E-Mail-Adresse. Die Seite mit den Daten des Lizenzkontos wird angezeigt. Ihre Lizenzdateien sind in Kürze verfügbar.
3. Überprüfen Sie, ob Sie eine weitere E-Mail vom Raritan Licensing Portal (Raritan-Lizenzierungsportal) mit dem Absender "licensing@raritan.com" und dem Betreff "Your Raritan Commandcenter SG Software License Key is Available" (Ihr Lizenzschlüssel für die Raritan Commandcenter SG-Software ist verfügbar) erhalten haben.



Raritan.
Know more. Manage smarter.

Thank You for Registering

7/15/2010
0035000000ZeXEa

Customer Name
Customer Address

Dear Customer

This is an important email regarding your recent Raritan CommandCenter Sec
purchase. Your Software License Key may now be generated. This License
required to activate this Software Product.

You can access that license key(s), as well as review the history of Raritan s
products that you have purchased with their associated license keys, at our w
here - http://www.raritan.com/licensing.

4. Über den in der E-Mail enthaltenen Link gelangen Sie zur Anmeldeseite für den Software-Lizenzschlüssel auf der Raritan-Website und können sich über Ihr gerade erstelltes Benutzerkonto anmelden.
5. Klicken Sie auf die Registerkarte "Product License" (Produktlizenz). Die von Ihnen erworbenen Lizenzen werden in einer Liste angezeigt. Sie können über eine oder mehrere Lizenzen verfügen.
6. Um die einzelnen Lizenzen zu erhalten, klicken Sie neben dem entsprechenden Element in der Liste auf "Create" (Erstellen). Wenn Sie mehrere Lizenzen haben, müssen Sie zuerst die Basislizenz erstellen.
7. Wählen Sie "New License Server Deployment" (Neue Lizenzserver-Implementierung) aus, wenn Sie zum ersten Mal eine Lizenz erstellen. Wenn Sie über mehrere CC-SG-Implementierungen mit mehr als einem Lizenzserver verfügen, wählen Sie zunächst "Add to an Existing License Server Deployment" (Zu bestehender Lizenzserver-Implementierung hinzufügen) und dann den Lizenzserver, dem Sie diese Lizenz hinzufügen möchten.
8. Wählen Sie "Single" (Einzeln) als Implementierungsmodus und Pfad aus. Lassen Sie "Vendor Daemon Path" (Pfad des Daemon eines Drittanbieters) leer, und klicken Sie auf "Weiter".
9. Wählen Sie "Hostname" oder "Host IP" (Host-IP) aus, und geben Sie entweder den Hostnamen oder die IP-Adresse des Lizenzservers ein.
10. Geben Sie die Host-ID des Lizenzservers ein. Verwenden Sie dazu die unten stehenden Anweisungen zum Abrufen der ID. Die Host-ID ist eine lange Zeichenfolge aus Buchstaben und Zahlen, z. B. `A005B983-8DFE-D511-A510-00112FCB87F6`.

- Zum Abrufen der Host-ID Ihres Lizenzservers führen Sie das Programm `dmidecode` aus dem unten angegebenen Verzeichnis auf dem Lizenzserver aus.
  - Linux: `su - root; dmidecode -s system-uuid`
  - Windows: Wechseln Sie mit dem Befehl `cd` zum Verzeichnis "/flexnet-win/i86_n3", und führen Sie dann `dmidecode -s system-uuid` aus.
  - Geben Sie die TCP-Portnummer ein, über die CC-SG mit dem Lizenzserver kommuniziert. Der Standardport ist Port 27000. Befindet sich der Lizenzserver hinter einer Firewall, müssen Sie sicherstellen, dass die eingegebene Portnummer offen ist.

11. Klicken Sie auf "Create License" (Lizenz erstellen). Die von Ihnen eingegebenen Details werden in einem Popup-Fenster angezeigt. Überprüfen Sie, dass die Host-ID korrekt ist.

    Warnhinweis: Vergewissern Sie sich, dass die Host-ID korrekt ist! Eine mit einer falschen Host-ID erstellte Lizenz ist ungültig, und zur Behebung des Problems ist die Unterstützung des technischen Supports von Raritan erforderlich.

12. Klicken Sie auf OK. Die Lizenzdatei wird erstellt.
13. Klicken Sie auf "Download Now" (Jetzt herunterladen), und speichern Sie die Lizenzdatei.

Lizenzdatei auf Lizenzserver kopieren

Lizenzdateien müssen zum Lizenzserver hinzugefügt werden. Wenn Sie mehrere Lizenzdateien besitzen, kopieren Sie ggf. den gesamten Inhalt jeder Datei in eine einzige Datei und speichern sie mit einem Texteditor auf Ihrem Lizenzserver. Stellen Sie sicher, dass Sie die Datei mit der Erweiterung .LIC speichern.

Linux-Server

- Kopieren Sie die Lizenzdatei in das Verzeichnis "/home/flex/flexserverv11.8/i86_lsb/".

Windows-Server

- Kopieren Sie die Lizenzdatei in das Verzeichnis "c:\flexnet-win\i86_n3\".

Lizenzserver starten

Linux-Server

1. `cd /home/flex/flexserverv11.8/i86_lsb/`

2. Führen Sie `lmgrd` aus, um den Server zu starten. In den Beispielbefehlen steht "Lizenzdatei.lic" für den Namen der .LIC-Datei. Wenn Sie mehrere Lizenzdateien besitzen, müssen Sie die Dateinamen im Befehl angeben. Trennen Sie die Dateinamen dabei durch einen Doppelpunkt. Siehe Beispiele.

   ```
   /lmgrd -c ./Lizenzdatei.lic
   ```

   ```
   /lmgrd -c ./Lizenzdatei1.lic:Lizenzdatei2.lic
   ```

Windows-Server

1. Starten Sie die Windows-Shell "cmd.exe".
2. Geben Sie den folgenden Befehl ein, um das Verzeichnis zu wechseln:

   ```
   cd c:\flexnet-win\i86_n3\
   ```

3. Führen Sie `lmgrd` aus, um den Server zu starten. In den Beispielbefehlen steht "Lizenzdatei.lic" für den Namen der .LIC-Datei. Wenn Sie mehrere Lizenzdateien besitzen, müssen Sie die Dateinamen im Befehl angeben. Trennen Sie die Dateinamen dabei durch einen Strichpunkt. Siehe Beispiele.

   ```
   lmgrd -z -c Lizenzdatei.lic
   ```

   ```
   lmgrd -z -c Lizenzdatei1.lic;Lizenzdatei2.lic
   ```

CommandCenter Secure Gateway unter VMware ESX Server 4.0 installieren

1. Stellen Sie mithilfe von vSphere 4.0 über Ihren Client-Computer eine Verbindung zu ESX 4.0 her.
2. Melden Sie sich als Benutzer mit der Berechtigung zum Erstellen, Starten und Stoppen virtueller Geräte an.
3. Wählen Sie "File > Deploy OVF Template" (Datei > OVF-Vorlage bereitstellen).
4. Wählen Sie "Deploy From File" (Von Datei bereitstellen) aus, und klicken Sie auf "Durchsuchen", um in das Verzeichnis zu wechseln, in dem Sie die Dateien entpackt haben. Wählen Sie die .OVF-Datei aus. Klicken Sie auf "Weiter".
5. Es werden Details zum virtuellen Gerät angezeigt, das erstellt wird. Sie können den Standardnamen des virtuellen Geräts ändern. Klicken Sie auf "Weiter".
6. Wählen Sie den Standort des Bestands aus. Klicken Sie auf "Weiter".
7. Wählen Sie den Host aus, auf dem Sie das CommandCenter Secure Gateway bereitstellen möchten. **Zur Ausfallsicherung wird ein Host empfohlen, der Teil eines hoch verfügbaren Clusters ist.** Klicken Sie auf "Weiter".

8. Wenn Sie ein Cluster ausgewählt haben, wählen Sie den entsprechenden Host aus. Klicken Sie auf "Weiter".
9. Wählen Sie den Datenspeicher, in dem alle Dateien gespeichert werden. Stellen Sie sicher, dass der Datenspeicher 40 GB an freiem Datenspeicher besitzt. Klicken Sie auf "Weiter".
10. Wählen Sie das Netzwerk, in dem CC-SG bereitgestellt wird. Klicken Sie auf "Weiter".
11. Sehen Sie sich die Übersicht an, und klicken Sie auf "Fertig stellen". Warten Sie ein paar Minuten, bis das virtuelle Gerät erstellt wurde.
12. Schalten Sie das virtuelle Gerät ein.
13. Öffnen Sie die Registerkarte "Konsole", um auf die CC-SG-Diagnosekonsole zuzugreifen.

Anmelden bei Diagnosekonsole und Einstellen der IP-Adresse für CC-SG

1. Melden Sie sich als *admin/raritan* an. Bei Benutzernamen und Kennwörtern wird die Groß-/Kleinschreibung beachtet.
2. Sie werden zur Änderung des Kennworts für die lokale Konsole aufgefordert.
   a. Geben Sie das Standardkennwort (*raritan*) erneut ein.
   b. Geben Sie es ein, und bestätigen Sie das neue Kennwort. Das neue Kennwort muss sicher sein und aus einer Zahlen- und Buchstabenkombination von mindestens acht Zeichen bestehen.
3. Drücken Sie STRG+X, sobald der Begrüßungsbildschirm angezeigt wird.
4. Wählen Sie "Operation > Network Interfaces > Network Interface Config". Die Administrationskonsole wird angezeigt.
5. Wählen Sie im Feld "Configuration" die Option "DHCP" oder "Static" aus. Wenn Sie "Static" auswählen, geben Sie eine statische IP-Adresse ein. Definieren Sie bei Bedarf DNS-Server, Netzmaske und Gateway-Adresse.
6. Wählen Sie "Save" (Speichern). Warten Sie einige Minuten, während CC-SG neu gestartet wird.

CC-SG-Standardeinstellungen

IP-Address (IP-Adresse): 192.168.0.192

Subnetzmaske: 255.255.255.0

Benutzername/Kennwort: admin/raritan

Anmelden bei CC-SG

1. Starten Sie einen unterstützten Browser, und geben Sie die URL von CC-SG ein: https://<IP-Adresse>/admin.

   (z. B. https://192.168.0.192/admin).

   Hinweis: Die Standardeinstellung für Browserverbindungen lautet HTTPS/SSL-verschlüsselt.

2. Akzeptieren Sie im Fenster mit dem Sicherheitshinweis die Verbindung.
3. Wenn Sie eine nicht unterstützte Version der Java Runtime Environment verwenden, werden Sie durch eine Warnung darauf hingewiesen. Folgen Sie den Anweisungen, um entweder die richtige Version herunterzuladen oder fortzufahren. Das Fenster Anmeldung wird geöffnet.
4. Geben Sie den Standardbenutzernamen (*admin*) und das Standardkennwort (*raritan*) ein, und klicken Sie auf "Anmeldung".

   Der CC-SG-Administrations-Client wird geöffnet.

Installieren und Auschecken der Lizenz

1. Wählen Sie "Administration > License Management (Lizenzverwaltung)".
2. Klicken Sie auf "Add License" (Lizenz hinzufügen).
3. Lesen Sie die gesamte Lizenzvereinbarung, und aktivieren Sie anschließend das Kontrollkästchen "I Agree" (Ich stimme den Lizenzbedingungen zu).
4. Klicken Sie auf "Durchsuchen", und wählen Sie die Basislizenzdatei der virtuellen Appliance aus.
5. Klicken Sie auf "Öffnen". CC-SG stellt eine Verbindung zum Lizenzserver her und ruft eine Liste der lizenzierten Funktionen ab. Die Funktionen werden in einer Liste angezeigt.
6. Wählen Sie die CCSG128-VA-Basislizenz aus, und klicken Sie auf "Check-Out" (Auschecken), um sie zu aktivieren.
7. Zum Aktivieren von Add-On-Lizenzen wählen Sie die einzelnen Lizenzen aus und klicken dann auf "Check-Out" (Auschecken).

Im CC-SG-Administratorhandbuch erhalten Sie weitere Informationen zu Lizenzen. In der Dokumentation zu Flexera™ FlexNet Publisher® finden Sie weitere Informationen zum Verwalten Ihres Lizenzservers. Sie können den FlexNet Publisher License Administration Guide für das FlexNet Publisher Licensing Toolkit 11.8 von der Website www.flexera.com unter "Support > Documentation Center" (Support > Dokumentationscenter) herunterladen.

Kommunikation mit Lizenzserver

Die Verbindung zwischen der virtuellen CC-SG-Appliance und dem Lizenzserver muss bestehen bleiben. CC-SG verwendet diese Verbindung, um sicherzustellen, dass der Lizenzserver verfügbar ist, und um festzustellen, welche Lizenzdateien zur Verfügung stehen. Darüber hinaus wird diese Verbindung zum Ein- und Auschecken von Lizenzen verwendet.

Zugriff auf Lizenzen

Alle ausgecheckten Lizenzen müssen jederzeit auf dem Lizenzserver verfügbar sein. Wenn eine Lizenzdatei verschoben oder vom Lizenzserver gelöscht wird, kann CC-SG die Lizenz beim Abfragen des Lizenzservers nicht prüfen. Wenn eine ausgecheckte Lizenz auf dem Lizenzserver nicht auffindbar ist, beendet CC-SG den Zugriff.

Um dies zu vermeiden, müssen Sie Lizenzen immer einchecken, bevor Sie sie verschieben oder vom Lizenzserver löschen.

Ausfall des Lizenzservers

Wenn CC-SG keine Verbindung zum Lizenzserver herstellen kann, bleiben Ihre Lizenzen noch 7 Tage lang gültig. Bei jeder Anmeldung an CC-SG werden Sie an den letzten Tag erinnert, an dem Sie Zugriff erhalten, sofern die Verbindung zum Lizenzserver nicht wiederhergestellt wird.

Ihre ausgecheckten Lizenzen werden eingecheckt und CC-SG beendet den Zugriff, wenn die Frist von 7 Tagen verstreicht, ohne dass die Verbindung zum Lizenzserver wiederhergestellt wird. Sie haben dann Zugriff auf begrenzte Optionen in CC-SG. Siehe ***Lizenzierung – Beschränkter Betrieb vor der Lizenzinstallation*** (auf Seite 31).

Wenn der Lizenzserver wieder verfügbar ist, müssen Sie die einzelnen Lizenzen erneut auschecken, um den normalen Betrieb wiederaufzunehmen. Siehe ***Installieren und Auschecken der Lizenz*** (auf Seite 26).

Neustart des Lizenzservers nach einem Ausfall

Starten Sie den Lizenzserver neu, wenn er ausfällt und den Betrieb anschließend wieder aufnimmt oder wenn Sie Lizenzdateien verschieben, hinzufügen oder löschen.

Ein Neustart des Lizenzservers stellt sicher, dass CC-SG mit den neuesten Informationen synchronisiert wird.

Hinweis: Ein Windows-Lizenzserver führt nach einem Ausfall automatisch eine Synchronisierung durch. Ein Linux-Lizenzserver führt nach einem Zeitlimit von 2 Stunden eine Synchronisierung durch. Über einen Neustart wird nach einem Ausfall jedoch sofort eine Synchronisierung durchgeführt.

So starten Sie einen Lizenzserver neu:

Führen Sie den Befehl `lmdown` aus, um den Lizenzserver normal herunterzufahren.

Befehlszeilenprogramme zum Verwalten des Lizenzservers

Die unten genannten Dienstprogramme werden bei der Installation der Lizenzserversoftware installiert. Sie können jedes dieser Programme über die Befehlszeile ausführen, um den Lizenzserver zu verwalten.

In den Beispielen werden die folgenden Werte für die Elemente in Klammern verwendet.

<Funktionsname> ist der Wert in der Spalte "Feature" (Funktion) auf der Seite "Administration > Lizenzmanager" des Administrations-Clients. Beispiel: "CCSG128-VA" ist der Funktionsname für die Basislizenz der virtuellen Appliance.

<Lizenzdateiname> ist der Dateiname der installierten Lizenzdatei, die auf dem Lizenzserver installiert ist.

In der Dokumentation zu Flexera™ FlexNet Publisher® finden Sie weitere Informationen zum Verwalten Ihres Lizenzservers. Sie können den FlexNet Publisher License Administration Guide für das FlexNet Publisher Licensing Toolkit 11.8 von der Website www.flexera.com unter "Support > Documentation Center" (Support > Dokumentationscenter) herunterladen.

Befehl	Beschreibung
lmborrow	Ermöglicht einem Benutzer das Auschecken und Ausleihen einer Funktion für einen bestimmten Zeitraum, obwohl keine Verbindung zum Netzwerk besteht.

lmdiag	Ermöglicht einem Benutzer die Diagnose von Problemen, wenn eine Funktion nicht ausgecheckt werden kann. Versucht, die Funktion auszuchecken, und gibt an, ob der Versuch erfolgreich war oder fehlgeschlagen ist. `lmdiag -c <Lizenzdateiname> <Funktionsname> -n`
lmdown	Ermöglicht das normale Herunterfahren ausgewählter Lizenz-Daemons. `lmdown -vendor raritan` wird zum Herunterfahren des von Raritan bereitgestellten Daemon eines Drittanbieters verwendet.
lmhostid	Ermöglicht dem Benutzer das Abrufen der Host-ID der aktuellen Plattform. Beinhaltet die Argumente –uuid und –hostdomain oder –internet.
lminstall	Ermöglicht die Konvertierung von Lizenzen zwischen dem lesbaren Textformat und dem Dezimalformat.
lmnewlog	Verschiebt die bestehenden Berichtsprotokolldaten in eine neue Datei und beginnt einen neuen Bericht mit dem ursprünglichen Namen der Berichtsprotokolldatei.
lmpath	Ergänzt oder überschreibt die aktuellen Lizenzpfadeinstellungen oder ruft diese ab.
lmremove	Entfernt die Lizenz eines einzelnen Benutzers für eine bestimmte Funktion. Der Lizenzservermanager lässt sich so konfigurieren, dass eine unerlaubte Ausführung von lmremove verhindert wird.
lmreread	`lmreread – vendor raritan` weist den von Raritan bereitgestellten Daemon eines Drittanbieters an, die Lizenz und die Optionsdateien erneut zu lesen.

lmswitchr	Schließt das bestehende Berichtsprotokoll und beginnt ein neues Berichtsprotokoll mit einem neuen Dateinamen. Mit dem Befehl lässt sich auch eine neue Berichtsprotokolldatei beginnen, wenn noch keine vorhanden ist.
lmswitch	Schließt das bestehende Debugprotokoll für den Daemon eines Drittanbieters und beginnt ein neues Debugprotokoll für diesen Daemon mit einem neuen Dateinamen. Mit dem Befehl lässt sich auch eine neue, vom Daemon eines Drittanbieters erzeugte Debugprotokolldatei beginnen, wenn noch keine vorhanden ist.
lmstat	Ruft den Status der Lizenzdateien, die Verfügbarkeit der Funktionen und die Nutzungsinformationen ab, die vom Lizenzserver empfangen werden, und zeigt diese an. `lmstat -c <Lizenzdateiname> -f <Funktionsname>`
lmver	Meldet die Version einer FLEXnet Publisher-Bibliothek oder -Binärdatei wie lmgrd, lmadmin, lmdown, Daemon eines Drittanbieters.

VMware Tools installieren oder aktualisieren

VMware Tools werden von VMware für alle Implementierungen virtueller Geräte empfohlen. Nach Installation der VMware Tools auf der virtuellen CommandCenter Secure Gateway-Appliance können Sie diese anhand der folgenden Anweisungen aktualisieren, wenn VMware eine neue Version zur Verfügung stellt.

Mit dem virtuellen CC-SG OVF-Paket wird standardmäßig eine Version der VMware Tools installiert.

So installieren oder aktualisieren Sie VMware Tools:

1. Melden Sie sich beim vSphere-Client an, und stellen Sie eine Verbindung zu dem ESX-Host her, auf dem sich die virtuelle CC-SG-Appliance befindet.
2. Wählen Sie das virtuelle Gerät aus, und klicken Sie auf die Registerkarte "Konsole". Die Diagnosekonsole wird angezeigt.

3. Klicken Sie mit der rechten Maustaste auf das virtuelle Gerät, und wählen Sie "Guest > Install/Upgrade VMware Tools" (Gast > VMware Tools installieren/aktualisieren). Damit werden die Dateien auf dem virtuellen Gerät bereitgestellt, sodass CC-SG die Installation vornehmen kann.
4. Öffnen Sie einen Browser, und melden Sie sich beim Administrations-Client an.
5. Wählen Sie "Systemwartung > Install / Upgrade VMware Tools" (VMware Tools installieren/aktualisieren). Nach Abschluss der Installation wird eine Erfolgsmeldung angezeigt.

Sicherungen und Schnappschüsse von virtueller Appliance und Speicherservern konfigurieren

Nach Implementierung der virtuellen CC-SG-Appliance müssen Sie über VMware® Sicherungen der virtuellen Appliance und der Speicherserver konfigurieren, die von der virtuellen Appliance verwendet werden.

Sie sollten über VMware zudem Schnappschüsse aktivieren.

Weitere Informationen zum Konfigurieren dieser Funktionen finden Sie in der VMware-Dokumentation unter "http://www.vmware.com/support/pubs/vs_pubs.html".

Virtuelle Appliances mit Remote-Speicherservern

Wenn die virtuelle CC-SG-Appliance einen Remote-Server als Dateispeicher verwendet und der Zugriff auf den Speicher verloren geht, kann der Zugriff auf CC-SG so lange unterbrochen sein, bis der Speicherserver vollständig hochgefahren wurde. Möglicherweise wird eine Meldung angezeigt, dass Probleme beim Abruf von Konfigurationsdaten bestehen.

Lizenzierung – Beschränkter Betrieb vor der Lizenzinstallation

Bis Sie die jeweiligen Lizenzen installiert und ausgecheckt haben, ist der CC-SG-Betrieb eingeschränkt. Es kann nur auf die folgenden Menüpunkte zugegriffen werden.

- Diagnosekonsole: Zum Abrufen notwendiger Informationen und Protokolle konfigurieren Sie Netzwerkschnittstellen.

Hinweis: Sie können über den VGA-/Tastatur-/Mausport (falls zutreffend), den seriellen Port (falls zutreffend) oder SSH auf die Schnittstellen für die Administratorkonsole und die Statuskonsole zugreifen. Die Schnittstelle für die Statuskonsole steht auch über eine Webschnittstelle zur Verfügung, falls diese aktiviert ist.

- Kennwort ändern
- Secure Gateway: Zur Anzeige von "Tipp des Tages", "Drucken", "Fenster drucken", "Abmelden" und "Beenden".
- Administration > Clusterkonfiguration: Zum Konfigurieren des Clusters und Zuweisen von Rollen an die Cluster-Knoten. Das Erstellen des Clusters ist eine Voraussetzung für den Betrieb einer clusterbasierten Lizenz. Cluster sind nur auf physischen Appliances verfügbar.
- Administration > Lizenzmanager: Zum Hochladen und Entfernen von Lizenzdateien, zum Auschecken und Einchecken von Lizenzen.
- Systemwartung: Es kann auf die folgenden Menüpunkte zugegriffen werden.
  - Wiederherstellen: Zum Wiederherstellen von Lizenzen in CC-SG, falls Sie eine vollständige Rücksetzung durchführen und die Lizenzen versehentlich entfernen.
  - Wartungsmodus: Zum Aufrufen und Beenden des Wartungsmodus, um ggf. einen Cluster zu erstellen oder Aktualisierungen durchzuführen.
  - Neu starten
  - Aktualisieren
  - Herunterfahren
- Ansicht
- Hilfe: Zum Anzeigen der Online-Hilfe-Dokumentation.

Lizenzierung – Bestehende Kunden

Wenn Sie bereits CC-SG-Kunde mit einer physischen CC-SG-Appliance sind, wird bei der Aktualisierung der CC-SG-Einheit auf Version 5.0 oder höher eine Lizenzdatei erstellt und installiert, mit der Sie CC-SG mit der Anzahl der Knoten weiternutzen können, die zum Zeitpunkt der Aktualisierung konfiguriert war.

Alle bestehenden Kunden müssen auf Version 5.0 aktualisieren, bevor sie auf eine höhere Version als Version 5.0 aktualisieren können.

Gehen Sie wie unten beschrieben vor, um zu überprüfen, dass Ihre Lizenzdateien nach der Aktualisierung auf Version 5.0 vorhanden sind.

Schritt 1: Aktualisierung auf Version 5.0:

Siehe ***CC-SG aktualisieren*** (auf Seite 273).

Schritt 2: Zeigen Sie die Lizenzdateien an:

1. Wählen Sie im Administrations-Client "Administration > License Management (Lizenzverwaltung). Die Seite "Lizenzmanager" wird geöffnet.
   - Der Abschnitt "License Summary" (Lizenzübersicht) zeigt detaillierte Informationen zu Ihrer Lizenz bzw. Ihren Lizenzen an. Sie können die CC-SG-Host-ID anzeigen, die mit dieser Lizenzdatei verknüpft ist.
   - Die Anzahl der verwendeten Knoten und Anzahl der zulässigen Knoten wird in der Mitte der Seite aufgeführt.

Hinweis: Wenn Sie feststellen sollten, dass die Anzahl der zulässigen Knoten geringer ist als die Anzahl der ursprünglich lizenzierten Knoten, kontaktieren Sie einen Vertriebsmitarbeiter von Raritan.

Lizenzierung – Rehosting

Lizenzen für physische Appliances sind mit einer bestimmten CC-SG-Einheit verknüpft. Lizenzen für virtuelle Appliances sind mit einem bestimmten Lizenzserver verknüpft.

Wenn sich diese Elemente ändern, wenn Ihre Lizenzdatei der falschen Host-ID zugeordnet ist oder wenn etwas passiert, das zu einer Nichtübereinstimmung zwischen Lizenzdatei und dem CC-SG-System führen würde, müssen Sie eine neue Lizenzdatei mit der korrekten Host-ID erlangen.

So erhalten Sie eine neue Lizenzdatei mit einer anderen Host-ID:

Wenden Sie sich an den technischen Support von Raritan. Siehe ***Kontaktpersonen des technischen Supports*** (auf Seite 2).

Lizenz hinzufügen

Sie können einer CC-SG-Einheit eine Lizenz hinzufügen, wenn Sie eine neue Add-On-Lizenz kaufen oder Ihre Lizenzen ersetzen müssen.

Fügen Sie beim Ersetzen der Lizenzen zuerst die Basislizenz hinzu. Add-On-Lizenzen, die der vorherigen Basislizenz zugeordnet sind, werden automatisch gelöscht, wenn sie in Verbindung mit der neuen Basislizenz nicht gültig sind, weil sie entweder einen anderen Typ aufweisen (z. B. eigenständige Lizenz oder Clusterlizenz) oder weil sich die Host-IDs unterscheiden.

Die vollständigen Regeln zum Ersetzen von Lizenzen finden Sie unter ***Häufig gestellte Fragen zur Lizenzierung*** (auf Seite 455).

So fügen Sie eine Lizenz hinzu:

1. Wählen Sie "Administration > License Management (Lizenzverwaltung)".
2. Klicken Sie auf "Add License" (Lizenz hinzufügen).
3. Lesen Sie die gesamte Lizenzvereinbarung, und aktivieren Sie anschließend das Kontrollkästchen "I Agree" (Ich stimme den Lizenzbedingungen zu).
4. Klicken Sie auf "Durchsuchen", und wählen Sie die Lizenzdatei aus.
5. Klicken Sie auf "Öffnen".

Hinweis: Wenn Sie einen Lizenzserver verwenden, nimmt CC-SG Kontakt zum Lizenzserver auf und zeigt die vollständige Liste der auf dem Server gefundenen Funktionen an.

6. Wählen Sie die zu aktivierenden Funktionen aus, und klicken Sie auf "Check Out" (Auschecken).

IP-Adresse bestätigen

1. Wählen Sie "Administration > Konfiguration".
2. Klicken Sie auf die Registerkarte "Netzwerksetup".
3. Überprüfen Sie, dass die Netzwerkeinstellungen richtig sind, und nehmen Sie Änderungen vor, falls erforderlich. Weitere Informationen finden Sie unter ***Netzwerkeinrichtung*** (auf Seite 288). **Optional.**
4. Klicken Sie auf "Konfiguration aktualisieren", um die Änderungen zu übernehmen.
5. Klicken Sie auf "Jetzt neu starten", um Ihre Einstellungen zu bestätigen und CC-SG neu zu starten.

CC-SG-Serverzeit festlegen

Uhrzeit und Datum von CC-SG müssen korrekt verwaltet werden, um die Glaubwürdigkeit der Funktionen zur Geräteverwaltung zu gewährleisten.

Wichtig: Die Konfiguration von Uhrzeit/Datum wird zum Planen von Aufgaben im Aufgabenmanager verwendet. Weitere Informationen finden Sie unter *Aufgabenmanager* (auf Seite 330). Die Uhrzeit, die auf Ihrem Client-PC eingestellt ist, unterscheidet sich eventuell von der auf CC-SG eingestellten Uhrzeit.

Nur der CC-Superuser und Benutzer mit ähnlichen Berechtigungen dürfen Uhrzeit und Datum konfigurieren.

In einer Clusterkonfiguration kann die Zeitzone nicht geändert werden.

So konfigurieren Sie die Serveruhrzeit und das Datum von CC-SG:

1. Wählen Sie "Administration > Konfiguration".
2. Klicken Sie auf die Registerkarte "Datum/Uhrzeit".
   a. So stellen Sie das Datum und die Uhrzeit manuell ein:
   - Datum: Zum Einstellen des Datums klicken Sie auf den Pfeil neben der Dropdown-Liste und wählen darin den Monat aus. Wählen Sie das Jahr mit der Schaltfläche "Pfeil-nach-oben/unten", und klicken Sie im Kalenderbereich auf den Tag.

- Uhrzeit: Zum Einstellen der Uhrzeit klicken Sie auf die Schaltfläche "Pfeil-nach-oben/unten", um die Stunde, Minuten und Sekunden festzulegen. Klicken Sie anschließend auf die Dropdown-Liste "Zeitzone", um die Zeitzone auszuwählen, in der CC-SG betrieben wird.

a. So stellen Sie das Datum und die Uhrzeit mittels NTP ein: Markieren Sie das Kontrollkästchen "Network Time Protocol aktivieren" unten im Fenster, und geben Sie die IP-Adresse für den primären NTP-Server und dem sekundären NTP-Server in die entsprechenden Felder ein.

Hinweis: Zum Synchronisieren des Datums und der Uhrzeit von angeschlossenen Computern mit dem Datum und der Uhrzeit eines zugewiesenen NTP-Servers wird das Network Time Protocol (NTP) verwendet. Wird CC-SG mit NTP konfiguriert, kann es zur konsistenten Verwendung der korrekten Uhrzeit seine eigene Uhrzeit mit dem öffentlich verfügbaren NTP-Referenzserver synchronisieren.

3. Klicken Sie auf Konfiguration aktualisieren, um die Uhrzeit- und Datumsänderungen auf CC-SG anzuwenden.
4. Klicken Sie auf Aktualisieren, um die neue Serverzeit im Feld "Aktuelle Uhrzeit" zu aktualisieren.

Wählen Sie "Systemwartung > Neu starten", um CC-SG neu zu starten.

Kompatibilitätsmatrix überprüfen

Die Kompatibilitätsmatrix führt die Firmwareversionen von Raritan-Geräten und Softwareversionen von Anwendungen auf, die mit der aktuellen Version von CC-SG kompatibel sind. CC-SG überprüft diese Daten, wenn Sie ein Gerät hinzufügen, Gerätefirmware aktualisieren oder eine Anwendung zur Verwendung auswählen. Wenn die Firmware- oder Softwareversion inkompatibel ist, zeigt CC-SG eine Warnung an. Jede Version von CC-SG unterstützt nur die zum Erscheinungszeitpunkt aktuelle Firmwareversion und die vorherigen Firmwareversionen für Raritan-Geräte. Sie können die Kompatibilitätsmatrix auf der Support-Website von Raritan ansehen.

So überprüfen Sie die Kompatibilitätsmatrix:

- Wählen Sie "Administration > Kompatibilitätsmatrix".

Anwendungsversionen prüfen und aktualisieren

Prüfen und aktualisieren Sie die CC-SG-Anwendungen, einschließlich Raritan Console (RC) und Raritan Remote Client (RRC).

So überprüfen Sie eine Anwendungsversion:

1. Wählen Sie "Administration > Anwendungen".
2. Wählen Sie in der Liste einen Anwendungsnamen aus. Beachten Sie die Zahl im Feld Version. Für einige Anwendungen wird nicht automatisch eine Versionszahl angezeigt.

So aktualisieren Sie eine Anwendung:

Handelt es sich nicht um die aktuelle Anwendungsversion, müssen Sie die Anwendung aktualisieren. Sie können die Aktualisierungsdatei für die Anwendung auf der Website von Raritan herunterladen. Eine vollständige Liste der unterstützten Anwendungsversionen finden Sie in der Kompatibilitätsmatrix auf der Support-Website von Raritan.

Am besten starten Sie den Wartungsmodus, bevor Sie Anwendungen aktualisieren. Siehe ***Wartungsmodus starten*** (auf Seite 264).

1. Speichern Sie die Datei mit der Anwendung auf Ihrem Client-PC.
2. Klicken Sie auf die Dropdown-Liste Anwendungsname, und wählen Sie die zu aktualisierende Anwendung in der Liste aus. Wenn Sie die Anwendung nicht sehen, müssen Sie die Anwendung zuerst hinzufügen. Siehe ***Anwendungen hinzufügen*** (auf Seite 284).
3. Klicken Sie auf "Durchsuchen", und wählen Sie die Datei zur Anwendungsaktualisierung im angezeigten Dialogfeld aus. Klicken Sie auf "Öffnen".
4. Der Anwendungsname wird im Anwendungsmanager im Feld "Neue Anwendungsdatei" angezeigt.
5. Klicken Sie auf "Upload". Eine Statusanzeige informiert über den Ladevorgang der neuen Anwendung. Nach dem Laden wird in einem neuen Fenster angezeigt, dass die Anwendung der CC-SG-Datenbank hinzugefügt wurde und nun verwendet werden kann.
6. Wenn das Feld "Version" nicht automatisch aktualisiert wird, geben Sie die neue Versionszahl in das Feld "Version" ein. Das Feld "Version" wird bei einigen Anwendungen automatisch aktualisiert.
7. Klicken Sie auf "Aktualisieren".

Hinweis: Benutzer, die während der Aktualisierung angemeldet sind, müssen sich von CC-SG abmelden und dann wieder anmelden, um sicherzustellen, dass die neue Version der Anwendung gestartet wird. Siehe auch **Ältere Version der Anwendung öffnet sich nach Aktualisierung** *(auf Seite 284).*

Kapitel 4 Konfigurieren von CC-SG mit dem Setup-Assistenten

Der Setup-Assistent dient als einfache Möglichkeit, Erstkonfigurationsaufgaben für CC-SG auszuführen, nachdem die Netzwerkkonfiguration abgeschlossen ist. Der Setup-Assistent führt Sie durch die Definition von Zuordnungen, das Erkennen und Hinzufügen von Geräten zu CC-SG, das Erstellen von Geräte- und Knotengruppen, das Erstellen von Benutzergruppen, das Zuordnen von Richtlinien und Rechten für Benutzergruppen und das Hinzufügen von Benutzern. Nachdem Sie den Setup-Assistenten abgeschlossen haben, können Sie Ihre Konfigurationseinstellungen einzeln ändern.

Der Setup-Assistent ist in vier Aufgaben unterteilt:

- Zuordnungen: Definieren der Kategorien und Elemente, die Sie zum Verwalten Ihrer Geräte verwenden. Siehe ***Zuordnungen im Setup-Assistenten*** (auf Seite 40).
- Geräte-Setup: Erkennen von Geräten in Ihrem Netzwerk und Hinzufügen dieser Geräte zu CC-SG. Konfigurieren von Geräteports. Siehe ***Geräte-Setup*** (auf Seite 41).
- Gruppen erstellen: Kategorisieren der Geräte und Knoten, die CC-SG in Gruppen verwaltet, und Erstellen von Richtlinien mit unbeschränktem Zugriff für jede Gruppe. Siehe ***Gruppen erstellen*** (auf Seite 43).
- Benutzerverwaltung: Hinzufügen von Benutzern und Benutzergruppen zu CC-SG, und Auswählen der Richtlinien und Berechtigungen, die den Zugriff dieser Benutzer innerhalb von CC-SG und auf Geräte und Knoten bestimmen. Siehe ***Benutzerverwaltung*** (auf Seite 46).

Weitere Informationen zu den Regeln, die von CC-SG für die Länge von Namen verwendet werden, finden Sie unter ***Benennungskonventionen*** (siehe "***Benennungsregeln***" auf Seite 457).

In diesem Kapitel

Vor der Verwendung des Setup-Assistenten 40
Zuordnungen im Setup-Assistenten 40
Geräte-Setup 41
Gruppen erstellen 43
Benutzerverwaltung 46

Vor der Verwendung des Setup-Assistenten

Bevor Sie mit der CC-SG-Konfiguration fortfahren, müssen Sie die Systemkonfiguration abschließen.

- Konfigurieren und installieren Sie Dominion-Serie- und IP-Reach-Appliances (serielle und KVM-Geräte). Ordnen Sie dabei auch eine IP-Adresse zu.

Zuordnungen im Setup-Assistenten

Kategorien und Elemente erstellen

So erstellen Sie Kategorien und Elemente im Setup-Assistenten:

1. Klicken Sie im Fenster "Setup-Assistent" auf "Zuordnungen". Klicken Sie dann im linken Fensterbereich auf "Kategorien erstellen", um den Fensterbereich "Kategorien erstellen" zu öffnen.
2. Geben Sie zum Verwalten der Geräte im Feld "Kategoriename" den entsprechenden Namen der Kategorie wie "Standort" ein.
3. Im Feld "Anwendbar auf:" können Sie angeben, ob die Kategorie für Geräte, Knoten oder beides verfügbar sein soll. Klicken Sie auf das Dropdown-Menü "Anwendbar auf:", und wählen Sie einen Wert aus der Liste aus.
4. Geben Sie in der Tabelle "Elemente" den Namen eines Elements in der Kategorie ein (beispielsweise „Raritan Deutschland“).
   - Klicken Sie auf das Symbol zum Einfügen einer neuen Zeile , um eine neue Zeile in die Tabelle "Elemente" einzufügen.
   - Sie können Elemente löschen, indem Sie eine Zeile auswählen und auf das Symbol zum Löschen von Zeilen klicken.
5. Wiederholen Sie diese Schritte, bis Sie alle Elemente in der Kategorie zu der Tabelle "Elemente" hinzugefügt haben.
6. Zum Erstellen einer anderen Kategorie klicken Sie auf "Übernehmen", um diese Kategorie zu speichern. Wiederholen Sie dann die Schritte in diesem Abschnitt, um weitere Kategorien hinzuzufügen. **Optional**
7. Klicken Sie auf OK, wenn Sie alle Kategorien und Elemente erstellt haben. Der Fensterbereich "Zuordnungsübersicht" enthält eine Liste der Kategorien und Elemente, die Sie erstellt haben.
8. Klicken Sie zum Ausführen der nächsten Aufgabe Geräte-Setup auf "Weiter". Befolgen Sie die Schritte im nächsten Abschnitt.

Geräte-Setup

Die zweite Aufgabe im Setup-Assistenten lautet Geräte-Setup. Über Geräte-Setup können Sie in Ihrem Netzwerk nach Geräten suchen, diese erkennen und sie zu CC-SG hinzufügen. Beim Hinzufügen von Geräten können Sie ein Element pro Kategorie auswählen, das dem Gerät zugewiesen werden soll.

Wichtig: Während der CC-SG-Konfiguration dürfen keine anderen Benutzer am Gerät angemeldet sein.

Geräte erkennen und hinzufügen

Der Fensterbereich Geräte erkennen wird angezeigt, wenn Sie nach der Zuordnungsaufgabe auf Weiter klicken. Sie können auch auf Geräte-Setup und dann im linken Fensterbereich in der Strukturansicht "Aufgabenassistent auf Geräte erkennen" klicken, um den gleichnamigen Fensterbereich zu öffnen.

So erkennen Sie Geräte im Setup-Assistenten und fügen Geräte hinzu:

1. Geben Sie in die Felder "Von-Adresse" und "An-Adresse" den Bereich der IP-Adressen ein, den Sie nach den Geräten durchsuchen möchten.
2. Geben Sie in das Feld "Maske" die Subnetzmaske ein, die Sie nach Geräten durchsuchen möchten.
3. Wählen Sie in der Liste "Gerätetypen" die Gerätetypen aus, nach denen Sie in dem angegebenen Bereich suchen möchten. Sie können mehrere Gerätetypen auswählen, indem Sie die STRG-Taste bei der Auswahl gedrückt halten.
4. Aktivieren Sie das Kontrollkästchen "Broadcasterkennung", wenn Sie nach Geräten im selben Subnetz suchen, in dem sich CC-SG befindet. Deaktivieren Sie das Kontrollkästchen "Broadcasterkennung", wenn Geräte in allen Subnetzen erkannt werden sollen.
5. Klicken Sie auf "Erkennen".
6. Falls CC-SG Geräte des angegebenen Typs und im angegebenen Adressenbereich gefunden hat, werden die Geräte in der Tabelle unten im Fensterbereich "Geräte erkennen" angezeigt. Klicken Sie oben im Fensterbereich auf den schwarzen Pfeil, um den oberen Bereich auszublenden. Sie vergrößern dadurch die Suchergebnisse im unteren Fensterbereich.
7. Wählen Sie in der Tabelle der erkannten Geräte das Gerät aus, das Sie CC-SG hinzufügen möchten, und klicken Sie auf "Hinzufügen". Der Fensterbereich "Gerät hinzufügen" wird angezeigt. Dieser Fensterbereich hängt vom Gerätetyp ab, den Sie hinzufügen.

8. Sie können neuen Text in die entsprechenden Felder "Gerätename" und "Beschreibung" eingeben.
9. Vergewissern Sie sich, dass die IP-Adresse, die Sie beim Hinzufügen des Geräts zu CC-SG angegebenen haben, im Feld "Geräte-IP" oder "Hostname" angezeigt wird. Geben Sie andernfalls die richtige Adresse in das Feld ein.
10. Die Nummer des TCP-Ports wird abhängig vom Gerätetyp automatisch eingefügt.
11. Geben Sie in die entsprechenden Felder Benutzername und Kennwort ein, die Sie beim Hinzufügen des Geräts zu CC-SG erstellt haben.
12. Geben Sie im Feld "Heartbeat-Zeitlimit" die Dauer in Sekunden ein, die vor Überschreitung des Zeitlimits zwischen Gerät und CC-SG verstreichen sollte.
13. Wenn Sie ein Dominion SX- oder Dominion KXII-Gerät der Version 2.2 oder höher hinzufügen, markieren Sie das Kontrollkästchen "Allow Direct Device Access" (Direkten Gerätezugriff zulassen), wenn ein lokaler Zugriff auf das Gerät zugelassen werden soll. Deaktivieren Sie das Kontrollkästchen "Lokaler Zugriff: Zulässig", wenn Sie dem Gerät keinen lokalen Zugriff erlauben möchten.
14. Wenn Sie manuell ein PowerStrip-Gerät hinzufügen, klicken Sie auf den Pfeil neben der Dropdown-Liste "Anzahl der Ports", und wählen Sie die Anzahl der PowerStrip-Ausgänge aus.
15. Wenn Sie einen IPMI-Server hinzufügen, geben Sie in die entsprechenden Felder ein Überprüfungsintervall für die Verfügbarkeitsprüfung und eine Methode für die Authentifizierung ein, die der im IPMI-Server konfigurierten Methode entsprechen muss.
16. Wenn Sie alle verfügbaren Ports des Geräts konfigurieren möchten, markieren Sie das Kontrollkästchen "Alle Ports" konfigurieren. CC-SG fügt alle Ports des Geräts zu CC-SG hinzu und erstellt einen Knoten für jeden Port.
17. Klicken Sie unten im Fensterbereich unter Gerätezuordnungen auf den Pfeil der Dropdown-Spalte "Element", die mit jeder Kategorie übereinstimmt, die Sie dem Gerät zuordnen möchten. Wählen Sie dann das gewünschte Element für die Zuordnung zum Gerät in der Liste aus.

    Hinweis: Ein Knoten oder Gerät, dem mehr als ein Element der gleichen Kategorie zugewiesen ist, wird je nach Kategorien und Elementen mehr als einmal in einer benutzerdefinierten Ansicht angezeigt.

18. Soll das Element auf das Gerät und die mit dem Gerät verbundenen Knoten angewendet werden, markieren Sie das Kontrollkästchen "Auf Knoten anwenden".

19. Wenn Sie ein weiteres Gerät hinzufügen möchten, klicken Sie auf "Übernehmen", um dieses Gerät zu speichern, und wiederholen Sie diese Schritte. **Optional.**
20. Klicken Sie auf OK, nachdem Sie alle gewünschten Geräte hinzugefügt haben. Im Fensterbereich "Geräteübersicht" wird eine Liste der Geräte angezeigt, die Sie hinzugefügt haben.
21. Klicken Sie zum Ausführen der nächsten Aufgabe Gruppen erstellen auf "Weiter". Befolgen Sie die Schritte im nächsten Abschnitt.

Gruppen erstellen

Die dritte Aufgabe im Setup-Assistenten lautet Gruppen erstellen. Über Gruppen erstellen können Sie Geräte- und Knotengruppen definieren und den Satz von Geräten oder Knoten angeben, der in jeder Gruppe enthalten sein soll. Administratoren können Zeit sparen, indem Sie Gruppen ähnlicher Geräte und Knoten anstatt jedes Gerät oder jeden Knoten einzeln verwalten.

Gerätegruppen und Knotengruppen hinzufügen

So fügen Sie Gerätegruppen und Knotengruppen im Setup-Assistenten hinzu:

1. Der Fensterbereich "Gerätegruppe: Das neue Fenster wird angezeigt, wenn Sie nach Abschluss der Geräte-Setup-Aufgabe auf "Weiter" klicken. Sie können auch auf "Gruppen erstellen" und dann im linken Fensterbereich in der Strukturansicht "Aufgabenassistent auf Gerätegruppen hinzufügen" klicken, um den Fensterbereich "Gerätegruppe: "Geräte beschreiben".
2. Geben Sie in das Feld "Gruppenname" einen Namen für die Gerätegruppe ein, die Sie erstellen möchten.
3. Sie haben zwei Möglichkeiten, Geräte einer Gruppe hinzuzufügen: Geräte auswählen und Geräte beschreiben. Auf der Registerkarte "Geräte auswählen" können Sie auswählen, welche Geräte zur Gruppe zugeordnet werden sollen. Wählen Sie die Geräte dazu einfach in der Liste der verfügbaren Geräte aus. Auf der Registerkarte "Geräte beschreiben" können Sie Regeln angeben, die Geräte beschreiben. Geräte, deren Parameter diesen Regeln entsprechen, werden der Gruppe hinzugefügt.
   - **Geräte auswählen**

     a. Klicken Sie im Fensterbereich "Gerätegruppe: Neu" auf die Registerkarte "Geräte beschreiben".

     b. Wählen Sie in der Liste "Verfügbar" das Gerät aus, das Sie der Gruppe hinzufügen möchten, und klicken Sie dann auf "Hinzufügen", um das Gerät in die Liste "Ausgewählt" zu verschieben. Geräte, die sich in der Liste "Ausgewählt" befinden, werden der Gruppe hinzugefügt.

c. Wählen Sie zum Entfernen eines Geräts aus der Gruppe den Gerätenamen in der Liste "Ausgewählt" aus, und klicken Sie auf "Entfernen".

d. Sie können das Gerät in der Liste "Verfügbar" oder "Ausgewählt" suchen. Geben Sie den Suchbegriff in das Feld unter der Liste ein, und klicken Sie auf "Los".

- **Geräte beschreiben**

a. Klicken Sie im Fensterbereich "Gerätegruppe: Neu" auf die Registerkarte "Geräte beschreiben". Auf der Registerkarte "Geräte beschreiben" erstellen Sie eine Regeltabelle, in der die Geräte beschrieben werden, die Sie der Gruppe zuordnen möchten.

b. Klicken Sie auf das Symbol zum Einfügen einer neuen Zeile , um eine neue Zeile in die Tabelle einzufügen.

c. Doppelklicken Sie auf die Zelle, die für jede Spalte erstellt wurde, um das Dropdown-Menü anzuzeigen. Wählen Sie in jeder Liste die gewünschten Regelkomponenten aus.

4. Markieren Sie das Kontrollkästchen "Richtlinie mit unbeschränktem Zugriff für Gruppe erstellen", wenn Sie eine Richtlinie für diese Gerätegruppe erstellen möchten, die jederzeit den Zugriff auf alle Knoten und Geräte in der Gruppe mit Steuerungsberechtigung zulässt.

5. Um eine weitere Gerätegruppe hinzuzufügen, klicken Sie auf "Übernehmen", um diese Gruppe zu speichern, und wiederholen Sie diese Schritte. **Optional.**

6. Klicken Sie auf OK, nachdem Sie alle gewünschten Gerätegruppen hinzugefügt haben. Der Fensterbereich "Knotengruppe: Neu" wird geöffnet. Sie können auch auf "Gruppen erstellen" und dann im linken Fensterbereich in der Strukturansicht "Aufgabenassistent auf Knotengruppen hinzufügen" klicken, um den Fensterbereich "Knotengruppe: "Geräte beschreiben".

7. Geben Sie in das Feld "Gruppenname" einen Namen für die Knotengruppe ein, die Sie erstellen möchten.

8. Sie haben zwei Möglichkeiten, Knoten einer Gruppe hinzuzufügen: Knoten auswählen und Knoten beschreiben. Auf der Registerkarte "Knoten auswählen" können Sie auswählen, welche Knoten zur Gruppe zugeordnet werden sollen. Wählen Sie die Knoten dazu einfach in der Liste der verfügbaren Knoten aus. Auf der Registerkarte "Knoten beschreiben" können Sie Regeln angeben, die Knoten beschreiben. Knoten, deren Parameter diesen Regeln entsprechen, werden der Gruppe hinzugefügt.

   - **Knoten auswählen**

a. Klicken Sie im Fensterbereich "Knotengruppe: Neu" auf die Registerkarte "Geräte beschreiben".

b. Wählen Sie in der Liste "Verfügbar" den Knoten aus, den Sie der Gruppe hinzufügen möchten, und klicken Sie dann auf "Hinzufügen", um den Knoten in die Liste "Ausgewählt" zu verschieben. Knoten in der Liste "Ausgewählt" werden der Gruppe hinzugefügt.

c. Wählen Sie zum Entfernen eines Knotens aus der Gruppe den Knotennamen in der Liste "Ausgewählt" aus, und klicken Sie auf "Entfernen".

d. Sie können den Knoten in der Liste "Verfügbar" oder "Ausgewählt" suchen. Geben Sie den Suchbegriff in das Feld unter der Liste ein, und klicken Sie auf "Los".

- **Knoten beschreiben**

a. Klicken Sie im Fensterbereich "Knotengruppe: Neu" auf die Registerkarte "Geräte beschreiben". Auf der Registerkarte "Knoten beschreiben" erstellen Sie eine Regeltabelle, in der die Knoten beschrieben werden, die Sie der Gruppe zuordnen möchten.

b. Klicken Sie auf das Symbol zum Einfügen einer neuen Zeile , um eine neue Zeile in die Tabelle einzufügen.

c. Doppelklicken Sie auf die Zelle, die für jede Spalte erstellt wurde, um das Dropdown-Menü anzuzeigen. Wählen Sie in jeder Liste die gewünschten Regelkomponenten aus. Siehe ***Richtlinien für die Zugriffssteuerung*** (auf Seite 210).

9. Wählen Sie das Kontrollkästchen "Richtlinie mit unbeschränktem Zugriff für Gruppe erstellen", wenn Sie eine Richtlinie für diese Knotengruppe erstellen möchten, die jederzeit den Zugriff auf alle Knoten in der Gruppe mit Steuerungsberechtigung zulässt.

10. Um eine weitere Knotengruppe hinzuzufügen, klicken Sie auf "Übernehmen", um diese Gruppe zu speichern, und wiederholen Sie diese Schritte. **Optional.**

11. Klicken Sie auf OK, nachdem Sie alle gewünschten Knotengruppen hinzugefügt haben. Im Fensterbereich "Gruppenübersicht" wird eine Liste der Gruppen angezeigt, die Sie hinzugefügt haben.

12. Klicken Sie zum Ausführen der nächsten Aufgabe Benutzerverwaltung auf Weiter. Befolgen Sie die Schritte im nächsten Abschnitt.

Benutzerverwaltung

Die vierte Aufgabe im Setup-Assistenten lautet Benutzerverwaltung. Mit Benutzerverwaltung können Sie die Berechtigungen und Richtlinien auswählen, die den Zugriff und die Aktivitäten der Benutzergruppen bestimmen. Berechtigungen legen fest, welche Aktivitäten die Mitglieder der Benutzergruppe in CC-SG ausführen können. Richtlinien legen fest, welche Geräte und Knoten die Mitglieder der Gruppe anzeigen und bearbeiten können. Richtlinien basieren auf den Kategorien und Elementen. Nachdem Sie Benutzergruppen erstellt haben, können Sie einzelne Benutzer definieren und sie diesen Benutzergruppen hinzufügen.

Benutzergruppen und Benutzer hinzufügen

Der Fensterbereich "Benutzergruppe hinzufügen" wird angezeigt, wenn Sie nach der Aufgabe zum Erstellen von Gruppen auf "Weiter" klicken. Sie können auch auf Benutzermanagement und dann im linken Fensterbereich in der Strukturansicht "Aufgabenassistent auf Benutzergruppe hinzufügen" klicken, um den gleichnamigen Fensterbereich zu öffnen.

So fügen Sie Benutzergruppen und Benutzer im Setup-Assistenten hinzu:

1. Geben Sie in das Feld "Benutzergruppenname" einen Namen für die Benutzergruppe ein, die Sie erstellen möchten. Benutzergruppennamen können aus bis zu 64 Zeichen bestehen.
2. Geben Sie in das Feld "Beschreibung" eine Beschreibung für die Benutzergruppe ein.
3. Um für den Zugriff auf Geräte, auf denen diese Funktion aktiviert ist, eine maximal mögliche Anzahl an KVM-Sitzungen pro Benutzer dieser Benutzergruppe festzulegen, aktivieren Sie das Kontrollkästchen "Limit Number of KVM Sessions per Device" (Einschränken der Anzahl an KVM-Sitzungen pro Gerät) und wählen Sie im Feld "Max KVM Sessions (1-8)" (Max. KVM-Sitzungen (1-8)) die zulässige Anzahl an Sitzungen aus. **Optional.** Weitere Informationen finden Sie unter ***Anzahl an KVM-Sitzungen pro Benutzer einschränken*** (auf Seite 192).
4. Klicken Sie auf die Registerkarte "Berechtigungen", wählen Sie dann die Kontrollkästchen aus, die den Berechtigungen oder CC-SG-Aktivitäten entsprechen, die Sie der Benutzergruppe zuordnen möchten.
5. Im Bereich "Knotenzugriff" können Sie angeben, ob die Benutzergruppe über Zugriff auf In Band- und Out-of-Band-Knoten und auf Funktionen zur Stromversorgungsverwaltung verfügen soll. Markieren Sie die Kontrollkästchen, die den Zugriffsarten entsprechen, die Sie der Gruppe zuordnen möchten.

6. Klicken Sie auf die Registerkarte "Richtlinien".
7. Wählen Sie in der Liste "Alle Richtlinien" die Richtlinie aus, die Sie der Benutzergruppe zuweisen möchten, und klicken Sie auf "Hinzufügen", um die Richtlinie in die Liste "Ausgewählte Richtlinien" zu verschieben. Richtlinien in der Liste "Ausgewählte Richtlinien" werden der Benutzergruppe zugewiesen. Wiederholen Sie diesen Schritt, um der Benutzergruppe weitere Richtlinien zuzuweisen.
8. Wählen Sie zum Löschen einer Richtlinie in der Benutzergruppe den Namen der Richtlinie in der Liste "Ausgewählte Richtlinien" aus, und klicken Sie auf "Löschen".
9. Wenn Sie Benutzer, für die Remoteauthentifizierung verwendet wird, mit Active Directory-Modulen verknüpfen möchten, klicken Sie auf die Registerkarte "Active Directory-Zuordnungen", sofern die AD konfigurierte Registerkarte "Active Directory-Zuordnungen" nicht ausgeblendet ist. Markieren Sie das Kontrollkästchen, das jedem Active Directory-Modul entspricht, das Sie mit dieser Benutzergruppe verknüpfen möchten.
10. Um eine weitere Benutzergruppe hinzuzufügen, klicken Sie auf "Übernehmen", um diese Gruppe zu speichern, und wiederholen Sie diese Schritte. **Optional.**
11. Klicken Sie auf OK, nachdem Sie alle gewünschten Benutzergruppen hinzugefügt haben. Der Fensterbereich "Benutzer hinzufügen" wird angezeigt. Sie können auch auf Benutzermanagement und dann im linken Fensterbereich in der Strukturansicht "Aufgabenassistent auf Benutzer hinzufügen" klicken, um den gleichnamigen Fensterbereich zu öffnen.
12. Geben Sie im Feld "Benutzername" den Namen für den Benutzer zur Anmeldung bei CC-SG ein.
13. Markieren Sie das Kontrollkästchen "Anmeldung aktiviert", wenn der Benutzer über die Anmeldeberechtigung für CC-SG verfügen soll.
14. Markieren Sie das Kontrollkästchen "Remoteauthentifizierung" nur, wenn der Benutzer mithilfe eines anderen Servers wie TACACS+, RADIUS, LDAP oder AD authentifiziert werden soll. Bei der Remoteauthentifizierung wird kein Kennwort benötigt. Die Felder "Neues Kennwort" und "Neues Kennwort" erneut eingeben sind deaktiviert wenn das Feld "Remoteauthentifizierung" markiert ist.
15. Geben Sie in die Felder "Neues Kennwort" und "Neues Kennwort erneut eingeben" das Kennwort ein, das der Benutzer zur Anmeldung in CC-SG verwenden soll.
16. Markieren Sie das Kontrollkästchen "Änderung des Kennworts" bei der nächsten Anmeldung erzwingen, wenn der Benutzer gezwungen werden soll, das zugewiesene Kennwort bei der nächsten Anmeldung zu ändern.
17. Markieren Sie das Kontrollkästchen "Änderung des Kennworts periodisch erzwingen", wenn Sie festlegen möchten, wie oft der Benutzer zur Kennwortänderung gezwungen werden soll.

18. Geben Sie in das Feld "Gültigkeitsdauer (in Tagen)" die Anzahl von Tagen ein, die der Benutzer dasselbe Kennwort verwenden kann, bevor eine Änderung erzwungen wird.
19. Geben Sie die E-Mail-Adresse des Benutzers in das Feld "E-Mail-Adresse" ein.
20. Klicken Sie auf den Pfeil neben der Dropdown-Liste "Benutzergruppe", und wählen Sie in der Liste die Benutzergruppe aus, der Sie den Benutzer zuweisen möchten.
21. Wenn Sie einen weiteren Knoten hinzufügen möchten, klicken Sie auf Übernehmen, um diesen Benutzer zu speichern. Wiederholen Sie dann die Schritte in diesem Abschnitt, um weitere Benutzer hinzuzufügen.
22. Klicken Sie auf OK, nachdem Sie alle gewünschten Benutzer hinzugefügt haben. Im Fensterbereich "Benutzerübersicht" wird eine Liste der Benutzergruppen und Benutzer angezeigt, die Sie hinzugefügt haben. **Optional.**

Kapitel 5 Zuordnungen, Kategorien und Elemente

In diesem Kapitel

Zuordnungen 49
Kategorien und Elemente hinzufügen, bearbeiten und löschen.....50
Kategorien und Elemente per CSV-Dateiimport hinzufügen.....52

Zuordnungen

Sie können zur Organisation der von CC-SG verwalteten Geräte Zuordnungen einrichten. Jede Zuordnung enthält eine Kategorie (oberste Gruppe) und zugehörige Elemente (Kategorie-Untergruppen). Beispiel: Sie haben Raritan-Geräte, die Zielserver in einem Rechenzentrum in Amerika, Asien-Pazifik und Europa verwalten. Sie können eine Zuordnung einrichten, die diese Geräte nach Standort organisiert. Sie können dann CC-SG so anpassen, dass Ihre Raritan-Geräte und Knoten nach der von Ihnen ausgewählten Kategorie (Standort) und den zugewiesenen Elementen (Amerika, Asien-Pazifik und Europa) über die CC-SG-Schnittstelle angezeigt werden. Sie können die Organisation und Anzeige Ihrer Server in CC-SG beliebig nach Ihren Wünschen anpassen.

Zuordnungsterminologie

- Zuordnungen: Beziehungen zwischen Kategorien und Kategorieelementen zu Knoten und Geräten.
- Kategorie: Eine Variable, die bestimmte Werte (genannt Elemente) enthält. "Standort" ist ein Beispiel für eine Kategorie, die Elemente wie "Amerika" und "Asien-Pazifik" enthält. "Betriebssystemtyp" ist eine weitere Kategorie, die Elemente wie "Windows", "Unix" oder "Linux" enthalten kann.
- Elemente: Die Werte einer Kategorie. Das Element "Amerika" gehört beispielsweise zur Kategorie "Standort".

Zuordnungsbestimmende Kategorien und Elemente

Raritan-Geräte und Knoten werden nach Kategorien und Elementen organisiert. Jedes Paar Kategorie/Element wird einem Gerät und/oder einem Knoten zugeordnet.

Eine Kategorie ist eine Gruppe gleichartiger Elemente.

Kategorie	Elemente
Betriebssystemtyp	Unix, Windows, Linux

Kategorie	Elemente
Abteilung	Vertrieb, IT, Technik

Kategorien und Elemente können auch von Richtlinien verwendet werden, um den Benutzerzugriff auf Server zu steuern. Mit dem Paar Kategorie/Element (Standort/Amerika) können Sie beispielsweise eine Richtlinie erstellen, um den Benutzerzugriff auf Server in Amerika zu steuern. Siehe ***Richtlinien für die Zugriffssteuerung*** (auf Seite 210).

Sie können einem Knoten oder Gerät über den CSV-Dateiimport mehr als ein Element einer Kategorie zuweisen.

Geräte und Knoten werden beim Hinzufügen zu CC-SG mit den vordefinierten Kategorien und Elementen verknüpft. Wenn Sie Knoten- und Gerätegruppen erstellen und ihnen Richtlinien zuordnen, definieren Sie anhand der Kategorien und Elemente, welche Knoten und Geräte zu den einzelnen Gruppen gehören.

Zuordnungen erstellen

Sie haben zwei Möglichkeiten, Zuordnungen zu erstellen: Setup-Assistent und Zuordnungsmanager.

- Setup-Assistent vereint viele Konfigurationsaufgaben mithilfe einer automatisierten Schnittstelle. Der Setup-Assistent wird für die CC-SG-Erstkonfiguration empfohlen. Nachdem Sie den Setup-Assistenten abgeschlossen haben, können Sie Ihre Konfigurationseinstellungen einzeln ändern. Siehe ***Konfigurieren von CC-SG mit dem Setup-Assistenten*** (auf Seite 39).
- Mit dem Zuordnungsmanager können Sie nur mit Zuordnungen arbeiten. Konfigurationsaufgaben werden nicht automatisiert. Mit dem Zuordnungsmanager können Sie auch Ihre Zuordnungen bearbeiten, nachdem Sie den Setup-Assistenten verwendet haben. Siehe ***Kategorien und Elemente hinzufügen, bearbeiten und löschen*** (auf Seite 50).

Kategorien und Elemente hinzufügen, bearbeiten und löschen

Mit dem Zuordnungsmanager können Sie Kategorien und Elemente hinzufügen, ändern oder löschen.

Hinweis: Standardmäßig verwendet CC-SG die Standardkategorienamen für "Systemtyp" und "US-Bundesstaaten und -Staatsgebiete" in Englisch.

Kategorien hinzufügen

So fügen Sie eine Kategorie hinzu:

1. Wählen Sie "Zuordnungen > Zuordnung".
2. Klicken Sie auf "Hinzufügen". Das Fenster "Kategorie hinzufügen" wird geöffnet.
3. Geben Sie im Feld "Kategoriename" einen Kategorienamen ein. Weitere Informationen zu den Regeln, die von CC-SG für die Länge von Namen verwendet werden, finden Sie unter ***Benennungskonventionen*** (siehe "***Benennungsregeln***" auf Seite 457).
4. Wählen Sie den Datentyp für Elemente.
   - Wählen Sie "Zeichenfolge", wenn der Wert als Text gelesen wird.
   - Wählen Sie "Ganze Zahl", wenn der Wert eine Zahl ist.
5. Wählen Sie im Feld "Anwendbar auf", worauf diese Kategorie angewendet wird: Geräte, Knoten oder Geräte und Knoten.
6. Klicken Sie auf "OK", um die neue Kategorie zu erstellen. Der neue Kategoriename wird im Feld Kategoriename angezeigt.

Kategorien löschen

Durch das Löschen einer Kategorie werden alle in dieser Kategorie erstellten Elemente gelöscht. Die gelöschte Kategorie wird in der Knoten- oder Gerätestrukturansicht nicht mehr angezeigt, sobald das Fenster aktualisiert wird oder der Benutzer sich in CC-SG ab- und wieder anmeldet.

So löschen Sie eine Kategorie:

1. Wählen Sie "Zuordnungen > Zuordnung".
2. Klicken Sie auf die Dropdown-Liste "Kategoriename", und wählen Sie die zu löschende Kategorie aus.
3. Klicken Sie im Fensterbereich "Kategorie" auf "Löschen", um die Kategorie zu löschen. Das Fenster "Kategorie löschen" wird angezeigt.
4. Klicken Sie auf "Ja", um die Kategorie zu löschen.

Elemente hinzufügen

So fügen Sie ein Element hinzu:

1. Wählen Sie "Zuordnungen > Zuordnung".

2. Klicken Sie auf die Dropdown-Liste "Kategoriename", und wählen Sie die Kategorie aus, der Sie ein neues Element hinzufügen möchten.
3. Klicken Sie auf das Symbol zum Einfügen einer neuen Zeile.
4. Geben Sie den Namen des neuen Elements in die leere Zeile ein. Weitere Informationen zu den Regeln, die von CC-SG für die Länge von Namen verwendet werden, finden Sie unter ***Benennungskonventionen*** (siehe "***Benennungsregeln***" auf Seite 457). Bei Elementnamen wird die Groß- und Kleinschreibung berücksichtigt.
5. Klicken Sie zum Speichern der Änderungen auf OK.

Kategorien und Elemente per CSV-Dateiimport hinzufügen

Sie können Kategorien und Elemente zu CC-SG hinzufügen, indem Sie eine CSV-Datei, in der die Werte enthalten sind, importieren. Sie benötigen die Berechtigungen "Benutzersicherheitsverwaltung" und "CC-Setup und -Steuerung", um Kategorien und Elemente importieren bzw. exportieren zu können.

Anforderungen an CSV-Dateien – Kategorien und Elemente

Durch die CSV-Datei für Kategorien und Elemente werden die Kategorien, deren zugewiesene Elemente, deren Typ und deren mögliche Gültigkeit für Geräte, Knoten oder beides definiert.

- Alle CATEGORY (Kategorie)- und CATEGORYELEMENT (Kategorie-Element)-Einträge sind zusammengehörig. Ein CATEGORY (Kategorie)-Eintrag muss über einen oder mehrere CATEGORYELEMENT (Kategorie-Element)-Einträge verfügen.
- CATEGORYELEMENT (Kategorie-Element)-Einträge erfordern keinen zugehörigen CATEGORY (Kategorie)-Eintrag, wenn diese CATEGORY (Kategorie) bereits in CC-SG vorhanden ist. Wenn Sie beispielsweise weitere Elemente zu einer bestehenden Kategorie hinzufügen möchten, müssen Sie keine Zeile zum Neudefinieren der Kategorie, zu der das neue Element gehört, einfügen.
- Exportieren Sie eine Datei aus CC-SG, um die Kommentare anzuzeigen. Diese enthalten alle Tags und Parameter, die zum Erstellen einer gültigen CSV-Datei erforderlich sind. Siehe ***Kategorien und Elemente exportieren*** (auf Seite 54).
- Erfüllen Sie die zusätzlichen Anforderungen für alle CSV-Dateien. Siehe ***Häufige Anforderungen an CSV-Dateien*** (siehe "***Häufige Anforderungen für CSV-Dateien***" auf Seite 434).

So fügen Sie eine Kategorie zur CSV-Datei hinzu:

Spalte 1	Spalte 2	Spalte 3	Spalte 4	Spalte 5
ADD (Hinzufügen)	CATEGORY (Kategorie)	Kategoriename	Typ	Übernehmen
			Werte: ▪ Ganze Zahl ▪ Zeichenfolge Die Standardeinstellung ist Zeichenfolge.	Werte: ▪ Knoten ▪ Geräte ▪ Beides Die Standardeinstellung ist Beides.

So fügen Sie ein Element zur CSV-Datei hinzu:

Spalte 1	Spalte 2	Spalte 3	Spalte 4
ADD (Hinzufügen)	CATEGORYELEMENT (Kategorie-Element)	Kategoriename	Elementname

Beispiel-CSV-Datei für Kategorien und Elemente

ADD (Hinzufügen), CATEGORY (Kategorie), OS (Betriebssystem), Zeichenfolge, Knoten

ADD (Hinzufügen), CATEGORYELEMENT (Kategorie-Element), OS (Betriebssystem), UNIX

ADD (Hinzufügen), CATEGORYELEMENT (Kategorie-Element), OS (Betriebssystem), WINDOWS

ADD (Hinzufügen), CATEGORYELEMENT (Kategorie-Element), OS (Betriebssystem), LINUX

ADD (Hinzufügen), CATEGORY (Kategorie), Position, Zeichenfolge, Gerät

ADD (Hinzufügen), CATEGORYELEMENT (Kategorie-Element), Position, Gang 1

ADD (Hinzufügen), CATEGORYELEMENT (Kategorie-Element), Position, Gang 2

ADD (Hinzufügen), CATEGORYELEMENT (Kategorie-Element), Position, Gang 3

Kategorien und Elemente importieren

Wenn Sie die CSV-Datei erstellt haben, überprüfen Sie sie auf Fehler und importieren Sie sie anschließend.

Doppelte Einträge werden übersprungen und somit nicht hinzugefügt.

So importieren Sie die CSV-Datei:

1. Wählen Sie "Administration > Importieren >Kategorien importieren".
2. Klicken Sie auf "Durchsuchen" und wählen Sie die zu importierende CSV-Datei aus. Klicken Sie auf "Öffnen".
3. Klicken Sie auf Überprüfen. Die Dateiinhalte werden im Bereich "Analysebericht" angezeigt.
   - Wenn die Datei ungültig ist, wird eine Fehlermeldung angezeigt. Klicken Sie auf "OK". Im Bereich "Probleme" auf der Seite wird eine Beschreibung der Dateiprobleme aufgeführt. Klicken Sie auf "In Datei speichern", um die Liste der Probleme zu speichern. Korrigieren Sie die CSV-Datei und versuchen Sie sie anschließend erneut zu validieren. Siehe ***Problembehebung bei CSV-Dateien*** (auf Seite 436).
4. Klicken Sie auf "Importieren".
5. Die Ergebnisse des Imports werden im Bereich "Aktionen" angezeigt. Erfolgreich importierte Elemente werden grün dargestellt. Nicht erfolgreich importierte Elemente werden rot dargestellt. Elemente, die aufgrund eines bereits vorhandenen oder bereits importierten Duplikats nicht erfolgreich importiert wurden, werden ebenso rot dargestellt.
6. Um weitere Details zu den Importergebnissen anzuzeigen, rufen Sie den Überwachungslistenbericht auf. Siehe ***Einträge in der Überwachungsliste für Importe*** (auf Seite 435).

Kategorien und Elemente exportieren

In der Exportdatei sind als erstes Kommentare enthalten, die jedes Element in der Datei beschreiben. Die Kommentare können als Anweisungen zum Erstellen einer Datei oder zum Importieren verwendet werden.

So exportieren Sie Kategorien und Elemente:

1. Wählen Sie "Administration > Exportieren >Kategorien exportieren".
2. Klicken Sie auf "In Datei exportieren".
3. Geben Sie einen Namen für die Datei ein, und wählen Sie den Speicherort aus.
4. Klicken Sie auf Speichern.

Wenn Sie die Datei zum ersten Mal in Excel speichern, wählen Sie "Speichern unter" und STELLEN SIE SICHER, dass Sie CSV als Dateityp auswählen. Anschließend speichert Excel die Datei automatisch als CSV-Datei.

Wenn Sie den Dateityp nicht korrekt festlegen, wird die Datei beschädigt und kann nicht für den Import verwendet werden.

Kapitel 6 Geräte, Gerätegruppen und Ports

Informationen darüber, wie Sie an andere Geräte angeschlossene Raritan-PowerStrip-Geräte zu CC-SG hinzufügen, finden Sie unter ***Verwaltete PowerStrips*** (auf Seite 111).

Hinweis: Verwenden Sie zur Konfiguration von iLO/RILOE-Geräten, IPMI-Geräten, Dell DRAC-Geräten, IBM RSA-Geräten oder anderen Geräten, die nicht von Raritan hergestellt wurden, das Menü "Knoten hinzufügen", und fügen Sie diese Elemente als Schnittstelle hinzu. Siehe **Knoten, Knotengruppen und Schnittstellen** *(auf Seite 121).*

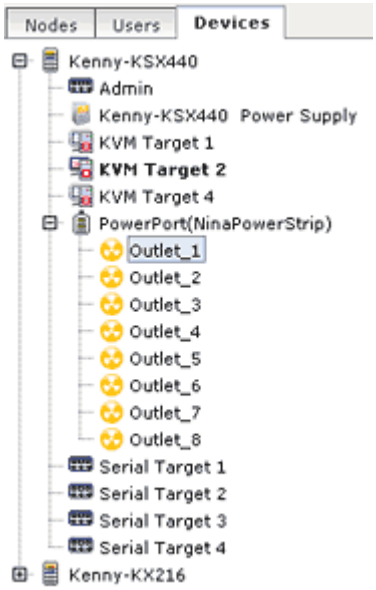
In diesem Kapitel

Geräte anzeigen 57
Geräte suchen 61
Geräte erkennen 62
Geräte hinzufügen 63
Geräte bearbeiten 67
Ändern der HTTP- und HTTPS-Ports für ein KX2-Gerät 68
PowerStrip- oder Dominion PX-Geräte bearbeiten 68
Hinweise zu einem Geräteprofil hinzufügen 69
Einsatzort und Kontakte zu einem Geräteprofil hinzufügen 69
Geräte löschen 70
Ports konfigurieren 70
Ports bearbeiten 73
Ports löschen 74
An KX2 angeschlossenes Blade-Chassis-Gerät konfigurieren 74
Blade-Server-Ports als normale KX2-Ports wiederherstellen 81
Massenkopieren für Gerätezuordnungen, Einsatzort und Kontakte 82
Konfigurieren der mit KX2 2.3 oder höher verbundenen analogen KVM-Switches 83
Gerätegruppenmanager 85
Geräte per CSV-Dateiimport hinzufügen 92
Gerät aktualisieren 99
Gerätekonfiguration sichern 100
Gerätekonfiguration wiederherstellen 101
Gerätekonfiguration kopieren 105
Gerät neu starten 106
Gerät anpingen 106
CC-SG-Verwaltung eines Geräts unterbrechen 106
Geräteverwaltung fortsetzen 107
Geräteverwaltung mit einer geplanten Aufgabe unterbrechen und fortsetzen 107
Gerätestrommanager 108
Verwaltungsseite eines Geräts aufrufen 109
Benutzerverbindung trennen 109
Sonderzugriff auf Paragon II-Systemgeräte 110

Geräte anzeigen

Die Registerkarte "Geräte"

Klicken Sie auf die Registerkarte "Geräte", um alle Geräte anzuzeigen, die in CC-SG verwaltet werden.



Die konfigurierten Ports der einzelnen Geräte werden unter den Geräten, zu denen sie gehören, verschachtelt angezeigt. Geräte mit konfigurierten Ports werden in der Liste mit einem Pluszeichen (+) angezeigt. Klicken Sie auf das Pluszeichen (+) oder das Minuszeichen (-), um die Portliste ein- bzw. auszublenden.

Geräte- und Portsymbole

Die KVM-, Stromversorgungs- und seriellen Geräte und Ports werden zur einfacheren Unterscheidung in der Gerätestrukturansicht durch unterschiedliche Symbole gekennzeichnet. Bewegen Sie den Mauszeiger auf ein Symbol in der Gerätestruktur, um einen Tooltip mit Informationen zum Gerät oder Port anzuzeigen.

Symbol	Bedeutung
	Gerät verfügbar
	KVM-Port verfügbar oder verbunden

Symbol	Bedeutung
	KVM-Port inaktiv
	Serieller Port verfügbar
	Serieller Port nicht verfügbar
	Verwaister Port (Weitere Informationen zum Ghosting-Modus finden Sie im **Benutzerhandbuch für Paragon II-Geräte** von Raritan.)
	Gerät wurde angehalten
	Gerät nicht verfügbar
	Powerstrip
	Ausgangsport
	Blade-Chassis verfügbar
	Blade-Chassis nicht verfügbar
	Blade-Server verfügbar
	Blade-Server nicht verfügbar

Portsortieroptionen

Auf der Registerkarte "Geräte" werden konfigurierte Ports unter ihren übergeordneten Geräten verschachtelt angezeigt. Sie können die Sortierung der Ports ändern. Nach Status aufgelistete Ports werden innerhalb ihrer Verbindungsstatusgruppe alphabetisch sortiert. Geräte werden ebenfalls entsprechend sortiert angezeigt.

So sortieren Sie die Ports auf der Registerkarte "Geräte":

1. Wählen Sie "Geräte > Portsortieroptionen".

2. Wählen Sie "Nach Portname", "Nach Portstatus" oder "Nach Portnummer" aus, um die Ports im Gerät alphabetisch nach Namen, nach Verfügbarkeitsstatus oder numerisch nach Portnummer zu sortieren.

Hinweis: Für Blade-Server ohne integrierten KVM-Switch, wie z. B. HP BladeSystem-Server, ist das übergeordnete Gerät das virtuelle Blade-Chassis, das von CC-SG erstellt wird, und nicht das KX2-Gerät. Diese Server werden nur innerhalb des virtuellen Blade-Chassis-Geräts sortiert, d. h. sie werden nicht in der Reihenfolge mit den anderen KX2-Ports angezeigt, es sei denn, Sie stellen diese Blade-Server-Ports wieder als normale KX2-Ports her. Siehe **Blade-Server-Ports als normale KX2-Ports wiederherstellen** *(auf Seite 81).*

Fenster "Geräteprofil"

Wenn Sie auf der Registerkarte "Geräte" ein Gerät auswählen, wird das Fenster "Geräteprofil" mit Informationen zum ausgewählten Gerät angezeigt.

Wenn ein Gerät nicht verfügbar ist, werden die Informationen im Fenster "Geräteprofil" mit Lesezugriff angezeigt. Sie können nicht verfügbare Geräte löschen. Siehe ***Gerät löschen*** (siehe "***Geräte löschen***" auf Seite 70).

Das Geräteprofil verfügt über Registerkarten, die Informationen über das Gerät enthalten.

Registerkarte "Zuordnungen"

Die Registerkarte "Zuordnungen" enthält alle Kategorien und Elemente, die dem Knoten zugeordnet sind. Sie können die Zuordnungen durch eine unterschiedliche Auswahl ändern. Siehe ***Zuordnungen, Kategorien und Elemente*** (auf Seite 49).

Registerkarte "Einsatzort & Kontakte"

Die Registerkarte "Einsatzort & Kontakte" enthält Informationen zu Einsatzort und Kontakten (z. B. Telefonnummern), die bei der Arbeit mit einem Gerät erforderlich sind. Sie können die Informationen in den Feldern durch Eingabe neuer Informationen ändern. Siehe ***Einsatzort und Kontakte zu einem Geräteprofil hinzufügen*** (auf Seite 69).

Registerkarte "Hinweise"

Die Registerkarte "Hinweise" enthält ein Tool, mit dem Benutzer anderen Benutzern Hinweise zu einem Gerät hinterlassen können. Alle Hinweise werden mit dem Datum, dem Benutzernamen und der IP-Adresse des Benutzers angezeigt, der den Hinweis hinzugefügt hat.

Wenn Sie über die Berechtigung "Geräte-, Port- und Knotenverwaltung" verfügen, können Sie durch Klicken auf "Löschen" alle Knoten aus dem Knotenprofil löschen.

Siehe ***Hinweise zu einem Geräteprofil hinzufügen*** (auf Seite 69).

Registerkarte "Blades"

Blade-Chassis-Knoten, wie z. B. IBM BladeCenter, enthalten die Registerkarte "Blades". Die Registerkarte "Blades" enthält Informationen zu den Blade-Servern im Blade-Chassis.

Sie können nicht nur die Blade-Informationen anzeigen, sondern auch die nicht konfigurierten Blade-Server konfigurieren, indem Sie die den Blade-Servern entsprechenden Kontrollkästchen auf dieser Registerkarte auswählen.

Siehe ***Slots auf einem Blade-Chassis-Gerät konfigurieren*** (auf Seite 77).

Topologieansicht

Die Topologieansicht zeigt das strukturelle Setup aller angeschlossenen Appliances in Ihrer Konfiguration an.

Bis Sie die Topologieansicht schließen, ersetzt diese Ansicht den Bildschirm "Geräteprofil", der normalerweise angezeigt wird, wenn ein Gerät ausgewählt wird.

So öffnen Sie die Topologieansicht:

1. Klicken Sie auf die Registerkarte "Geräte", und wählen Sie das Gerät aus, dessen Topologieansicht Sie anzeigen möchten.
2. Wählen Sie "Geräte > Gerätemanager > Topologieansicht". Die Topologieansicht für das ausgewählte Gerät wird angezeigt.
   - Klicken Sie auf + oder -, um die Ansicht ein- oder auszublenden.

Kontextmenüoptionen auf der Registerkarte Geräte

Sie können auf der Registerkarte Geräte mit der rechten Maustaste auf ein Gerät oder einen Port klicken, um ein Menü mit Befehlen anzuzeigen, die für das ausgewählte Gerät oder den ausgewählten Port verfügbar sind.

Geräte suchen

Mithilfe der Registerkarte "Geräte" können Sie in der Struktur nach Geräten suchen. Die Suche zeigt Geräte nur als Ergebnisse ohne Portnamen an. Die Suchmethode kann unter "Mein Profil" konfiguriert werden. Siehe ***Eigene Standardsucheinstellungen ändern*** (auf Seite 206).

So suchen Sie ein Gerät:

- Geben Sie unten auf der Registerkarte "Geräte" in das Feld "Gerät suchen" eine Suchzeichenfolge ein, und drücken Sie die Eingabetaste.
- Die Suchfunktion unterstützt Platzhalter in der Suchzeichenfolge. Siehe ***Platzhalter für die Suche*** (auf Seite 62).

Platzhalter für die Suche

Platzhalter	Beschreibung
?	Beliebiges Zeichen
[-]	Zeichen in einem Bereich
*	Kein oder mehrere Zeichen

Beispiele mit Platzhaltern

Beispiel	Beschreibung
KX?	Sucht nach KX1 und KXZ, aber nicht nach KX1Z.
KX*	Sucht nach KX1, KX, KXZ und KX1Z.
KX[0-9][0-9]T	Sucht nach KX95T, KX66T, aber nicht nach KXZ und KX5PT.

Geräte erkennen

Mit Geräte erkennen wird eine Suche nach allen Geräten in Ihrem Netzwerk gestartet. Nach dem Erkennen der Geräte können Sie diese zu CC-SG hinzufügen, falls sie nicht bereits verwaltet werden.

So erkennen Sie Geräte:

1. Wählen Sie "Geräte > Geräte erkennen".
2. Geben Sie in die Felder "Von IP-Adresse" und "Bis IP-Adresse" den Bereich der IP-Adressen ein, in dem sich die Geräte vermutlich befinden. Die Adresse im Feld "Bis IP-Adresse" sollte größer sein als die im Feld Von IP-Adresse. Legen Sie eine Maske für den Bereich fest. Wenn Sie keine Maske festlegen, wird die Broadcastadresse 255.255.255.255 gesendet, die an alle lokalen Netzwerke überträgt. Damit Geräte in Subnetzen erkannt werden, muss eine Maske festgelegt werden.
3. Klicken Sie auf Broadcasterkennung, wenn Sie nach Geräten im selben Subnetz suchen, in dem sich CC-SG befindet. Deaktivieren Sie "Broadcasterkennung", wenn Geräte in verschiedenen Subnetzen erkannt werden sollen.
4. Wenn Sie nach einem bestimmten Gerätetyp suchen, können Sie ihn in der Liste Gerätetypen markieren. Standardmäßig sind alle Gerätetypen markiert. Klicken Sie bei gedrückter Strg-Taste auf einen oder mehrere Gerätetypen, um diese auszuwählen.

5. Markieren Sie das Kontrollkästchen "IPMI-Agenten einschließen", wenn Sie Ziele suchen möchten, die eine IPMI-Stromversorgungssteuerung bieten.
6. Klicken Sie auf Erkennen, um die Suche zu starten. Sie können jederzeit während der Suche auf Stopp klicken, um den Suchvorgang abzubrechen. Die erkannten Geräte werden in einer Liste angezeigt.
7. Um mindestens ein erkanntes Gerät zu CC-SG hinzuzufügen, wählen Sie das gewünschte Gerät aus der Liste aus, und klicken Sie auf "Hinzufügen". Der Bildschirm "Gerät hinzufügen" wird angezeigt, in dem bereits einige Daten eingefügt sind.

   Wenn Sie mehrere Geräte zum Hinzufügen ausgewählt haben, können Sie unten im Bildschirm auf "Zurück" und "Überspringen" klicken, um die Geräte zu suchen, die Sie hinzufügen möchten.
8. Die Seite "Gerät hinzufügen" ist je nach Gerätetyp verschieden. Hinweise zum Hinzufügen der einzelnen erkannten CC-SG-Gerätetypen finden Sie in den entsprechenden Anweisungen.
   - Informationen zu KVM- oder seriellen Geräten finden Sie unter ***KVM- oder serielle Geräte hinzufügen*** (auf Seite 64).
   - Informationen zu PowerStrips finden Sie unter ***PowerStrip-Geräte hinzufügen*** (auf Seite 66).
   - Informationen zu Dominion PX-PowerStrips im IP-Netzwerk finden Sie unter ***Dominion PX-Geräte hinzufügen*** (auf Seite 66).
9. Klicken Sie auf "Übernehmen", um ein erkanntes Gerät hinzuzufügen und mit dem nächsten erkannten Gerät fortzufahren. Klicken Sie auf OK, um das aktuelle erkannte Gerät, aber keine weiteren erkannten Geräte hinzuzufügen.

Geräte hinzufügen

Sie müssen CC-SG Geräte hinzufügen, bevor Sie Ports konfigurieren oder Schnittstellen, die Zugriff auf die mit den Ports verbundenen Knoten bieten, hinzufügen können. Der Bildschirm "Gerät hinzufügen" wird verwendet, um ein Gerät hinzuzufügen, dessen Eigenschaften Sie kennen und für CC-SG bereitstellen können. Verwenden Sie für die Suche nach hinzuzufügenden Geräten die Option "Geräte erkennen". Siehe ***Geräte erkennen*** (auf Seite 62).

Informationen darüber, wie Sie an andere Geräte angeschlossene Raritan-PowerStrip-Geräte zu CC-SG hinzufügen, finden Sie unter ***Verwaltete PowerStrips*** (auf Seite 111).

So fügen Sie CC-SG ein Gerät hinzu:

1. Wählen Sie "Geräte > Gerätemanager > Gerät hinzufügen".

2. Klicken Sie auf die Dropdown-Liste "Gerätetyp", und wählen Sie einen Gerätetyp zum Hinzufügen in der Liste aus. Abhängig vom ausgewählten Gerätetyp, sieht die Seite "Gerät hinzufügen" etwas anders aus.

- Anweisungen zum Hinzufügen von KVM- oder seriellen Geräten finden Sie unter ***KVM- oder serielle Geräte hinzufügen*** (auf Seite 64).
- Anweisungen zum Hinzufügen von PowerStrip-Geräten finden Sie unter ***PowerStrip-Geräte hinzufügen*** (auf Seite 66).
- Anweisungen zum Hinzufügen von Dominion PX-Geräten finden Sie unter ***Dominion PX-Geräte hinzufügen*** (auf Seite 66).

KVM- oder serielle Geräte hinzufügen

KVM- und serielle Geräte können die 256-Bit-AES-Verschlüsselung unterstützten, die auch von CC-SG ab Version 4.1 unterstützt wird. Wenn für das Gerät der Standardverschlüsselungsmodus "auto-negotiate" (automatisch vereinbaren) eingestellt ist, vereinbart das Gerät mit CC-SG die Auswahl einer entsprechenden Verschlüsselungsstufe, die mit CC-SG funktioniert.

1. Geben Sie den Namen des neuen Geräts im Feld Gerätename ein. Weitere Informationen zu den Regeln, die von CC-SG für die Länge von Namen verwendet werden, finden Sie unter ***Benennungskonventionen*** (siehe "***Benennungsregeln***" auf Seite 457).
2. Geben Sie die IP-Adresse oder den Hostnamen des Geräts im Feld "Geräte-IP" oder "Hostname" ein. Die Regeln zur Vergabe von Hostnamen werden unter ***Terminologie/Abkürzungen*** (auf Seite 2) beschrieben.
3. Geben Sie in das Feld "Discovery Port" (Erkennungsport) die Nummer des TCP-Kommunikationsports ein, der zur Kommunikation mit dem Gerät verwendet wird. Sie können maximal fünf numerische Zeichen zwischen 1 und 65535 eingeben. Die Standardportnummer für die meisten Raritan-Geräte lautet 5000.
4. Geben Sie den für die Anmeldung verwendeten Benutzernamen im Feld "Benutzername" ein. Der Benutzer muss für den Zugriff Administratorberechtigungen besitzen.
5. Geben Sie das für den Zugriff auf dieses Gerät erforderliche Kennwort im Feld "Kennwort" ein. Der Benutzer muss für den Zugriff Administratorberechtigungen besitzen.
6. Geben Sie im Feld "Heartbeat-Timeout (Sek.)" die Zeit (in Sekunden) ein, die verstreichen soll, bevor zwischen dem neuen Gerät und CC-SG ein Zeitüberschreitungsfehler auftritt.

7. Wenn Sie ein Dominion SX- oder Dominion KX2-Gerät der Version 2.2 oder höher hinzufügen, können Sie durch Aktivierung des Kontrollkästchens "Allow Direct Device Access" (Direkten Gerätezugriff zulassen) über das Gerät direkt auf Zielgeräte zugreifen, auch wenn dieses von CC-SG verwaltet wird.
8. Geben Sie eine kurze Beschreibung für das Gerät in das Feld "Beschreibung" ein. **Optional.**
9. Markieren Sie das Kontrollkästchen "Alle Ports konfigurieren", wenn alle Ports dieses Geräts automatisch der Registerkarte "Geräte" hinzugefügt werden sollen und ein Knoten für jeden Port dieses Geräts auf der Registerkarte "Knoten" erstellt werden soll.
   - Entsprechende Knoten und Ports werden mit übereinstimmenden Namen konfiguriert.
   - Es wird ein neuer Knoten für jeden Port und eine Out-of-Band-Schnittstelle für diesen Knoten erstellt, mit Ausnahme eines Blade-Chassis-Knotens oder eines generischen analogen KVM-Switch-Knotens.
   - Für ein an einen KX2-Port angeschlossenes Blade-Chassis-Gerät oder einen generischen analogen KVM-Switch kann ein Knoten erstellt werden oder nicht. Dies hängt davon ab, ob eine IP-Adresse oder ein Hostname für das Blade-Chassis oder den generischen analogen KVM-Switch in KX2 eingegeben wurde. Weitere Informationen finden Sie im Benutzerhandbuch zu KX II. In CC-SG wird standardmäßig eine Browserschnittstelle zu einem Blade-Chassis-Knoten zugewiesen.
   - Auf der Registerkarte "Geräte" für direkt an KX2-Ports angeschlossene Blade-Server wird ein virtuelles Blade-Chassis-Gerät erstellt, wenn Blade-Port-Gruppen für diese Blade-Server ordnungsgemäß in KX2 konfiguriert wurden. Weitere Informationen finden Sie im Benutzerhandbuch zu KX II.
10. Sie können eine Liste der Kategorien und Elemente konfigurieren, um dieses Gerät und die damit verbundenen Knoten besser beschreiben und verwalten zu können. Siehe ***Zuordnungen, Kategorien und Elemente*** (auf Seite 49).
11. Klicken Sie für jede aufgeführte Kategorie auf das Dropdown-Menü "Element". Wählen Sie dann das Element zum Anwenden auf das Gerät in der Liste aus. Wählen Sie das leere Element im Feld Element für jede Kategorie aus, die Sie nicht verwenden möchten.

    Wenn Sie das Element verknüpften Knoten und Geräten zuweisen möchten, markieren Sie das Kontrollkästchen "Auf Knoten anwenden".
12. Wenn die Werte für Kategorie oder Element, die Sie verwenden möchten, nicht angezeigt werden, können Sie über das Menü "Zuordnungen" weitere hinzufügen. Siehe ***Zuordnungen, Kategorien und Elemente*** (auf Seite 49).

13. Wenn Sie mit der Konfiguration des Geräts fertig sind, klicken Sie auf "Übernehmen", um dieses Gerät hinzuzufügen und einen neuen, leeren Bildschirm "Gerät hinzufügen" anzuzeigen, in dem Sie weitere Geräte hinzufügen können. Sie können auch auf OK klicken, um dieses Gerät hinzuzufügen, ohne einen neuen Bildschirm "Gerät hinzufügen" zu öffnen.
14. Wenn die Firmwareversion des Geräts mit CC-SG nicht kompatibel ist, wird eine Meldung angezeigt. Klicken Sie auf "Ja", um das Gerät zu CC-SG hinzuzufügen. Sie können die Firmware des Geräts aktualisieren, nachdem Sie es zu CC-SG hinzugefügt haben. Siehe ***Gerät aktualisieren* (auf Seite 99).**

PowerStrip-Geräte hinzufügen

Das Hinzufügen eines PowerStrip-Geräts zu CC-SG hängt davon ab, mit welchem Raritan-Gerät der PowerStrip physisch verbunden ist. Siehe ***Verwaltete PowerStrips*** (auf Seite 111).

Informationen zum Hinzufügen eines Dominion PX-Geräts, das nicht an ein anderes Raritan-Gerät angeschlossen ist, finden Sie unter ***Dominion PX-Geräte hinzufügen*** (auf Seite 66).

Dominion PX-Geräte hinzufügen

Dominion PX-Geräte sind PowerStrips, die nur an Ihr IP-Netzwerk angeschlossen sind. Dominion PX-Geräte werden nicht von anderen Raritan-Geräten verwaltet. Beim Hinzufügen eines PowerStrip-Geräts, das von einem anderen Raritan-Gerät verwaltet wird, muss auf andere Weise vorgegangen werden. Siehe ***Verwaltete PowerStrips*** (auf Seite 111).

1. Geben Sie den Namen des Geräts im Feld "Gerätename" ein. Weitere Informationen zu den Regeln, die von CC-SG für die Länge von Namen verwendet werden, finden Sie unter ***Benennungskonventionen*** (siehe "***Benennungsregeln***" auf Seite 457).
2. Geben Sie die IP-Adresse oder den Hostnamen des Geräts im Feld "IP-Adresse/Hostname" ein. Die Regeln zur Vergabe von Hostnamen werden unter ***Terminologie/Abkürzungen*** (auf Seite 2) beschrieben.
3. Geben Sie den für die Anmeldung verwendeten Benutzernamen im Feld "Benutzername" ein. Der Benutzer muss für den Zugriff Administratorberechtigungen besitzen.
4. Geben Sie das für den Zugriff auf dieses Gerät erforderliche Kennwort im Feld "Kennwort" ein. Der Benutzer muss für den Zugriff Administratorberechtigungen besitzen.

Warnhinweis: CC-SG verliert die Verbindung zum Dominion PX-Gerät, wenn der Benutzername oder das Kennwort geändert wird. Wenn Sie das Kennwort auf dem PX ändern, müssen Sie das Kennwort für das PX-Gerät in CC-SG ändern. Siehe **Geräte bearbeiten** *(auf Seite 67).*

5. Geben Sie eine kurze Beschreibung für das Gerät in das Feld "Beschreibung" ein. **Optional.**
6. Markieren Sie das Kontrollkästchen "Alle Ausgänge konfigurieren", um alle Ausgänge dieses Dominion PX automatisch zur Registerkarte "Geräte" hinzuzufügen.
7. Sie können eine Liste mit Kategorien und Elementen konfigurieren, um dieses Gerät besser beschreiben und verwalten zu können.
   - Wählen Sie für jede aufgelistete Kategorie das Element aus der Liste aus, das auf das Gerät angewendet werden soll. Wählen Sie das leere Element im Feld Element für jede Kategorie aus, die Sie nicht verwenden möchten.
   - Wenn die Werte für "Kategorie" oder "Element", die Sie verwenden möchten, nicht angezeigt werden, können Sie weitere hinzufügen. Siehe ***Zuordnungen, Kategorien und Elemente*** (auf Seite 49).
8. Wenn Sie mit der Konfiguration des Geräts fertig sind, klicken Sie auf "Übernehmen", um dieses Gerät hinzuzufügen und einen neuen, leeren Bildschirm "Gerät hinzufügen" anzuzeigen, in dem Sie weitere Geräte hinzufügen können. Sie können auch auf OK klicken, um dieses Gerät hinzuzufügen, ohne einen neuen Bildschirm "Gerät hinzufügen" zu öffnen.

Geräte bearbeiten

Sie können ein Gerät bearbeiten, um es umzubenennen und seine Eigenschaften zu ändern, einschließlich den Benutzernamen und das Kennwort eines PX-Geräts ändern.

So bearbeiten Sie ein Gerät:

1. Klicken Sie auf die Registerkarte "Geräte", und wählen Sie das Gerät zum Bearbeiten aus.
2. Ändern Sie auf der Seite "Geräteprofil" die Parameter nach Bedarf. Ändern Sie die Parameter nach Bedarf.
3. Klicken Sie zum Speichern der Änderungen auf OK.

Ändern der HTTP- und HTTPS-Ports für ein KX2-Gerät

Ändern Sie die HTTP- und HTTPS-Ports für ein KX2-Gerät, Version 2.3 oder höher, durch Bearbeiten des Geräteprofils. CC-SG propagiert die neuen Portnummern an das KX2-Gerät.

Die neuen Ports werden für die Kommunikation zwischen CC-SG und den KX2-Geräten oder für die Kommunikation durch Client-Anwendungen, wie z. B. AKC und VKC, direkt mit den KX2-Geräten verwendet. Die neuen Portnummern werden nicht für die Kommunikation zwischen dem Client-Computer des Benutzers und CC-SG verwendet.

So ändern Sie die HTTP- und HTTPS-Ports für ein KX2-Gerät:

Hinweis: Nur für KX2 Version 2.3 und höher.

1. Klicken Sie auf die Registerkarte "Geräte", und wählen Sie das Gerät zum Bearbeiten aus.
2. Ändern Sie auf der Seite "Geräteprofil" die Parameter nach Bedarf. Geben Sie neue Werte für den HTTP- und HTTPS-Port ein.
3. Klicken Sie auf OK.

PowerStrip- oder Dominion PX-Geräte bearbeiten

Sie können ein verwaltetes PowerStrip-Gerät oder ein Dominion PX-Gerät bearbeiten, um es umzubenennen, die Eigenschaften zu ändern und den Status der Ausgangskonfiguration anzuzeigen.

So bearbeiten Sie ein Powerstrip-Gerät:

1. Klicken Sie auf die Registerkarte "Geräte", und wählen Sie das Powerstrip-Gerät zum Bearbeiten aus.
2. Geben Sie die neuen Geräteeigenschaften in die entsprechenden Felder ein. Bearbeiten Sie bei Bedarf die Kategorien und Elemente, die dem Gerät zugewiesen sind.
3. Klicken Sie auf die Registerkarte "Ausgang", um alle Ausgänge des PowerStrip anzuzeigen.
4. Ist ein Ausgang mit einem Knoten verknüpft, klicken Sie auf den Hyperlink "Knoten", um das Knotenprofil anzuzeigen.
5. Ist ein Ausgang mit einem Knoten verknüpft, wählen Sie den Ausgang aus, und klicken Sie dann auf "Stromversorgungssteuerung", um die Stromversorgungssteuerung für den verknüpften Knoten anzuzeigen.
6. Um einen Ausgang zu löschen, deaktivieren Sie das Kontrollkästchen neben dem Namen des Ausgangs.

7. Zum Konfigurieren eines Ausgangs aktivieren Sie das Kontrollkästchen neben dem Namen des Ausgangs.
8. Klicken Sie zum Speichern der Änderungen auf OK. Eine Meldung wird eingeblendet, wenn das Gerät geändert wurde.

Hinweise zu einem Geräteprofil hinzufügen

Sie können auf der Registerkarte "Hinweise" Hinweise zu einem Gerät für andere Benutzer hinzufügen. Alle Hinweise werden mit dem Datum, dem Benutzernamen und der IP-Adresse des Benutzers angezeigt, der den Hinweis hinzugefügt hat.

Wenn Sie über die Berechtigung "Geräte-, Port- und Knotenverwaltung" verfügen, können Sie alle auf der Registerkarte "Hinweise" angezeigten Hinweise löschen.

So fügen Sie Hinweise zum Geräteprofil hinzu:

1. Wählen Sie ein Gerät auf der Registerkarte "Geräte". Die Seite "Geräteprofil" wird angezeigt.
2. Klicken Sie auf die Registerkarte "Hinweise".
3. Geben Sie den Hinweis im Feld "Neuer Hinweis" ein.
4. Klicken Sie auf "Hinzufügen". Ihr Hinweis wird in der Liste "Hinweise" angezeigt.

So löschen Sie alle Knoten:

1. Klicken Sie auf die Registerkarte "Hinweise".
2. Klicken Sie auf "Hinweise löschen".
3. Klicken Sie zum Bestätigen auf "Ja". Alle Hinweise werden aus der Registerkarte "Hinweise" gelöscht.

Einsatzort und Kontakte zu einem Geräteprofil hinzufügen

Geben Sie Details zum Einsatzort des Geräts sowie Kontaktinformationen für die Personen ein, die das Gerät verwalten oder verwenden.

So fügen Sie einen Einsatzort und Kontakte zu einem Geräteprofil hinzu:

1. Wählen Sie ein Gerät auf der Registerkarte "Geräte". Die Seite "Geräteprofil" wird angezeigt.
2. Klicken Sie auf die Registerkarte "Einsatzort & Kontakte".
3. Geben Sie Informationen zum Einsatzort ein.

- Abteilung: Maximal 64 Zeichen.
- Standort: Maximal 64 Zeichen.
- Speicherort: Maximal 128 Zeichen.

4. Geben Sie Kontaktinformationen ein.
   - "Erster Ansprechpartner" und "Zweiter Ansprechpartner": Maximal 64 Zeichen.
   - "Telefonnummer" und "Mobilfunknummer": Maximal 32 Zeichen.
5. Klicken Sie zum Speichern der Änderungen auf OK.

Geräte löschen

Sie können Geräte löschen, damit sie nicht mehr von CC-SG verwaltet werden.

Wichtig: Wenn Sie ein Gerät löschen, werden alle Ports entfernt, die für das Gerät konfiguriert sind. Alle Schnittstellen, die diesen Ports zugewiesen sind, werden von den Knoten entfernt. Besteht keine weitere Schnittstelle für diese Knoten, werden die Knoten auch aus CC-SG entfernt.

So löschen Sie ein Gerät:

1. Klicken Sie auf die Registerkarte "Geräte", und wählen Sie das Gerät zum Löschen aus.
2. Wählen Sie "Geräte > Gerätemanager > Gerät löschen".
3. Klicken Sie zum Löschen des Geräts auf OK. Eine Meldung wird eingeblendet, wenn das Gerät gelöscht wurde.

Ports konfigurieren

Wenn Sie beim Hinzufügen des Geräts **das Kontrollkästchen "Alle Ports konfigurieren" nicht markiert haben und die Ports des Geräts aus diesem Grund nicht automatisch hinzugefügt werden, können Sie einzelne oder mehrere Ports des Geräts über den Bildschirm "Ports konfigurieren" zu CC-SG hinzufügen.**

Nachdem Sie Ports konfiguriert haben, wird in CC-SG für jeden Port ein Knoten erstellt. Außerdem wird die Standardschnittstelle erstellt. Siehe ***Durch das Konfigurieren von Ports erstellte Knoten*** (auf Seite 72).

Seriellen Port konfigurieren

So konfigurieren Sie einen seriellen Port:

1. Klicken Sie auf die Registerkarte "Geräte", und wählen Sie ein serielles Gerät.
2. Wählen Sie "Geräte > Portmanager > Ports konfigurieren".

   Klicken Sie auf eine Spaltenüberschrift, um die Ports in aufsteigender Reihenfolge nach diesem Attribut zu sortieren. Klicken Sie erneut auf die Spaltenüberschrift, um die Ports in absteigender Reihenfolge zu sortieren.
3. Klicken Sie neben dem zu konfigurierenden seriellen Port auf die entsprechende Schaltfläche Konfigurieren.
4. Geben Sie in das Feld "Portname" einen Namen ein. Der Einfachheit halber sollten Sie den Port nach dem mit dem Port verbundenen Ziel benennen. Weitere Informationen zu den Regeln, die von CC-SG für die Länge von Namen verwendet werden, finden Sie unter ***Benennungskonventionen*** (siehe "***Benennungsregeln***" auf Seite 457).
5. Geben Sie einen Knotennamen in das Feld "Knotenname" ein, um einen neuen Knoten mit einer Out-of-Band-Schnittstelle über diesen Port zu erstellen. Der Einfachheit halber sollten Sie den Knoten nach dem mit dem Port verbundenen Ziel benennen. Sie geben also denselben Namen in die Felder Portname und Knotenname ein.
6. Klicken Sie auf das Dropdown-Menü "Zugriffsanwendung", und wählen Sie die Anwendung aus, die Sie beim Verbinden mit dem Port über die Liste verwenden möchten. CC-SG wählt die entsprechende Anwendung basierend auf Ihrem Browser automatisch aus, wenn Sie Automatisch erkennen markieren.
7. Klicken Sie zum Hinzufügen des Ports auf OK.

KVM-Port konfigurieren

So konfigurieren Sie einen KVM-Port:

1. Klicken Sie auf die Registerkarte "Geräte", und wählen Sie ein KVM-Gerät.
2. Wählen Sie "Geräte > Portmanager > Ports konfigurieren".
   - Klicken Sie auf eine Spaltenüberschrift, um die Ports in aufsteigender Reihenfolge nach diesem Attribut zu sortieren. Klicken Sie erneut auf die Spaltenüberschrift, um die Ports in absteigender Reihenfolge zu sortieren.
3. Klicken Sie neben dem zu konfigurierenden KVM-Port auf die entsprechende Schaltfläche "Konfigurieren".

4. Geben Sie in das Feld "Portname" einen Portnamen ein. Der Einfachheit halber sollten Sie den Port nach dem mit dem Port verbundenen Ziel benennen. Weitere Informationen zu den Regeln, die von CC-SG für die Länge von Namen verwendet werden, finden Sie unter ***Benennungskonventionen*** (siehe "***Benennungsregeln***" auf Seite 457).
5. Geben Sie einen Knotennamen in das Feld "Knotenname" ein, um einen neuen Knoten mit einer Out-of-Band-Schnittstelle über diesen Port zu erstellen. Der Einfachheit halber sollten Sie den Knoten nach dem mit dem Port verbundenen Ziel benennen. Sie geben also denselben Namen in die Felder Portname und Knotenname ein.
6. Klicken Sie auf das Dropdown-Menü "Zugriffsanwendung", und wählen Sie die Anwendung aus, die Sie beim Verbinden mit dem Port über die Liste verwenden möchten. CC-SG wählt die entsprechende Anwendung basierend auf Ihrem Browser automatisch aus, wenn Sie Automatisch erkennen markieren.
7. Klicken Sie zum Hinzufügen des Ports auf OK.

Durch das Konfigurieren von Ports erstellte Knoten

Beim Konfigurieren der Ports eines Geräts wird automatisch ein Knoten für jeden Port erstellt. Für jeden Knoten wird auch eine Schnittstelle erstellt.

Wird ein Knoten automatisch erstellt, wird ihm der gleiche Name wie dem Port gegeben, dem er zugewiesen ist. Wenn dieser Knotenname bereits vorhanden ist, wird dem Knotennamen eine Erweiterung hinzugefügt. Ein Beispiel ist Kanal1(1). Die Erweiterung ist die Zahl in Klammern. Diese Erweiterung ist bei der Zeichenanzahl des Knotennamens nicht eingeschlossen. Wenn Sie den Knotennamen bearbeiten, ist der neue Name auf die maximale Anzahl an Zeichen beschränkt. Siehe ***Benennungskonventionen*** (siehe "***Benennungsregeln***" auf Seite 457).

Ports bearbeiten

Sie können Ports bearbeiten, um verschiedene Parameter zu ändern, z. B. den Portnamen, die Zugriffsanwendung sowie die Einstellungen für serielle Ports. Die Änderungen, die Sie vornehmen können, variieren je nach Port- und Gerätetyp.

Hinweis: Sie können die Dominion KX2-Porteinstellungen auch über "Administration starten" und die Webschnittstelle von KX2 bearbeiten.

So bearbeiten Sie den Namen eines KVM- oder seriellen Ports oder eine Zugriffsanwendung:

Manche Ports unterstützen nur eine Zugriffsanwendung, sodass Sie die Einstellung für die Zugriffsanwendung nicht ändern können.

1. Klicken Sie auf die Registerkarte "Geräte", und wählen Sie den Port zum Bearbeiten aus.
2. Geben Sie bei Bedarf einen neuen Portnamen in das Feld Portname ein.
3. Klicken Sie auf das Dropdown-Menü "Zugriffsanwendung", und wählen Sie die Anwendung aus, die Sie beim Verbinden mit dem Port über die Liste verwenden möchten. CC-SG wählt die entsprechende Anwendung basierend auf Ihrem Browser automatisch aus, wenn Sie Automatisch erkennen markieren.
4. Klicken Sie zum Speichern der Änderungen auf OK.

So bearbeiten Sie die Einstellungen (z. B. Baudrate, Flusssteuerung oder Parität/Datenbit) eines seriellen KSX2- oder KSX-Ports:

1. Klicken Sie auf die Registerkarte "Geräte", und wählen Sie den zu bearbeitenden seriellen Port, oder wählen Sie einfach das Gerät, das den zu bearbeitenden Port enthält.
2. Wählen Sie "Geräte > Gerätemanager > Administration starten". Die Verwaltungsseite des Geräts wird angezeigt.
3. Klicken Sie auf "Portkonfiguration".
4. Klicken Sie auf den seriellen Port, den Sie bearbeiten möchten.
5. Bearbeiten Sie die Porteinstellungen.
6. Klicken Sie zum Speichern der Änderungen auf OK. Schließen Sie die Verwaltungsseite, und kehren Sie zu CC-SG zurück.

So bearbeiten Sie die Einstellungen (z. B. Baudrate, Flusssteuerung oder Parität/Datenbit) eines seriellen SX-Ports:

1. Klicken Sie auf die Registerkarte "Geräte", und wählen Sie den Port zum Bearbeiten aus. Die Seite "Portprofil" wird angezeigt.
2. Bearbeiten Sie die Porteinstellungen.
3. Klicken Sie zum Speichern der Änderungen auf OK.

Ports löschen

Löschen Sie Ports, um den Porteintrag aus einem Gerät zu löschen. Wenn ein Port nicht verfügbar ist, werden die Informationen im Fenster "Portprofil" mit Lesezugriff angezeigt. Sie können nicht verfügbare Ports löschen.

Wichtig: Wenn Sie einen Port löschen, der einem Knoten zugewiesen ist, wird die verknüpfte Out-of-Band-KVM- oder serielle Schnittstelle, die vom Port bereitgestellt wird, aus dem Knoten entfernt. Verfügt der Knoten über keine weiteren Schnittstellen, wird der Knoten auch aus CC-SG entfernt.

So löschen Sie einen Port:

1. Klicken Sie auf die Registerkarte "Geräte", und wählen Sie das Gerät aus, dessen Ports Sie löschen möchten.
2. Wählen Sie "Geräte > Portmanager > Ports löschen".
3. Markieren Sie das Kontrollkästchen des zu löschenden Ports.
4. Klicken Sie zum Löschen eines Ports auf OK. Eine Meldung wird eingeblendet, wenn der Port gelöscht wurde.

An KX2 angeschlossenes Blade-Chassis-Gerät konfigurieren

Übersicht über das Blade-Chassis

Es gibt zwei Blade-Chassis-Gerätetypen: ein Gerätetyp enthält einen integrierten KVM-Switch, der als IP-fähiger KVM-Switch verwendet werden kann, der andere Gerätetyp enthält diesen Switch nicht.

Blade-Chassis mit integriertem KVM-Switch

Ein Blade-Chassis mit einem integrierten KVM-Switch, wie z. B. Dell PowerEdge und IBM BladeCenter, wird über ein CIM an KX2 angeschlossen. Da für den Zugriff auf alle Blade-Server in diesem Chassis nur ein CIM zur Verfügung steht, wenn ein Benutzer auf einen Blade-Server zugreift, sind keine weiteren Pfade für andere Benutzer vorhanden.

Nachdem alle KX2-Ports in CC-SG konfiguriert wurden, wird das *Blade-Chassis* konfiguriert, das an das KX2-Gerät angeschlossen ist. Siehe ***Blade-Chassis-Gerät hinzufügen*** (auf Seite 75). Die Blade-Server in diesem Blade-Chassis-Typ sind noch nicht konfiguriert, d. h. Sie müssen die Blade-Server zu einem späteren Zeitpunkt konfigurieren. Siehe ***Slots auf einem Blade-Chassis-Gerät konfigurieren*** (auf Seite 77).

Blade-Chassis ohne integrierten KVM-Switch

Ein Blade-Chassis ohne einen integrierten KVM-Switch, wie z. B. HP BladeSystem, ermöglicht mithilfe eines CIM das Anschließen jedes Blade-Servers an ein KX2. Da jeder Blade-Server in diesem Chassis über ein CIM für den Zugriff verfügt, können Benutzer weiterhin auf die restlichen Blade-Server zugreifen, während ein Benutzer auf einen Blade-Server zugreift.

Nachdem alle KX2-Ports in CC-SG konfiguriert wurden, werden die *Blade-Server* konfiguriert, die an das KX2-Gerät angeschlossen sind. Wenn Sie eine Blade-Port-Gruppe für diese Blade-Server ordnungsgemäß auf dem KX2-Gerät konfiguriert haben, erstellt CC-SC ein *virtuelles* Blade-Chassis auf KX2-Port-Ebene als Container für diese Blade-Server. Siehe ***Blade-Chassis-Gerät hinzufügen*** (auf Seite 75). Andernfalls werden diese Blade-Server als normale KX2-Ports auf der Registerkarte "Geräte" des CC-SG angezeigt.

Blade-Chassis-Gerät hinzufügen

Die Schritte für das Hinzufügen eines Blade-Chassis hängen vom Blade-Chassis-Typ ab.

Bei Blade-Chassis-Geräten werden immer zwei Namen auf der Registerkarte "Geräte" angezeigt: Der Name, der nicht in Klammern steht, wird vom KX2-Gerät abgerufen, der Name in Klammern ist der in CC-SG gespeicherte Chassis-Name.

▶ So fügen Sie ein Blade-Chassis-Gerät *mit* einem integrierten KVM-Switch hinzu:

1. Konfigurieren Sie das Blade-Chassis ordnungsgemäß in KX2. Weitere Informationen finden Sie im Benutzerhandbuch zu KX II.

2. Konfigurieren Sie das KX2-Gerät ordnungsgemäß in CC-SG. Siehe ***KVM- oder serielle Geräte hinzufügen*** (auf Seite 64).
3. CC-SG erkennt das Blade-Chassis-Gerät und fügt das Blade-Chassis-Symbol auf einer oder zwei Registerkarten hinzu:
   - Auf der Registerkarte "Geräte" wird das Blade-Chassis-Gerät unterhalb des KX2-Geräts angezeigt, an das es angeschlossen ist.
   - Auf der Registerkarte "Knoten" wird das Blade-Chassis als Knoten mit einer hinzugefügten Browserschnittstelle angezeigt, wenn Sie die IP-Adresse oder den Hostnamen für das Blade-Chassis auf dem KX2-Gerät eingegeben haben.

Hinweis: Für diesen Blade-Chassis-Typ müssen Sie die Blade-Server zu einem späteren Zeitpunkt konfigurieren. Siehe **Slots auf einem Blade-Chassis-Gerät konfigurieren** *(auf Seite 77).*

So fügen Sie ein Blade-Chassis-Gerät *ohne* einen integrierten KVM-Switch hinzu:

1. Konfigurieren Sie eine Blade-Port-Gruppe für die Blade-Server ordnungsgemäß in KX2. Weitere Informationen finden Sie im Benutzerhandbuch zu KX II.
2. Konfigurieren Sie das KX2-Gerät ordnungsgemäß in CC-SG. Siehe ***KVM- oder serielle Geräte hinzufügen*** (auf Seite 64).
3. CC-SG erstellt automatisch ein *virtuelles* Blade-Chassis und fügt das Blade-Chassis-Symbol auf einer Registerkarte ein. Beachten Sie, dass ein virtuelles Blade-Chassis nie als Knoten auf der Registerkarte "Knoten" angezeigt wird.
   - Auf der Registerkarte "Geräte" wird das virtuelle Blade-Chassis-Gerät unter dem KX2-Gerät als virtueller Container für Blade-Server angezeigt, die unter dem virtuellen Blade-Chassis angezeigt werden.

Hinweis: Wenn Sie vor der Konfiguration der KX2-Ports in CC-SG keine Blade-Port-Gruppe für die Blade-Server konfiguriert haben, wählen Sie "Geräte > Gerätemanager > Administration starten", um die Blade-Port-Gruppe festzulegen. Konfigurieren Sie anschließend die Blade-Server in CC-SG. Siehe **Slots auf einem Blade-Chassis-Gerät konfigurieren** *(auf Seite 77).*

Slots auf einem Blade-Chassis-Gerät konfigurieren

Wenn die Blade-Server oder Slots noch nicht in CC-SG konfiguriert wurden, müssen Sie sie gemäß den Anweisungen in diesem Abschnitt konfigurieren. Andernfalls werden die Blade-Server nicht auf den Registerkarten "Geräte" und "Knoten" angezeigt. Eine Out-of-Band-KVM-Schnittstelle wird automatisch zu einem Blade-Server-Knoten hinzugefügt.

So konfigurieren Sie die Slots im Blade-Chassis-Profil:

1. Klicken Sie auf der Registerkarte "Geräte" auf das Pluszeichen (+) neben dem KX2-Gerät, das an das Blade-Chassis-Gerät angeschlossen ist.
2. Wählen Sie das Blade-Chassis-Gerät aus, dessen Slots Sie konfigurieren möchten.
3. Wählen Sie im Bildschirm "Geräteprofil" die Registerkarte "Blades".
4. Markieren Sie das Kontrollkästchen für jeden Slot, den Sie konfigurieren möchten, und klicken Sie dann auf OK.

So konfigurieren Sie Slots im Bildschirm "Ports konfigurieren":

1. Klicken Sie auf der Registerkarte "Geräte" auf das Pluszeichen (+) neben dem KX2-Gerät, das an das Blade-Chassis-Gerät angeschlossen ist.
2. Wählen Sie das Blade-Chassis-Gerät aus, dessen Slots Sie konfigurieren möchten.
3. Wählen Sie "Geräte > Portmanager > Ports konfigurieren".
   - Wenn Sie mehrere Slots mit den im Bildschirm angezeigten Standardnamen konfigurieren möchten, markieren Sie das Kontrollkästchen für jeden Slot, den Sie konfigurieren möchten. Klicken Sie dann auf OK, um jeden Slot mit dem Standardnamen zu konfigurieren.
   - Um jeden Slot einzeln zu konfigurieren, klicken Sie neben dem entsprechenden Slot auf die Schaltfläche "Konfigurieren". Geben Sie anschließend einen Namen für den Slot im Feld "Portname" und einen Knotennamen im Feld "Knotenname" ein. Die standardmäßige Zugriffsanwendung wird gemäß der Standardanwendung festgelegt, die Sie für "Blade-Chassis: KVM" im Anwendungsmanager ausgewählt haben. Um die Standardanwendung zu ändern, klicken Sie auf das Dropdown-Menü "Zugriffsanwendung" und wählen die gewünschte Anwendung aus der Liste aus. Klicken Sie zum Konfigurieren des Slots auf OK.

So konfigurieren Sie Slots mithilfe des Befehls "Blades konfigurieren":

1. Klicken Sie auf der Registerkarte "Geräte" auf das Pluszeichen (+) neben dem KX2-Gerät, das an das Blade-Chassis-Gerät angeschlossen ist.
2. Wählen Sie das Blade-Chassis-Gerät aus, dessen Slots Sie konfigurieren möchten.
3. Wählen Sie "Knoten > Blades konfigurieren".
   - Wenn Sie mehrere Slots mit den im Bildschirm angezeigten Standardnamen konfigurieren möchten, markieren Sie das Kontrollkästchen für jeden Slot, den Sie konfigurieren möchten. Klicken Sie dann auf OK, um jeden Slot mit dem Standardnamen zu konfigurieren.
   - Um jeden Slot einzeln zu konfigurieren, klicken Sie neben dem entsprechenden Slot auf die Schaltfläche "Konfigurieren". Geben Sie anschließend einen Namen für den Slot im Feld "Portname" und einen Knotennamen im Feld "Knotenname" ein. Die standardmäßige Zugriffsanwendung wird gemäß der Standardanwendung festgelegt, die Sie für "Blade-Chassis: KVM" im Anwendungsmanager ausgewählt haben. Um die Standardanwendung zu ändern, klicken Sie auf das Dropdown-Menü "Zugriffsanwendung" und wählen die gewünschte Anwendung aus der Liste aus. Klicken Sie zum Konfigurieren des Slots auf OK.

Blade-Server-Status ändern

Dieser Abschnitt bezieht sich nur auf das Blade-Chassis mit integriertem KVM-Switch, wie z. B. Dell PowerEdge und IBM BladeCenter.

Wenn der Status "Installed" (Installiert) für den entsprechenden Blade-Server oder Slot nicht im KX2-Gerät aktiviert ist, zeigt CC-SG immer den Port-Status "Nicht verfügbar" für den Blade-Server an. Wenn Sie sich sicher sind, dass einige Blade-Slots mit installierten Blade-Servern aktiv sind, müssen Sie ihren Status im KX2-Gerät ändern, damit CC-SG den Status ordnungsgemäß reflektiert.

So ändern Sie den Blade-Server-Status:

1. Klicken Sie auf die Registerkarte "Geräte", und wählen Sie das KX2-Gerät aus, dessen Blade-Slot-Status Sie ändern möchten.
2. Wählen Sie "Geräte > Gerätemanager > Administration starten". Der KX2-Administrations-Client wird geöffnet.
3. Wählen Sie "Geräteeinstellungen > Portkonfiguration".

4. Klicken Sie auf den Blade-Chassis-Port, den Sie konfigurieren möchten.
5. Führen Sie einen Bildlauf durch, bis Sie den Bereich mit den Blade-Slots sehen. Markieren Sie das Kontrollkästchen "Installed" (Installiert) neben den Blade-Slots, die mit installierten Blade-Servern aktiv sind.
6. Klicken Sie zum Speichern der Änderungen auf OK.

Slots auf einem Blade-Chassis-Gerät löschen

Sie können nicht verwendete Blade-Server oder Slots löschen, sodass sie nicht auf den Registerkarten "Geräte" und "Knoten" angezeigt werden.

So löschen Sie einen Slot im Bildschirm "Ports löschen":

1. Klicken Sie auf der Registerkarte "Geräte" auf das Pluszeichen (+) neben dem KX2-Gerät, das an das Blade-Chassis-Gerät angeschlossen ist.
2. Wählen Sie das Blade-Chassis-Gerät aus, dessen Slots Sie löschen möchten.
3. Wählen Sie "Geräte > Portmanager > Ports löschen".
4. Markieren Sie das Kontrollkästchen für jeden Slot, den Sie löschen möchten, und klicken Sie dann auf OK, um den Slot zu löschen.

So löschen Sie einen Slot mithilfe des Befehls "Blade löschen":

1. Klicken Sie auf der Registerkarte "Geräte" auf das Pluszeichen (+) neben dem KX2-Gerät, das an das Blade-Chassis-Gerät angeschlossen ist.
2. Klicken Sie auf das Pluszeichen (+) neben dem Blade-Chassis-Gerät, dessen Slots Sie löschen möchten.
3. Klicken Sie mit der rechten Maustaste auf den zu löschenden Blade-Slot.
4. Wählen Sie "Blade löschen" aus, und klicken Sie anschließend auf OK, um den Slot zu löschen.

Blade-Chassis-Gerät bearbeiten

Sie können ein Blade-Chassis-Gerät bearbeiten, um es umzubenennen, die Eigenschaften zu ändern und den Status der Slotkonfiguration anzuzeigen.

So bearbeiten Sie ein Blade-Chassis:

1. Klicken Sie auf der Registerkarte "Geräte" auf das Pluszeichen (+) neben dem KX2-Gerät, das an das Blade-Chassis-Gerät angeschlossen ist.

2. Wählen Sie das zu bearbeitende Blade-Chassis-Gerät aus.
3. Geben Sie die neuen Geräteeigenschaften in die entsprechenden Felder ein. Bearbeiten Sie bei Bedarf die Kategorien und Elemente, die dem Gerät zugewiesen sind.
4. Klicken Sie auf die Registerkarte "Blades", um alle Slots dieses Blade-Chassis-Geräts anzuzeigen.
5. Wenn ein Slot als Knoten konfiguriert wurde, können Sie auf den Hyperlink "Knoten" klicken, um das Knotenprofil anzuzeigen. **Optional.**
6. Klicken Sie zum Speichern der Änderungen auf OK. Eine Meldung wird eingeblendet, wenn das Gerät geändert wurde.

Blade-Chassis-Gerät löschen

Sie können ein Blade-Chassis-Gerät in CC-SG löschen, das an ein KX2-Gerät angeschlossen ist. Wenn Sie das Blade-Chassis-Gerät aus dem KX2-Gerät löschen, wird das Blade-Chassis-Gerät sowie alle konfigurierten Blade-Server oder Slots nicht mehr auf den Registerkarten "Geräte" und "Knoten" angezeigt.

So löschen Sie ein Blade-Chassis-Gerät:

1. Klicken Sie auf die Registerkarte "Geräte", und wählen Sie das KX2-Gerät aus, dessen Blade-Chassis-Gerät Sie löschen möchten.
2. Wählen Sie "Geräte > Portmanager > Ports löschen".
3. Markieren Sie das Kontrollkästchen des zu löschenden Blade-Chassis-Ports.
4. Klicken Sie zum Löschen des ausgewählten Blade-Chassis-Ports auf OK. Sie werden in einer Meldung aufgefordert, das Löschen des Blade-Chassis-Geräts sowie der dazugehörigen Blade-Server zu bestätigen.

Blade-Chassis-Gerät auf einen anderen Port verschieben

Wenn Sie ein Blade-Chassis-Gerät von einem KX2-Gerät oder -Port auf ein anderes KX2-Gerät oder einen anderen Port verschieben möchten, kann CC-SG die Konfigurationsdaten des Blade-Chassis-Geräts auf dem neuen Port nicht automatisch erkennen und aktualisieren. Sie müssen das Blade-Chassis-Gerät erneut auf CC-SG konfigurieren.

So verschieben Sie ein Blade-Chassis-Gerät auf ein anderes KX2-Gerät oder auf einen anderen Port:

1. Löschen Sie das Blade-Chassis-Gerät aus CC-SG. Siehe ***Blade-Chassis-Gerät löschen*** (auf Seite 80).
2. Trennen Sie die Verbindung zum Blade-Chassis, und schließen Sie es wieder an ein anderes KX2-Gerät oder an einen anderen Port an.

3. Fügen Sie das Blade-Chassis-Gerät in CC-SG hinzu. Siehe ***Blade-Chassis-Gerät hinzufügen*** (auf Seite 75).

Blade-Server-Ports als normale KX2-Ports wiederherstellen

Dieser Abschnitt bezieht sich nur auf das Blade-Chassis ohne integrierten KVM-Switch, wie z. B. HP BladeSystem.

Auf der Registerkarte "Geräte" können Sie Blade-Server unter dem virtuellen Blade-Chassis erneut als normale KX2-Ports konfigurieren.

So stellen Sie Blade-Server als normale KX2-Ports wieder her:

1. Wählen Sie auf der Registerkarte "Geräte" das KX2-Gerät aus, dessen Blade-Server Sie erneut als normale KVM-Ports konfigurieren möchten.
2. Ändern Sie die Blade-Port-Gruppe für diese Blade-Server in eine Nicht-Blade-Port-Gruppe.
   a. Wählen Sie in CC-SG "Geräte > Gerätemanager > Administration starten". Der KX2-Administrations-Client wird geöffnet.
   b. Klicken Sie auf "Port Group Management" (Portgruppenverwaltung).
   c. Klicken Sie auf die Blade-Port-Gruppe, deren Gruppeneigenschaften Sie ändern möchten.
   d. Deaktivieren Sie das Kontrollkästchen "Blade Server Group" (Bladeservergruppe).
   e. Klicken Sie auf OK.
   f. Beenden Sie den KX2-Administrations-Client.
3. Das virtuelle Blade-Chassis wird nicht mehr auf der Registerkarte "Geräte" angezeigt. Nun können Sie die Blade-Server-Ports erneut als normale KX2-Ports in CC-SG konfigurieren. Siehe ***KVM-Port konfigurieren*** (auf Seite 71).

Massenkopieren für Gerätezuordnungen, Einsatzort und Kontakte

Mit dem Befehl "Massenkopieren" können Sie Kategorien, Elemente, Einsatzort und Kontaktinformationen von einem Gerät auf mehrere andere Geräte mittels Kopieren übertragen. Die ausgewählten Informationen sind die einzigen bei diesem Vorgang kopierten Eigenschaften. Wenn dieselben Informationstypen bereits auf einem ausgewählten Gerät vorhanden sind, werden mit dem Befehl "Massenkopieren" die vorhandenen Daten durch die neuen zugeordneten Informationen ÜBERSCHRIEBEN.

So führen Sie das Massenkopieren von Gerätezuordnungen, Einsatzort und Kontaktinformationen aus:

1. Klicken Sie auf die Registerkarte "Geräte", und wählen Sie in der Gerätestrukturansicht ein Gerät aus.
2. Wählen Sie "Geräte > Gerätemanager > Massenkopieren".
3. Wählen Sie in der Liste "Verfügbare Geräte" die Geräte aus, auf die Sie die Zuordnungen, Einsatzort und Kontaktinformationen des im Feld "Gerätename" angezeigten Geräts kopieren möchten.
4. Klicken Sie auf > (Pfeil nach rechts), um der Liste "Ausgewählte Geräte" ein Gerät hinzuzufügen.
5. Wählen Sie das gewünschte Gerät aus, und klicken Sie auf < (Pfeil nach links), um es aus der Liste "Ausgewählte Geräte" zu entfernen.
6. Markieren Sie auf der Registerkarte "Zuordnungen" das Kontrollkästchen "Zuordnungen kopieren", um alle Kategorien und Elemente des Geräts zu kopieren.
   - Sie können auf dieser Registerkarte beliebige Daten ändern, hinzufügen oder löschen. Die geänderten Daten werden auf mehrere Geräte in der Liste "Ausgewählte Geräte" sowie auf das Gerät kopiert, das aktuell im Feld "Gerätename" angezeigt wird. **Optional.**
7. Markieren Sie auf der Registerkarte "Einsatzort und Kontakte" das Kontrollkästchen für die zu kopierenden Informationen.
   - Markieren Sie das Kontrollkästchen "Standortinformationen kopieren", um die Standortinformationen zu kopieren, die im Bereich "Einsatzort" angezeigt werden.
   - Markieren Sie das Kontrollkästchen "Kontaktinformationen kopieren", um die Kontaktinformationen zu kopieren, die im Bereich "Kontakte" angezeigt werden.
   - Sie können auf diesen Registerkarten beliebige Daten ändern, hinzufügen oder löschen. Die geänderten Daten werden auf mehrere Geräte in der Liste "Ausgewählte Geräte" sowie auf das Gerät kopiert, das aktuell im Feld "Gerätename" angezeigt wird. **Optional.**

8. Klicken Sie zum Massenkopieren auf OK. Eine Meldung wird eingeblendet, nachdem die ausgewählten Informationen kopiert wurden.

Konfigurieren der mit KX2 2.3 oder höher verbundenen analogen KVM-Switches

KX2 Version 2.3 ermöglicht Ihnen, einen generischen analogen KVM-Switch mit einem Zielport zu verbinden. Der generische analoge KVM-Switch und seine Ports stehen CC-SG als Knoten zur Verfügung.

Sie müssen diese zuerst in der KX2-Webschnittstelle konfigurieren und KX2 dann zu CC-SG hinzufügen.

Hinzufügen eines mit KX2 verbundenen KVM-Switches

Mit dieser Vorgehensweise wird KX2 über den Administrations-Client ein KVM-Switch hinzugefügt. Sie können KVM-Switches auch über einen CSV-Import hinzufügen. Siehe ***Anforderungen an Geräte-CSV-Dateien*** (siehe "***Anforderungen an CSV-Dateien – Geräte***" auf Seite 93).

So fügen Sie einen mit KX2 verbundenen KVM-Switch hinzu:

1. Konfigurieren Sie den KVM-Switch in KX2 korrekt. Siehe Konfigurieren und Aktivieren von Schichten sowie Konfigurieren von KVM-Switches im Dominion KX II-Benutzerhandbuch. Auf die Dominion KX II-Online-Hilfe können Sie über http://www.raritan.com/support/online-help/ zugreifen.
2. Konfigurieren Sie das KX2-Gerät ordnungsgemäß in CC-SG. Siehe ***KVM- oder serielle Geräte hinzufügen*** (auf Seite 64).
3. CC-SG erkennt den KVM-Switch am Port von KX2 und fügt das Gerätesymbol auf ein oder zwei Registerkarten hinzu:
   - Auf der Registerkarte "Geräte" wird der KVM-Switch unterhalb des KX2-Geräts angezeigt, an das er angeschlossen ist.
   - Auf der Registerkarte "Knoten" wird der KVM-Switch als Knoten mit einer hinzugefügten Browserschnittstelle angezeigt, wenn Sie eine URL-Adresse für den Zugriff auf den KVM-Switch auf dem KX2-Gerät eingegeben haben.

Konfigurieren von Ports auf einem mit KX2 verbundenen analogen KVM-Switch-Gerät

Wenn die Ports des analogen KVM-Switch-Geräts noch nicht in CC-SG konfiguriert wurden, müssen Sie sie gemäß den Anweisungen in diesem Abschnitt konfigurieren. Andernfalls werden der KVM-Switch und dessen Ports nicht auf den Registerkarten "Geräte" und "Knoten" angezeigt. Eine Out-of-Band-KVM-Schnittstelle wird automatisch zu einem KVM-Switch-Knoten hinzugefügt.

So konfigurieren Sie Ports im KVM-Switch-Geräteprofil:

1. Klicken Sie auf der Registerkarte "Geräte" auf das Pluszeichen (+) neben dem KX2-Gerät, das an das KVM-Switch-Gerät angeschlossen ist.
2. Wählen Sie den KVM-Switch aus, dessen Ports Sie konfigurieren möchten.
3. Wählen Sie im Bildschirm "Geräteprofil" die Registerkarte "KVM Switch Ports" (KVM-Switch-Ports).
4. Aktivieren Sie das Kontrollkästchen für jeden zu konfigurierenden Slot, und klicken Sie dann auf OK.

So konfigurieren Sie Slots im Bildschirm "Ports konfigurieren":

1. Klicken Sie auf der Registerkarte "Geräte" auf das Pluszeichen (+) neben dem KX2-Gerät, das an das KVM-Switch-Gerät angeschlossen ist.
2. Wählen Sie das KVM-Switch-Gerät aus, dessen Ports Sie konfigurieren möchten.
3. Wählen Sie "Geräte > Portmanager > Ports konfigurieren".
   - Wenn Sie mehrere Ports mit den auf der Seite angezeigten Standardnamen konfigurieren möchten, aktivieren Sie das Kontrollkästchen für jeden zu konfigurierenden Port. Klicken Sie dann auf OK, um jeden Port mit dem Standardnamen zu konfigurieren.
   - Um jeden Port einzeln zu konfigurieren, klicken Sie neben dem entsprechenden Port auf die Schaltfläche "Konfigurieren". Geben Sie anschließend einen Namen für den Port in das Feld "Portname" und einen Knotennamen in das Feld "Knotenname" ein. Die standardmäßige Zugriffsanwendung wird entsprechend der Standardanwendung festgelegt, die Sie für "KVM-Switch: KVM" im Anwendungsmanager ausgewählt haben. Um die Standardanwendung zu ändern, klicken Sie auf das Dropdown-Menü "Zugriffsanwendung" und wählen die gewünschte Anwendung aus der Liste aus. Klicken Sie zum Konfigurieren des Ports auf OK.

So konfigurieren Sie Slots mithilfe des Befehls "Blades konfigurieren":

1. Klicken Sie auf der Registerkarte "Geräte" auf das Pluszeichen (+) neben dem KX2-Gerät, das an das KVM-Switch-Gerät angeschlossen ist.
2. Wählen Sie das KVM-Switch-Gerät aus, dessen Ports Sie konfigurieren möchten.
3. Wählen Sie "Knoten > Ports konfigurieren".
   - Wenn Sie mehrere Ports mit den auf der Seite angezeigten Standardnamen konfigurieren möchten, aktivieren Sie das Kontrollkästchen für jeden zu konfigurierenden Port. Klicken Sie dann auf OK, um jeden Port mit dem Standardnamen zu konfigurieren.
   - Um jeden Port einzeln zu konfigurieren, klicken Sie neben dem entsprechenden Port auf die Schaltfläche "Konfigurieren". Geben Sie anschließend einen Namen für den Port in das Feld "Portname" und einen Knotennamen in das Feld "Knotenname" ein. Die standardmäßige Zugriffsanwendung wird entsprechend der Standardanwendung festgelegt, die Sie für "KVM-Switch: KVM" im Anwendungsmanager ausgewählt haben. Um die Standardanwendung zu ändern, klicken Sie auf das Dropdown-Menü "Zugriffsanwendung" und wählen die gewünschte Anwendung aus der Liste aus. Klicken Sie zum Konfigurieren des Ports auf OK.

Gerätegruppenmanager

Mit dem Gerätegruppenmanager können Sie Gerätegruppen hinzufügen, bearbeiten und löschen. Wenn Sie eine neue Gerätegruppe hinzufügen, können Sie eine Richtlinie mit unbeschränktem Zugriff für die Gruppe erstellen. Siehe ***Richtlinien für die Zugriffssteuerung*** (auf Seite 210).

Überblick über Gerätegruppen

Gerätegruppen werden zur Verwaltung von mehreren Geräten verwendet. Die Gerätegruppe dient als Basis für eine Richtlinie, die den Zugriff auf diese Gerätegruppe zulässt oder verweigert. Siehe ***Richtlinien hinzufügen*** (auf Seite 211). Geräte können manuell mit der Methode "Auswählen" oder durch Erstellen eines booleschen Ausdrucks gruppiert werden, der eine Gruppe gemeinsamer Attribute mithilfe der Methode "Beschreiben" beschreibt.

Wenn Sie den Setup-Assistenten zum Erstellen von Kategorien und Elementen für Geräte verwenden, werden einige Mittel zum Verwalten von Konten mit gemeinsamen Attributen erstellt. CC-SG erstellt automatisch Zugriffsrichtlinien basierend auf diesen Elementen. Ausführliche Informationen zum Erstellen von Kategorien und Elementen finden Sie unter ***Zuordnungen, Kategorien und Elemente*** (auf Seite 49).

So zeigen Sie Gerätegruppen an:

- Wählen Sie "Zuordnungen > Gerätegruppen". Das Fenster "Gerätegruppenmanager" wird angezeigt. Die Liste der vorhandenen Gerätegruppen wird links angezeigt, und Details der ausgewählten Gerätegruppe werden im Hauptfenster angezeigt.
  - Eine Liste der vorhandenen Gerätegruppen wird links angezeigt. Klicken Sie auf eine Gerätegruppe, um die Details dieser Gruppe im Gerätegruppenmanager anzuzeigen.
  - Die Gruppe wurde willkürlich zusammengestellt. Die Registerkarte "Geräte auswählen" wird mit einer Liste der Geräte angezeigt, die der Gruppe angehören oder nicht angehören.
  - Wurde die Gruppe basierend auf gemeinsamen Attributen gebildet, werden auf der Registerkarte "Geräte beschreiben" die Regeln angezeigt, die die Auswahl der Geräte für die Gruppe bestimmt haben.
  - Geben Sie zur Suche eines Geräts in der Gerätegruppenliste unten in der Liste einen Suchbegriff in das Feld "Suchen" ein. Klicken Sie dann auf "Suchen". Die Suchmethode wird über den Bildschirm Mein Profil konfiguriert. Siehe ***Benutzer und Benutzergruppen*** (auf Seite 185).
  - Wenn Sie eine Gruppe anzeigen, die auf Attributen basiert, können Sie über "Geräte anzeigen" eine Liste der Geräte anzeigen, die der Gerätegruppe zugeordnet sind. Im Fenster "Geräte in der Gerätegruppe" werden die Geräte und ihre Attribute angezeigt.
- Wählen Sie "Berichte > Geräte > Gerätegruppendaten". Eine Liste mit den vorhandenen Gerätegruppen wird angezeigt. Doppelklicken Sie auf eine Zeile, um die Geräte für eine Gerätegruppe anzuzeigen.

Gerätegruppen hinzufügen

So fügen Sie eine Gerätegruppe hinzu:

1. Wählen Sie "Zuordnungen > Gerätegruppen". Das Fenster "Gerätegruppenmanager" wird angezeigt. Vorhandene Gerätegruppen werden im linken Fensterbereich angezeigt.
2. Klicken Sie auf der Symbolleiste auf das Symbol "Neue Gruppe" . Der Fensterbereich "Gerätegruppe: Neu" wird angezeigt.
3. Geben Sie in das Feld "Gruppenname" einen Namen für die Gerätegruppe ein, die Sie erstellen möchten. Weitere Informationen zu den Regeln, die von CC-SG für die Länge von Namen verwendet werden, finden Sie unter ***Benennungskonventionen*** (siehe "***Benennungsregeln***" auf Seite 457).
4. Sie haben zwei Möglichkeiten, Geräte einer Gruppe hinzuzufügen: Geräte auswählen und Geräte beschreiben. Auf der Registerkarte "Geräte auswählen" können Sie auswählen, welche Geräte der Gruppe zugeordnet werden sollen. Wählen Sie die Geräte dazu einfach in der Liste der verfügbaren Geräte aus. Auf der Registerkarte "Geräte beschreiben" können Sie Regeln angeben, die Geräte beschreiben. Geräte, deren Parameter diesen Regeln entsprechen, werden der Gruppe hinzugefügt.

So fügen Sie eine Gerätegruppe mit der Option "Geräte auswählen" hinzu:

1. Klicken Sie im Fensterbereich "Gerätegruppe: Neu" auf die Registerkarte "Geräte beschreiben".
2. Wählen Sie in der Liste "Verfügbar" das Gerät aus, das Sie der Gruppe hinzufügen möchten, und klicken Sie dann auf "Hinzufügen", um das Gerät in die Liste "Ausgewählt" zu verschieben. Geräte, die sich in der Liste "Ausgewählt" befinden, werden der Gruppe hinzugefügt.
   - Wählen Sie zum Entfernen eines Geräts aus der Gruppe den Gerätenamen in der Liste "Ausgewählt" aus, und klicken Sie auf "Entfernen".
   - Sie können das Gerät in der Liste "Verfügbar" oder "Ausgewählt" suchen. Geben Sie den Suchbegriff in das Feld unter der Liste ein, und klicken Sie auf "Los".
3. Markieren Sie das Kontrollkästchen "Richtlinie mit unbeschränktem Zugriff für Gruppe erstellen", um eine Richtlinie für diese Gerätegruppe zu erstellen, die jederzeit den Zugriff auf alle Geräte in der Gruppe mit Steuerberechtigung zulässt.
4. Um eine weitere Gerätegruppe hinzuzufügen, klicken Sie auf "Übernehmen", um diese Gruppe zu speichern, und wiederholen Sie diese Schritte. **Optional.**

5. Klicken Sie auf OK, nachdem Sie alle gewünschten Gerätegruppen hinzugefügt haben, um Ihre Änderungen zu speichern.

So fügen Sie eine Gerätegruppe mit der Option "Geräte beschreiben" hinzu:

1. Klicken Sie im Fensterbereich "Gerätegruppe: Neu" auf die Registerkarte "Geräte beschreiben". Auf der Registerkarte "Geräte beschreiben" erstellen Sie eine Regeltabelle, in der die Geräte beschrieben werden, die Sie der Gruppe zuordnen möchten.
2. Klicken Sie auf das Symbol zum Einfügen einer neuen Zeile , um eine neue Zeile in die Tabelle einzufügen.
3. Doppelklicken Sie auf die Zelle, die für jede Spalte erstellt wurde, um das Dropdown-Menü anzuzeigen. Wählen Sie in jeder Liste die gewünschten Regelkomponenten aus.
   - Präfix: Feld leer lassen oder NOT auswählen. Wenn NOT ausgewählt ist, sucht diese Regel nach Werten, die dem Ausdruck nicht entsprechen.
   - Kategorie: Wählen Sie ein Attribut aus, das in der Regel bewertet wird. Es sind alle Kategorien verfügbar, die Sie im Zuordnungsmanager erstellt haben. Wenn ein Blade-Chassis im System konfiguriert wurde, ist standardmäßig eine Blade-Chassis-Kategorie verfügbar.
   - Operator: Wählen Sie einen Vergleichsvorgang, der zwischen Kategorien und Elementen durchgeführt werden soll. Es stehen drei Operatoren zur Verfügung: = (ist gleich), LIKE (zum Suchen des Elements in einem Namen) und <> (ist nicht gleich).
   - Element: Wählen Sie einen Wert für das Kategorieattribut zum Vergleich aus. Hier werden nur Elemente dargestellt, die der ausgewählten Kategorie zugewiesen sind. (Beispiel: wenn eine Kategorie "Abteilung" bewertet wird, werden Elemente mit der Bezeichnung "Einsatzort" nicht angezeigt).
   - Regelname: Der Name, der der Regel in dieser Zeile zugewiesen wurde. Dieser Name kann nicht bearbeitet werden. Er wird zur Beschreibung im Feld "Kurzer Ausdruck" verwendet.
4. Um eine weitere Regel hinzuzufügen, klicken Sie auf das Symbol "Neue Zeile einfügen" , und nehmen Sie dann die entsprechenden Konfigurationen vor. Wenn Sie mehrere Regeln konfigurieren, können Sie genauere Beschreibungen anfertigen, indem Sie mehrere Kriterien zur Bewertung von Geräten bereitstellen.

5. Die Tabelle mit Regeln stellt nur Kriterien zur Bewertung von Knoten bereit. Definieren Sie eine Beschreibung für die Gerätegruppe, indem Sie die Regeln nach Regelname zum Feld Kurzer Ausdruck hinzufügen. Erfordert die Beschreibung nur eine Regel, geben Sie den Namen der Regel in das Feld ein. Werden mehrere Regeln bewertet, geben Sie die Regeln in das Feld mithilfe logischer Operatoren ein, um die Regeln in ihrer Beziehung zueinander zu beschreiben:

   - &: der UND-Operator. Ein Knoten muss die Regeln auf beiden Seiten dieses Operators für die Beschreibung (oder den Abschnitt einer Beschreibung) erfüllen, um als wahr bewertet zu werden.
   - | - der ODER Operator. Ein Gerät muss nur eine Regel auf einer Seite dieses Operators für die Beschreibung (oder den Abschnitt einer Beschreibung) erfüllen, um als wahr bewertet zu werden.
   - (und) – Gruppierungsoperatoren. Die Beschreibung wird in einen Unterabschnitt aufgeteilt, der in Klammern steht. Der Abschnitt innerhalb der Klammern wird bewertet, bevor die restliche Beschreibung mit dem Knoten verglichen wird. Gruppen in Klammern können in anderen Gruppen in Klammern verschachtelt werden.

   Beispiel 1: Wenn Sie Geräte beschreiben möchten, die zur Technikabteilung gehören, muss die Regel wie folgt aussehen: Abteilung = Technik. Dies wird als Regel0 bezeichnet. Geben Sie Regel0 in das Feld "Kurzer Ausdruck" ein.

   Beispiel 2: Wenn Sie eine Gerätegruppe beschreiben möchten, die zur Technikabteilung gehört oder den Standort "Philadelphia" aufweist, und festlegen möchten, dass alle Geräte mindestens über 1 GB Speicher verfügen müssen, dann müssen Sie drei Regeln erstellen. Abteilung = Technik (Regel0) Standort = Philadelphia (Regel1) Speicher = 1GB (Regel2). Diese Regeln müssen in Relation zueinander gesetzt werden. Da das Gerät entweder der Technikabteilung angehören oder den Standort "Philadelphia" aufweisen kann, verwenden Sie den ODER Operator |, um die beiden zu verbinden: Regel0 | Regel1. Lassen Sie diesen Vergleich zuerst durchführen, indem Sie ihn in Klammern einschließen: (Regel0 | Regel1). Da die Geräte beide diesen Vergleich erfüllen UND 1 GB Speicher aufweisen müssen, wird der UND-Operator & verwendet, um diesen Abschnitt mit Regel2 zu verbinden: (Regel0 | Regel1) & Regel2. Geben Sie diesen Ausdruck in das Feld "Kurzer Ausdruck" ein.

Hinweis: Vor und nach den Operatoren muss ein Leerzeichen sowie das Zeichen | vorhanden sein. Andernfalls wird der Wert im Feld "Kurzer Ausdruck" auf den Standardausdruck zurückgesetzt, d. h. Regel0 & Regel1 & Regel2 usw., wenn Sie eine Regel aus der Tabelle löschen.

- Um eine Zeile aus der Tabelle zu entfernen, wählen Sie die Zeile aus, und klicken Sie auf das Symbol zum Entfernen der Zeile .
- Um eine Liste der Geräte anzuzeigen, deren Parameter den von Ihnen definierten Regeln entsprechen, klicken Sie auf "Geräte anzeigen".

6. Klicken Sie auf "Überprüfen", wenn eine Beschreibung im Feld "Kurzer Ausdruck" enthalten ist. Wurde die Beschreibung fehlerhaft gebildet, wird ein Warnhinweis angezeigt. Wurde die Beschreibung richtig gebildet, wird eine normalisierte Form des Ausdrucks im Feld "Normalisierter Ausdruck" angezeigt.
7. Klicken Sie auf "Geräte anzeigen", um anzuzeigen, welche Knoten diese Anforderungen erfüllen. Ein Ergebnisfenster "Geräte in der Gerätegruppe" wird mit den Geräten angezeigt, die durch den aktuellen Ausdruck zusammengefasst werden. Sie können dadurch prüfen, ob die Beschreibung richtig geschrieben wurde. Ist dies nicht der Fall, können Sie zur Regeltabelle oder dem Feld "Kurzer Ausdruck" wechseln, um Anpassungen vorzunehmen.
8. Markieren Sie das Kontrollkästchen "Richtlinie mit unbeschränktem Zugriff für Gruppe erstellen", um eine Richtlinie für diese Gerätegruppe zu erstellen, die jederzeit den Zugriff auf alle Geräte in der Gruppe mit Steuerberechtigung zulässt.
9. Um eine weitere Gerätegruppe hinzuzufügen, klicken Sie auf "Übernehmen", um diese Gruppe zu speichern, und wiederholen Sie diese Schritte. **Optional.**
10. Klicken Sie auf OK, nachdem Sie alle gewünschten Gerätegruppen hinzugefügt haben, um Ihre Änderungen zu speichern.

Methode "Beschreiben" und Methode "Auswählen"

Verwenden Sie die Methode "Beschreiben", wenn Ihre Gruppe auf einem Attribut des Knotens oder der Geräte basieren soll, z. B. den Kategorien und Elementen. Der Vorteil dieser Methode besteht darin, dass Geräte oder Knoten automatisch in die Gruppe aufgenommen werden, wenn Sie mehrere Geräte oder Knoten mit denselben beschriebenen Attributen hinzufügen.

Verwenden Sie die Methode "Auswählen", wenn Sie lediglich eine Gruppe bestimmter Knoten manuell erstellen möchten. Neue Knoten und Geräte, die zu CC-SG hinzugefügt werden, werden nicht automatisch in diese Gruppen eingefügt. Sie müssen die neuen Knoten bzw. Geräte manuell hinzufügen, nachdem Sie sie zu CC-SG hinzugefügt haben.

Diese beiden Methoden können nicht kombiniert werden.

Nachdem eine Gruppe mit einer Methode erstellt wurde, müssen Sie diese mit derselben Methode bearbeiten. Bei einem Methodenwechsel werden die aktuellen Gruppeneinstellungen überschrieben.

Gerätegruppen bearbeiten

So bearbeiten Sie eine Gerätegruppe:

1. Wählen Sie "Zuordnungen > Gerätegruppen". Das Fenster "Gerätegruppenmanager" wird angezeigt.
2. Vorhandene Gerätegruppen werden im linken Fensterbereich angezeigt. Wählen Sie die Gerätegruppe aus, deren Namen Sie ändern möchten. Der Fensterbereich für Gerätegruppendetails wird angezeigt.
3. Geben Sie einen neuen Namen für die Gerätegruppe in das Feld "Gruppenname" ein. **Optional.**
4. Bearbeiten Sie die Geräte, die in der Gerätegruppe enthalten sind, über die Registerkarten "Geräte auswählen" oder "Geräte beschreiben". Siehe ***Gerätegruppen hinzufügen*** (auf Seite 87).
5. Klicken Sie zum Speichern der Änderungen auf OK.

Gerätegruppen löschen

So löschen Sie eine Gerätegruppe:

1. Wählen Sie "Zuordnungen > Gerätegruppen". Das Fenster "Gerätegruppenmanager" wird angezeigt.
2. Vorhandene Gerätegruppen werden im linken Fensterbereich angezeigt. Wählen Sie die Gerätegruppe aus, die gelöscht werden soll. Der Fensterbereich für Gerätegruppendetails wird angezeigt.
3. Wählen Sie "Gruppen > Löschen".

4. Der Fensterbereich zum Löschen von Gerätegruppen wird angezeigt. Klicken Sie auf "Löschen".
5. Klicken Sie in der Bestätigungsmeldung auf "Ja".

Geräte per CSV-Dateiimport hinzufügen

Sie können Geräte zu CC-SG hinzufügen, indem Sie eine CSV-Datei, in der die Werte enthalten sind, importieren. Sie benötigen die Berechtigungen für Geräte-, Port- und Knotenverwaltung sowie CC-Setup und -Steuerung, um Geräte importieren bzw. exportieren zu können.

Ihnen muss eine Richtlinie zugewiesen sein, mit der Sie auf alle relevanten Geräte und Knoten zugreifen können. Hierfür wird eine Richtlinie mit vollständigem Zugriff auf alle Knoten und alle Geräte empfohlen.

Hinweis: Sie können keine P2SC-Geräte per CSV-Dateiimport hinzufügen.

Anforderungen an CSV-Dateien – Geräte

Durch die CSV-Datei für Geräte werden die Geräte, Ports sowie deren Informationen, die zum Hinzufügen zu CC-SG erforderlich sind, definiert.

- Bei Geräten, die an Ports angeschlossene Powerstrips unterstützen (SX, KX, KX2, KSX2), wird durch Konfigurieren des Ports der Powerstrip konfiguriert.
- Wenn Geräteports konfiguriert werden, wird von CC-SG außerdem ein Knoten mit Out-of-Band-KVM- oder serieller Out-of-Band-Schnittstelle für jeden Port hinzugefügt.
- Um Blades hinzuzufügen, muss der Blade-Server über ein CIM an ein KX2-Gerät angeschlossen sein. Das KX2-Gerät muss entweder bereits zu CC-SG hinzugefügt worden oder in der gleichen CSV-Datei enthalten sein.
- Exportieren Sie eine Datei aus CC-SG, um die Kommentare anzuzeigen. Diese enthalten alle Tags und Parameter, die zum Erstellen einer gültigen CSV-Datei erforderlich sind. Siehe ***Geräte exportieren*** (auf Seite 99).
- Erfüllen Sie die zusätzlichen Anforderungen für alle CSV-Dateien. Siehe ***Häufige Anforderungen an CSV-Dateien*** (siehe "***Häufige Anforderungen für CSV-Dateien***" auf Seite 434).

So fügen Sie ein Gerät zur CSV-Datei hinzu:

Spaltennummer	Tag oder Wert	Details
1	`ADD (Hinzufügen)`	Die erste Spalte für alle Tags ist der Befehl `ADD` (Hinzufügen).
2	`DEVICE (Gerät)`	Geben Sie das Tag wie beschrieben ein. Bei Tags wird die Groß- und Kleinschreibung nicht berücksichtigt.
3	Gerätetyp	Erforderliches Feld. Geben Sie den Gerätetyp wie hier angegeben ein: `KX, KX2, KSX, KSX2, KX101, KX2-101, IP-Reach, SX,` oder `PX`
4	Gerätename	Erforderliches Feld. Der Gerätename darf weder Leerzeichen noch bestimmte Sonderzeichen enthalten. Dominion PX-Gerätenamen dürfen keine Punkte enthalten. Beim

Spaltennummer	Tag oder Wert	Details
		Importieren werden Punkte in Bindestriche umgewandelt.
5	IP-Adresse oder Hostname	Erforderliches Feld.
6	Benutzername	Erforderliches Feld.
7	Kennwort	Erforderliches Feld.
8	Heartbeat	Die Standardwerte werden im Administrations-Client auf der Registerkarte "Administration > Konfiguration > Geräteeinstellungen" konfiguriert.
9	TCP-Port	Die Standardwerte werden im Administrations-Client auf der Registerkarte "Administration > Konfiguration > Geräteeinstellungen" konfiguriert.
10	Alle Ports konfigurieren	`TRUE` (Wahr) oder `FALSE` (Falsch) Der Standardwert für Dominion PX-Geräte ist `TRUE` (Wahr). Für alle anderen Gerätetypen ist der Standardwert `FALSE` (Falsch). Wenn "TRUE" (Wahr) eingestellt ist, werden alle Ports konfiguriert, und es werden Knoten mit der entsprechenden Out-of-Band-Schnittstelle erstellt. Wenn "FALSE" (Falsch) eingestellt ist, werden nur Ports konfiguriert, die über einen entsprechenden Eintrag ADD DEVICE-PORT (Geräteport hinzufügen) in der CSV-Datei verfügen.
11	Direkten Zugriff zulassen	`TRUE` (Wahr) oder `FALSE` (Falsch) Der Standardwert ist `FALSE` (Falsch). Diese Einstellung gilt nur für SX- und KX2-Geräte der Version 2.2 oder höher.
12	Beschreibung	Optional.

So fügen Sie einen Port zur CSV-Datei hinzu:

Verwenden Sie das Tag DEVICE-PORT (Geräteport) nur, wenn Sie ein Gerät hinzufügen, bei dem die Option "Alle Ports konfigurieren" auf "FALSE" (Falsch) eingestellt ist, und Sie Ports individuell festlegen möchten. Die von Ihnen hinzugefügten Ports dürfen beim Importieren der CSV-Datei in CC-SG nicht konfiguriert sein.

Spaltennummer	Tag oder Wert	Details
1	`ADD (Hinzufügen)`	Die erste Spalte für alle Tags ist der Befehl "ADD" (Hinzufügen).
2	`DEVICE-PORT (Geräteport)`	Geben Sie das Tag wie beschrieben ein. Bei Tags wird die Groß- und Kleinschreibung nicht berücksichtigt.
3	Gerätename	Erforderliches Feld.

4	Porttyp	Erforderliches Feld.
		Geben Sie den Porttyp wie hier angegeben ein:
		`KVM`
		`SERIELL`
		`OUTLET oder POWER`
		Verwenden Sie "`OUTLET`" oder "`POWER`", um Ausgänge auf einem PX-Gerät zu konfigurieren.

5	Port- oder Ausgangsnummer	Erforderliches Feld.
6	Port- oder Ausgangsname	Optional. Wenn keine Angaben gemacht werden, wird ein Standardname oder der bereits auf der Geräteebene zugewiesene Name verwendet.
7	Knotenname	Geben Sie für KVM- und serielle Ports einen Namen für den Knoten ein, der erstellt wird, wenn dieser Port konfiguriert wird.

So fügen Sie ein Blade zur CSV-Datei hinzu:

Spaltennummer	Tag oder Wert	Details
1	`ADD (Hinzufügen)`	Die erste Spalte für alle Tags ist der Befehl `ADD` (Hinzufügen).

Spaltennummer	Tag oder Wert	Details
2	`DEVICE-BLADE (Geräteblade)`	Geben Sie das Tag wie beschrieben ein. Bei Tags wird die Groß- und Kleinschreibung nicht berücksichtigt.
3	Gerätename	Erforderliches Feld.
4	Portnummer	Erforderliches Feld.
5	Bladenummer	Erforderliches Feld.
6	Bladename	Optional. Wenn keine Angaben gemacht werden, wird der auf der Geräteebene zugewiesene Name verwendet. Wenn in der CSV-Datei ein Name angegeben wird, wird dieser auf der Geräteebene übernommen.
7	Knotenname	Geben Sie einen Namen für den Knoten ein, der erstellt wird, wenn dieses Blade konfiguriert wird.

So fügen Sie einen mit KX2 verbundenen mehrschichtigen KVM-Switch hinzu:

KX2-Ports mit verbundenen mehrschichtigen KVM-Switches müssen als Typ "`KVM`" importiert werden.

Spaltennummer	Tag oder Wert	Details
1	`ADD (Hinzufügen)`	Die erste Spalte für alle Tags ist der Befehl "ADD" (Hinzufügen).
2	`DEVICE-KVMSWITCHPORT`	Geben Sie das Tag wie beschrieben ein. Bei Tags wird die Groß- und Kleinschreibung nicht berücksichtigt.
3	Gerätename	Erforderliches Feld.
4	Portnummer	Der Port, mit dem der KVM-Switch verbunden ist. Erforderliches Feld.
5	KVM-Switch-Port-Nummer	Erforderliches Feld.
6	KVM-Switch-Port-Name	Optional. Wenn keine Angaben gemacht werden, wird der auf der Geräteebene zugewiesene Name verwendet. Wenn in der CSV-Datei

Spaltennummer	Tag oder Wert	Details
		ein Name angegeben wird, wird dieser auf der Geräteebene übernommen.
7	Knotenname	Geben Sie einen Namen für den Knoten ein, der bei der Konfiguration dieses KVM-Switch-Ports erstellt wird.

So weisen Sie eine Kategorie oder ein Element einem Gerät in der CSV-Datei zu:

Kategorien und Elemente müssen bereits in CC-SG erstellt worden sein.

Sie können einem Gerät in der CSV-Datei mehrere Elemente derselben Kategorie zuweisen.

Spaltennummer	Tag oder Wert	Details
1	`ADD (Hinzufügen)`	Die erste Spalte für alle Tags ist der Befehl `ADD` (Hinzufügen).
2	`DEVICE-CATEGORYELEMENT (Gerätekategorie-Element)`	Geben Sie das Tag wie beschrieben ein. Bei Tags wird die Groß- und Kleinschreibung nicht berücksichtigt.
3	Gerätename	Erforderliches Feld.
4	Kategoriename	Erforderliches Feld.
5	Elementname	Erforderliches Feld.

Beispiel-CSV-Datei für Geräte

```
ADD (Hinzufügen), DEVICE (Gerät), DOMINION KX2,
Lab-Test,192.168.50.123,ST Lab-KVM, Benutzername,
Kennwort,,,,

ADD (Hinzufügen), DEVICE-PORT (Geräteport), Lab-Test,
KVM, 1, Mailserver, Mailserver

ADD (Hinzufügen), DEVICE-PORT (Geräteport), Lab-Test,
KVM, 2, DNS-Server, DNS-Server

ADD (Hinzufügen), DEVICE-PORT (Geräteport), Lab-Test,
KVM, 3

ADD (Hinzufügen), DEVICE-PORT (Geräteport), Lab-Test,
KVM, 4

ADD (Hinzufügen), DEVICE-CATEGORYELEMENT
(Gerätekategorie-Element), Lab-Test, Position, Rack17
```

Geräte importieren

Wenn Sie die CSV-Datei erstellt haben, überprüfen Sie sie auf Fehler und importieren Sie sie anschließend.

Doppelte Einträge werden übersprungen und somit nicht hinzugefügt.

So importieren Sie Geräte:

1. Wählen Sie "Administration > Importieren > Geräte importieren".
2. Klicken Sie auf "Durchsuchen" und wählen Sie die zu importierende CSV-Datei aus. Klicken Sie auf "Öffnen".
3. Klicken Sie auf Überprüfen. Die Dateiinhalte werden im Bereich "Analysebericht" angezeigt.
   - Wenn die Datei ungültig ist, wird eine Fehlermeldung angezeigt. Klicken Sie auf "OK". Im Bereich "Probleme" auf der Seite wird eine Beschreibung der Dateiprobleme aufgeführt. Klicken Sie auf "In Datei speichern", um die Liste der Probleme zu speichern. Korrigieren Sie die CSV-Datei und versuchen Sie sie anschließend erneut zu validieren. Siehe ***Problembehebung bei CSV-Dateien*** (auf Seite 436).
4. Klicken Sie auf "Importieren".
5. Die Ergebnisse des Imports werden im Bereich "Aktionen" angezeigt. Erfolgreich importierte Elemente werden grün dargestellt. Nicht erfolgreich importierte Elemente werden rot dargestellt. Elemente, die aufgrund eines bereits vorhandenen oder bereits importierten Duplikats nicht erfolgreich importiert wurden, werden ebenso rot dargestellt.

6. Um weitere Details zu den Importergebnissen anzuzeigen, rufen Sie den Überwachungslistenbericht auf. Siehe ***Einträge in der Überwachungsliste für Importe*** (auf Seite 435).

Geräte exportieren

In der Exportdatei sind als erstes Kommentare enthalten, die jedes Element in der Datei beschreiben. Die Kommentare können als Anweisungen zum Erstellen einer Datei oder zum Importieren verwendet werden.

Hinweis: P2SC-Geräte werden nicht exportiert.

So exportieren Sie Geräte:

1. Wählen Sie "Administration > Exportieren > Geräte exportieren".
2. Klicken Sie auf "In Datei exportieren".
3. Geben Sie einen Namen für die Datei ein, und wählen Sie den Speicherort aus.
4. Klicken Sie auf Speichern.

Gerät aktualisieren

Sie können Geräte aktualisieren, wenn eine neue Version der Gerätefirmware verfügbar ist.

Wichtig: Stellen Sie anhand der Kompatibilitätsmatrix sicher, dass die neue Gerätefirmwareversion mit Ihrer CC-SG-Firmwareversion kompatibel ist. Wenn Sie sowohl CC-SG als auch ein Gerät oder eine Gerätegruppe aktualisieren müssen, aktualisieren Sie zuerst CC-SG und dann die Geräte.

So aktualisieren Sie ein Gerät:

1. Klicken Sie auf die Registerkarte "Geräte", und wählen Sie in der Gerätestrukturansicht ein Gerät aus.
2. Wählen Sie "Geräte > Gerätemanager > Gerät aktualisieren".
3. Firmwarename: Wählen Sie die entsprechende Firmware in der Liste aus. Diese Informationen werden von Raritan oder Ihrem Händler bereitgestellt.
4. Klicken Sie zum Aktualisieren des Geräts auf OK.
   - Das Aktualisieren von SX- und KX-Geräten dauert ca. 20 Minuten.
   - Wenn die Firmwareversion des Geräts mit CC-SG nicht kompatibel ist, wird eine Meldung angezeigt. Klicken Sie zum Aktualisieren des Geräts auf "Ja". Klicken Sie zum Abbrechen der Aktualisierung auf "Nein".

5. Eine Meldung wird angezeigt. Klicken Sie zum Neustarten des Geräts auf "Ja". Eine Meldung wird eingeblendet, wenn das Gerät aktualisiert wurde.
6. Schließen Sie Ihr Browserfenster, um sicherzustellen, dass Ihr Browser alle aktualisierten Dateien lädt. Melden Sie sich dann bei CC-SG in einem neuen Browserfenster an.

Gerätekonfiguration sichern

Sie können alle Benutzerdateien zur Konfiguration und Systemkonfiguration für ein ausgewähltes Gerät sichern. Falls Probleme bei Ihrem Gerät auftreten, können Sie die vorherige Konfiguration von CC-SG mithilfe der erstellten Sicherungsdatei wieder herstellen.

Auf CC-SG können maximal 3 Sicherungsdateien pro Gerät gespeichert werden. Wenn Sie mehr Sicherungen benötigen, können Sie eine Sicherungsdatei im Netzwerk speichern und diese anschließend von CC-SG löschen. Sie können auch zulassen, dass CC-SG die älteste Sicherungsdatei löscht. Diese Option wird als Warnung angezeigt, wenn Sie versuchen, eine vierte Sicherung anzulegen. Siehe ***Alle Konfigurationsdaten auf einem KX2-, KSX2- oder KX2-101-Gerät wiederherstellen*** (auf Seite 103).

Jedes Gerät sichert eventuell unterschiedliche Komponenten der Konfiguration. Lesen Sie das Benutzerhandbuch des zu sichernden Geräts, um weitere Informationen zu erhalten.

Hinweis: Beim Sichern eines SX 3.0.1-Geräts werden die angefügten PowerStrip-Konfigurationen nicht gesichert. Wenn Sie das SX 3.0.1-Gerät mit der Sicherung wiederherstellen, müssen Sie die PowerStrips neu konfigurieren.

So sichern Sie eine Gerätekonfiguration:

1. Klicken Sie auf die Registerkarte "Geräte", und wählen Sie das Gerät zum Sichern aus.
2. Wählen Sie "Geräte > Gerätemanager > Konfiguration > Sicherungsknoten".
3. Geben Sie einen Namen für diese Sicherung in das Feld Sicherungsname ein.
4. Geben Sie eine kurze Beschreibung für die Sicherung in das Feld "Beschreibung" ein. **Optional.**
5. Klicken Sie auf OK, um die Gerätekonfiguration zu sichern. Eine Meldung wird eingeblendet, wenn die Gerätekonfiguration gesichert wurde.

Gerätekonfiguration wiederherstellen

Die folgenden Gerätetypen ermöglichen Ihnen die Wiederherstellung einer vollständigen Sicherung der Gerätekonfiguration.

- KX
- KSX
- KX101
- SX
- IP-Reach

Bei KX2-, KSX2- und KX2-101-Geräten können Sie auswählen, welche Komponenten einer Sicherung Sie auf dem Gerät wiederherstellen möchten.

- Geschützt: Der gesamte Inhalt der ausgewählten Sicherungsdatei, mit Ausnahme der Netzwerkeinstellungen (Personality Package) und bei KX2-Geräten der Portkonfigurationseinstellungen, wird auf dem Gerät wiederhergestellt. Sie können mit der Option "Geschützt" die Sicherung eines Geräts auf einem anderen Gerät des gleichen Modells wiederherstellen (nur KX2, KSX2 und KX2-101).
- Vollständig: Der gesamte Inhalt der ausgewählten Sicherungsdatei wird auf dem Gerät wiederhergestellt.
- Benutzerdefiniert: Mit dieser Option können Sie die Geräteeinstellung, die Einstellungen für Benutzer- und Benutzergruppendaten oder beides wiederherstellen.

Gerätekonfiguration wiederherstellen (KX, KSX, KX101, SX, IP-Reach)

Sie können eine vollständige Sicherungskonfiguration auf KX, KSX, KX101, SX- und IP-Reach-Geräten wiederherstellen.

So stellen Sie eine vollständige Sicherung der Gerätekonfiguration wieder her:

1. Klicken Sie auf die Registerkarte "Geräte", und wählen Sie die Geräte aus, die Sie für eine Sicherungskonfiguration wieder herstellen möchten.
2. Wählen Sie "Geräte > Gerätemanager > Konfiguration > Wiederherstellen".
3. Wählen Sie in der Tabelle "Verfügbare Sicherungen" die Sicherungskonfiguration aus, die Sie auf dem Gerät wiederherstellen möchten.
4. Klicken Sie auf OK.
5. Klicken Sie zum Neustarten des Geräts auf "Ja". Eine Meldung wird eingeblendet, wenn alle Daten wiederhergestellt wurden.

Alle Konfigurationsdaten mit Ausnahme der Netzwerkeinstellungen auf einem KX2-, KSX2- oder KX2-101-Gerät wiederherstellen

Mit der Wiederherstellungsoption "Geschützt" können Sie alle Konfigurationsdaten einer Sicherungsdatei mit Ausnahme der Netzwerkeinstellungen auf einem KX2-, KSX2- oder KX2-101-Gerät wiederherstellen. Sie können mit der Option "Geschützt" die Sicherung eines Geräts auf einem anderen Gerät des gleichen Modells wiederherstellen (nur KX2, KSX2 und KX2-101).

So stellen Sie alle Konfigurationsdaten mit Ausnahme der Netzwerkeinstellungen auf einem KX2-, KSX2- oder KX2-101-Gerät wieder her:

1. Klicken Sie auf die Registerkarte "Geräte", und wählen Sie die Geräte aus, die Sie für eine Sicherungskonfiguration wieder herstellen möchten.
2. Wählen Sie "Geräte > Gerätemanager > Konfiguration > Wiederherstellen".
3. Wählen Sie in der Tabelle "Verfügbare Sicherungen" die Sicherungskonfiguration aus, die Sie auf dem Gerät wiederherstellen möchten.
4. Wiederherstellungstyp: Wählen Sie "Geschützt".
5. Klicken Sie auf OK.
6. Klicken Sie zum Neustarten des Geräts auf "Ja". Eine Meldung wird eingeblendet, wenn alle Benutzer- und Systemkonfigurationsdaten wiederhergestellt wurden.

Nur Geräteeinstellungen oder Benutzer- und Benutzergruppendaten auf einem KX2-, KSX2- oder KX2-101-Gerät wiederherstellen

Mit der Wiederherstellungsoption Benutzerdefiniert können Sie Geräteeinstellungen, Benutzer- und Benutzergruppendaten oder beides wiederherstellen.

So stellen Sie nur Geräteeinstellungen oder Benutzer- und Benutzergruppendaten auf einem KX2-, KSX2- oder KX2-101-Gerät wieder her:

1. Klicken Sie auf die Registerkarte "Geräte", und wählen Sie die Geräte aus, die Sie für eine Sicherungskonfiguration wieder herstellen möchten.
2. Wählen Sie "Geräte > Gerätemanager > Konfiguration > Wiederherstellen".
3. Wählen Sie in der Tabelle "Verfügbare Sicherungen" die Sicherungskonfiguration aus, die Sie auf dem Gerät wiederherstellen möchten.

4. Wiederherstellungstyp: Wählen Sie "Benutzerdefiniert".
5. Wiederherstellungsoptionen: Wählen Sie die Komponenten aus, die Sie auf dem Gerät wiederherstellen möchten: Geräteeinstellungen, Benutzer- und Benutzergruppendaten.
6. Klicken Sie auf OK.
7. Klicken Sie zum Neustarten des Geräts auf "Ja". Eine Meldung wird eingeblendet, wenn die Daten wiederhergestellt wurden.

Alle Konfigurationsdaten auf einem KX2-, KSX2- oder KX2-101-Gerät wiederherstellen

Mit der Wiederherstellungsoption "Vollständig" können Sie alle Konfigurationsdaten einer Sicherungsdatei auf einem KX2-, KSX2- oder KX2-101-Gerät wiederherstellen.

So stellen Sie alle Konfigurationsdaten auf einem KX2-, KSX2- oder KX2-101-Gerät wieder her:

1. Klicken Sie auf die Registerkarte "Geräte", und wählen Sie die Geräte aus, die Sie für eine Sicherungskonfiguration wieder herstellen möchten.
2. Wählen Sie "Geräte > Gerätemanager > Konfiguration > Wiederherstellen".
3. Wählen Sie in der Tabelle "Verfügbare Sicherungen" die Sicherungskonfiguration aus, die Sie auf dem Gerät wiederherstellen möchten.
4. Wiederherstellungstyp: Wählen Sie "Vollständig".
5. Klicken Sie auf OK.
6. Klicken Sie zum Neustarten des Geräts auf "Ja". Eine Meldung wird eingeblendet, wenn alle Benutzer- und Systemkonfigurationsdaten wiederhergestellt wurden.

Sicherungsdateien von Geräten speichern, hochladen und löschen

Sie können die Sicherungsdateien von Geräten auf der Seite "Gerätekonfiguration wiederherstellen" an einer Position auf Ihrem Netzwerk oder Ihrem lokalen Computer speichern. Sie können Sicherungsdateien von Geräten löschen, wenn Sie Platz für neue Sicherungen auf CC-SG schaffen müssen. Sie können auf Ihrem Netzwerk gespeicherte Sicherungsdateien von Geräten wieder an CC-SG senden, um sie zum Wiederherstellen einer Gerätekonfiguration zu verwenden.

So speichern Sie die Sicherungsdatei eines Geräts von CC-SG:

1. Klicken Sie auf die Registerkarte "Geräte", und wählen Sie ein Gerät.

2. Wählen Sie "Geräte > Gerätemanager > Konfiguration > Wiederherstellen".
3. Wählen Sie die Sicherungsdatei des Geräts, die Sie speichern möchten. Klicken Sie auf "In Datei speichern".
4. Wechseln Sie zu der Position, an der Sie die Datei speichern möchten. Klicken Sie auf Speichern.

So löschen Sie die Sicherungsdatei eines Geräts von CC-SG:

1. Klicken Sie auf die Registerkarte "Geräte", und wählen Sie ein Gerät.
2. Wählen Sie "Geräte > Gerätemanager > Konfiguration > Wiederherstellen".
3. Wählen Sie die Sicherungsdatei des Geräts, die Sie löschen möchten. Klicken Sie auf "Löschen".
4. Klicken Sie zum Bestätigen auf "Ja".

So senden Sie die Sicherungsdatei eines Geräts an CC-SG:

1. Klicken Sie auf die Registerkarte "Geräte", und wählen Sie ein Gerät.
2. Wählen Sie "Geräte > Gerätemanager > Konfiguration > Wiederherstellen".
3. Klicken Sie auf "Upload". Wechseln Sie zur Sicherungsdatei des Geräts, und wählen Sie diese aus. Der Dateityp ist .rfp. Klicken Sie auf "Öffnen".

   Die Sicherungsdatei des Geräts wird an CC-SG gesendet und wird auf der Seite angezeigt.

Gerätekonfiguration kopieren

Mithilfe der folgende Gerätetypen können Sie Konfigurationen von einem Gerät auf andere Geräte kopieren.

- SX
- KX2
- KSX2
- KX2-101

Die Konfiguration kann nur zwischen denselben Modellen mit derselben Anzahl Ports kopiert werden. Sie können z. B. nur die Konfiguration von einem KX2-864-Gerät auf andere KX2-864-Geräte kopieren.

Der Befehl "Konfiguration kopieren" kopiert alle Konfigurationsdaten, mit Ausnahme der Netzwerkeinstellungen (Personality Package) und bei KX2-Geräten der Portkonfigurationseinstellungen. Geräteeinstellungen und Benutzer- und Benutzergruppendaten werden alle bei diesem Vorgang kopiert.

So kopieren Sie eine Gerätekonfiguration:

1. Klicken Sie auf die Registerkarte "Geräte", und wählen Sie in der Gerätestrukturansicht das Gerät aus, dessen Konfiguration Sie auf andere Geräte kopieren möchten.
2. Wählen Sie "Geräte > Gerätemanager > Konfiguration > Konfiguration kopieren".
3. Wählen Sie die Methode für das Kopieren der Konfiguration aus.
   - Um die aktuellen Konfigurationsdaten zu kopieren, wählen Sie "Copy From Device" (Von Gerät kopieren) aus.
   - Um die Konfigurationsdaten aus einer Sicherungsdatei zu kopieren, die Sie zuvor in CC-SG gespeichert haben, wählen Sie "Copy From Backup File" (Von Sicherungsdatei kopieren) aus. Wählen Sie anschließend die Datei aus der Dropdown-Liste aus. Wenn keine Sicherungsdatei zur Verfügung steht, ist diese Option deaktiviert.
4. Klicken Sie auf die Dropdown-Liste "Gerätegruppe", und wählen Sie eine Gerätegruppe aus der Liste aus. Alle Geräte der ausgewählten Gerätegruppe werden in der Spalte "Verfügbar" angezeigt.
5. Markieren Sie in der Spalte "Verfügbar" die Geräte, auf die Sie diese Konfiguration kopieren möchten, und klicken Sie auf den Pfeil nach rechts, um die Geräte in die Spalte "Ausgewählt" zu verschieben. Mit dem Pfeil nach links werden die ausgewählten Geräte aus der Spalte "Ausgewählt" verschoben.
6. Klicken Sie auf OK, um die Konfiguration auf die Geräte in der Spalte "Ausgewählt" zu kopieren.

7. Wenn die Meldung zum Neustart angezeigt wird, klicken Sie zum Neustarten des Geräts auf "Ja". Eine Meldung wird eingeblendet, wenn die Gerätekonfiguration kopiert wurde.

Gerät neu starten

Starten Sie ein Gerät mit dem Befehl "Gerät neu starten" neu.

So starten Sie ein Gerät neu

1. Klicken Sie auf die Registerkarte "Geräte", und wählen Sie das Gerät zum Neustart aus.
2. Wählen Sie "Geräte > Gerätemanager > Gerät neu starten".
3. Klicken Sie zum Neustarten des Geräts auf OK.
4. Klicken Sie auf "Ja", um zu bestätigen, dass alle Benutzer, die auf das Gerät zugreifen, abgemeldet werden.

Gerät anpingen

Durch Anpingen eines Geräts können Sie feststellen, ob das Gerät in Ihrem Netzwerk verfügbar ist.

So pingen Sie ein Gerät an:

1. Klicken Sie auf die Registerkarte "Geräte", und wählen Sie das Gerät zum Anpingen aus.
2. Wählen Sie "Geräte > Gerätemanager > Gerät anpingen". Das Fenster "Gerät anpingen" wird mit dem Ergebnis des Ping-Befehls angezeigt.

CC-SG-Verwaltung eines Geräts unterbrechen

Sie können den Gerätebetrieb unterbrechen und damit vorübergehend die Steuerung durch CC-SG aussetzen, ohne die in CC-SG gespeicherten Konfigurationsdaten zu verlieren.

Informationen zum Planen einer Aufgabe, die den Betrieb von Geräten unterbricht oder fortsetzt, finden Sie unter ***Aufgaben planen*** (auf Seite 332).

So unterbrechen Sie die CC-SG-Verwaltung eines Geräts:

1. Klicken Sie auf die Registerkarte "Geräte", und wählen Sie die Geräte aus, deren CC-SG-Verwaltung unterbrochen werden soll.
2. Wählen Sie "Geräte > Gerätemanager > Verwaltung unterbrechen". Das Gerätesymbol in der Gerätestruktur zeigt an, dass das Gerät unterbrochen wurde.

Geräteverwaltung fortsetzen

Sie können die CC-SG-Verwaltung für ein unterbrochenes Gerät fortsetzen, damit es wieder von CC-SG gesteuert werden kann.

So setzen Sie die CC-SG-Verwaltung eines Geräts fort, dessen Verwaltung unterbrochen wurde:

1. Klicken Sie auf die Registerkarte "Geräte", und wählen Sie in der Gerätestrukturansicht das unterbrochene Gerät aus.
2. Wählen Sie "Geräte > Gerätemanager > Verwaltung fortsetzen". Das Gerätesymbol in der Gerätestruktur zeigt an, dass das Gerät aktiv ist.

Geräteverwaltung mit einer geplanten Aufgabe unterbrechen und fortsetzen

Um die Verwaltung mehrerer Geräte oder Gerätegruppen auf einmal zu unterbrechen oder fortzusetzen, müssen Sie eine Aufgabe planen, die den Vorgang an der Gerätegruppe sequenziell ausführt.

Die Aufgabe "Pause/Resume Device Management" (Geräteverwaltung unterbrechen/fortsetzen) eignet sich nicht für an verwaltete Geräte angeschlossene Blade-Chassis, an verwaltete Geräte angeschlossene Powerstrips und verwaltete Powerstrips.

Die Aufgabe wird bei der Ausführung als erfolgreich protokolliert, wenn alle Gerätevorgänge erfolgreich sind. Die Aufgabe wird als erfolgreich mit Ausnahmen protokolliert, wenn die Aufgabe zwar ausgeführt wird, manche Gerätevorgänge aber selbst nach der zulässigen Anzahl an Wiederholungen fehlschlagen. Die Aufgabe wird als fehlgeschlagen protokolliert, wenn alle Gerätevorgänge fehlschlagen.

So nehmen Sie mithilfe einer geplanten Aufgabe eine Massenunterbrechung und Massenfortsetzung der Geräteverwaltung vor:

1. Wählen Sie "Administration > Aufgaben". Informationen zum Erstellen einer neuen Aufgabe sowie zum Bearbeiten der Registerkarten "Hauptfenster", "Serie", "Wiederholen" und "Benachrichtigung" finden Sie unter ***Aufgaben planen*** (auf Seite 332).
   - Serie: Die Serienintervalle sind auf Stunden und Tage begrenzt.
   - Wiederholen: CC-SG wiederholt den Vorgang nur für die Geräte, die nicht angehalten oder fortgesetzt werden können.
2. Wählen Sie auf der Registerkarte "Aufgabendaten" die Option "Pause/Resume Device Management" (Geräteverwaltung unterbrechen/fortsetzen) im Feld "Aufgabenvorgang".

3. Wählen Sie "Verwaltung unterbrechen" oder "Verwaltung fortsetzen". Wenn Sie beide Aufgaben ausführen müssen, planen Sie für jede eine Aufgabe, und stimmen Sie die beiden Aufgaben zeitlich aufeinander ab.
4. Wählen Sie im Feld "Intervall (Sekunden)" die Anzahl Sekunden aus, die zwischen dem Abschluss des einen Vorgangs und dem Beginn des nächsten Vorgangs verstreichen soll.
5. Aktivieren Sie das Kontrollkästchen "Skip Device if Restart Required" (Gerät überspringen, wenn Neustart erforderlich), wenn CC-SG den Unterbrechungs- oder Fortsetzungsvorgang für ausgewählte Geräte überspringen soll, für die ein Neustart erforderlich wäre.
6. Wählen Sie die Geräte aus, die in der Aufgabe enthalten sein sollen. Wählen Sie dazu eine Gerätegruppe aus der Dropdown-Liste "Gerätegruppe". Wählen Sie die Geräte aus, die in die Liste "Verfügbar" aufgenommen werden sollen. Verschieben Sie die Geräte anschließend mit den Pfeilschaltflächen in die Liste "Ausgewählt". Die in der Liste "Ausgewählt" enthaltenen Geräte werden in den Unterbrechungs- oder Fortsetzungsvorgang aufgenommen.
   - Alle ausgewählten Geräte, die einen Neustart erfordern würden, werden beim Ausführen der Aufgabe übersprungen, wenn Sie das Kontrollkästchen "Skip Device if Restart Required" (Gerät überspringen, wenn Neustart erforderlich) aktiviert haben.
7. Klicken Sie auf OK.

Gerätestrommanager

Verwenden Sie den Gerätestrommanager, um den Status eines PowerStrip-Geräts (einschließlich Spannung, Strom und Temperatur) anzuzeigen und alle Stromausgänge des PowerStrip-Geräts zu verwalten. Der Gerätestrommanager bietet eine auf PowerStrips zentrierte Ansicht der Ausgänge.

Bevor Sie den Gerätestrommanager verwenden können, muss eine physische Verbindung zwischen einer PowerStrip- und einer Dominion SX- oder Dominion KSX-Einheit hergestellt werden. Beim Hinzufügen des PowerStrip-Geräts müssen Sie definieren, welches Raritan-Gerät die Verbindung bereitstellt. Dadurch wird es mit dem seriellen Port des SX-Geräts oder mit dem Stromversorgungsport verknüpft, der dem KSX-Gerät zugeordnet ist und der die Verwaltung des PowerStrip bereitstellt.

So zeigen Sie den Gerätestrommanager an:

1. Wählen Sie auf der Registerkarte "Geräte" ein PowerStrip-Gerät aus.
2. Wählen Sie "Geräte > Gerätestrommanager".

3. Die Ausgänge werden im Fensterbereich Status der Ausgänge aufgeführt. Möglicherweise müssen Sie nach unten blättern, um alle Ausgänge anzuzeigen.
   - Wählen Sie für jeden Ausgang die Option "Ein" oder "Aus" aus der Dropdownliste, um den Ausgang ein- oder auszuschalten.
   - Wählen Sie "Ein-/Ausschalten" aus der Dropdownliste, um das mit dem Ausgang verbundene Gerät neu zu starten.

Verwaltungsseite eines Geräts aufrufen

Falls für das ausgewählte Gerät verfügbar, bietet der Befehl "Administration starten" Zugriff auf die Verwaltungsschnittstelle des Geräts.

So rufen Sie die Verwaltungsseite eines Geräts auf:

1. Klicken Sie auf die Registerkarte "Geräte", und wählen Sie das Gerät aus, dessen Verwaltungsschnittstelle Sie anzeigen möchten.
2. Wählen Sie "Geräte > Gerätemanager > Administration starten". Die Verwaltungsschnittstelle für das ausgewählte Gerät wird angezeigt.

Benutzerverbindung trennen

Administratoren können die Gerätesitzung eines Benutzers beenden. Dazu zählen Benutzer, die beliebige Gerätevorgänge durchführen, beispielsweise Benutzer, die Verbindungen zu Ports herstellen, die Konfiguration eines Geräts sichern bzw. wiederherstellen oder die Firmware eines Geräts aktualisieren.

Firmwareaktualisierungen sowie Sicherungen und Wiederherstellungen von Gerätekonfigurationen können vor Beendigung der Gerätesitzung des Benutzers abgeschlossen werden. Alle anderen Vorgänge werden sofort beendet.

Nur bei Dominion SX-Geräten können Sie neben den Benutzern, die mit dem Gerät über CC-SG verbunden sind, auch direkt am Gerät angemeldete Benutzer trennen.

So trennen Sie eine Benutzerverbindung zu einem Gerät:

1. Klicken Sie auf die Registerkarte "Geräte", und wählen Sie das Gerät aus, dessen Benutzerverbindung Sie trennen möchten.
2. Wählen Sie "Geräte > Gerätemanager > Benutzer trennen".
3. Wählen Sie die Benutzer, deren Sitzung beendet werden soll, in der Tabelle "Benutzer trennen" aus.
4. Klicken Sie auf "Trennen", um die Benutzer vom Gerät zu trennen.

Sonderzugriff auf Paragon II-Systemgeräte

Paragon II-Systemcontroller (P2-SC)

Benutzer der Paragon II-Systemintegration können ihre P2-SC-Geräte zur CC-SG-Gerätestruktur hinzufügen und mit der P2-SC-Administrationsanwendung in CC-SG konfigurieren. Weitere Informationen zur Verwendung der P2-SC-Administration finden Sie im **P2-SC-Benutzerhandbuch** von Raritan.

Nach dem Hinzufügen des Paragon-Systemgeräts (das Paragon-System umfasst das P2-SC-Gerät, angeschlossene UMT- sowie IP-Reach-Einheiten) zu CC-SG wird es in der Gerätestruktur angezeigt.

So greifen Sie von CC-SG auf den Paragon II-Systemcontroller zu:

1. Klicken Sie auf die Registerkarte "Geräte", und wählen Sie den Paragon II-Systemcontroller aus.
2. Wählen Sie "Geräte > Gerätemanager > Administration starten", um den Paragon II-Systemcontroller in einem neuen Browserfenster zu starten. Sie können die PII UMT-Einheiten konfigurieren.

IP-Reach- und UST-IP-Verwaltung

Sie können direkt auf der CC-SG-Benutzeroberfläche administrative Diagnoseaufgaben an IP-Reach- und UST-IP-Geräten durchführen, die am Paragon-System angeschlossen sind.

Nach dem Hinzufügen eines Paragon-Systemgeräts zu CC-SG wird es in der Gerätestruktur angezeigt.

So greifen Sie auf die Remotebenutzerstation-Verwaltung zu:

1. Klicken Sie auf die Registerkarte "Geräte", und wählen Sie den Paragon II-Systemcontroller aus.
2. Wählen Sie "Geräte > Gerätemanager > Benutzerstation-Administration starten".

Kapitel 7 Verwaltete PowerStrips

Es gibt drei Möglichkeiten, die Stromversorgungssteuerung mit Powerstrips in CC-SG zu konfigurieren.

1. Alle unterstützten PowerStrips der Marke Raritan können an ein anderes Raritan-Gerät angeschlossen und als PowerStrip-Gerät zu CC-SG hinzugefügt werden. Zu PowerStrips der Marke Raritan gehören Dominion PX- und RPC-PowerStrips. Stellen Sie anhand der Kompatibilitätsmatrix fest, welche Versionen unterstützt werden. Um diese Art des verwaltetem PowerStrip in CC-SG zu konfigurieren, müssen Sie wissen, an welches Raritan-Gerät der PowerStrip physisch angeschlossen ist. Siehe ***PowerStrips konfigurieren, die von einem anderen Gerät in CC-SG verwaltet werden*** (auf Seite 113).
2. Dominion PX-PowerStrips können direkt an das IP-Netzwerk angeschlossen und CC-SG als PX-Gerät hinzugefügt werden. Wenn PX-PowerStrips direkt an das IP-Netzwerk angeschlossen sind, müssen diese nicht an ein anderes Raritan-Gerät angeschlossen werden.
3. Durch die Konfiguration einer Raritan Power IQ-Serviceschnittstelle ist die Unterstützung mehrerer Anbieter für PDUs möglich. Siehe ***Stromversorgungssteuerung von Power IQ-IT-Geräten*** (auf Seite 399).

Bei allen Methoden müssen Sie verwaltete Powerstrip-Schnittstellen zu Knoten hinzufügen, um Stromversorgungszuordnungen zwischen den Ausgängen und den Knoten zu erstellen, die sie versorgen. Siehe ***Schnittstellen für verwaltete Powerstrip-Verbindungen*** (auf Seite 154).

Besonderer Hinweis zu Dominion PX

Unabhängig von der Methode, mit der Sie ein PX-Gerät konfigurieren, müssen Sie alle Stromversorgungszuordnungen mit einer einzigen Methode konfigurieren, d. h. als PowerStrip des verwalteten Geräts oder als PX-Gerät; beides ist nicht möglich. Wenn das Dominion PX-Gerät von Power IQ verwaltet wird, können Sie entweder eine Stromversorgungs-Steuerungsschnittstelle des Typs "Power Control – Managed Power Strip" oder des Typs "Power Control – Power IQ Proxy" für einen Knoten erstellen.

Außerdem können Sie das PX-Gerät an ein Verwaltungsgerät anschließen und Stromversorgungszuordnungen konfigurieren. Zudem können Sie dasselbe PX-Gerät an das IP-Netzwerk anschließen, sodass Sie die Stromversorgungsdaten mit dem PX-Webclient anzeigen und erfassen können. Informationen dazu finden Sie im **Dominion PX-Benutzerhandbuch** von Raritan, das Sie im Support-Bereich der Raritan-Website unter "Firmware und Dokumentation" finden.

In diesem Kapitel

PowerStrips konfigurieren, die von einem anderen Gerät in CC-SG verwaltet werden 113
PowerStrips, die an KX-, KX2-, KX2-101-, KSX2- und P2SC-Geräte angeschlossen sind, konfigurieren 114
PowerStrips, die an SX 3.0- und KSX-Geräte angeschlossen sind, konfigurieren 115
PowerStrips, die an SX 3.1-Geräte angeschlossen sind, konfigurieren118
Ausgänge auf einem PowerStrip konfigurieren 119

PowerStrips konfigurieren, die von einem anderen Gerät in CC-SG verwaltet werden

In CC-SG können verwaltete PowerStrips an eines der folgenden Geräte angeschlossen sein:

- Dominion KX
- Dominion KX2
- Dominion KX2-101
- Dominion SX 3.0
- Dominion SX 3,1
- Dominion KSX
- Dominion KSX2
- Paragon II/Paragon II-Systemcontroller (P2SC)
- Power IQ – Siehe ***Stromversorgungssteuerung von Power IQ-IT-Geräten*** (auf Seite 399).

Sie müssen wissen, an welches Raritan-Gerät der verwaltete PowerStrip physisch angeschlossen ist.

Hinweis: Ein Dominion PX-PowerStrip kann auch an Ihr IP-Netzwerk, aber nicht an ein anderes Raritan-Gerät angeschlossen sein. Weitere Informationen zum Konfigurieren der Stromverwaltungssteuerung für diese PowerStrips finden Sie unter **Verwaltete PowerStrips** *(auf Seite 111).*

So konfigurieren Sie verwaltete PowerStrips in CC-SG:

1. Schließen Sie alle physischen Verbindungen zwischen dem Gerät, dem PowerStrip und den Knoten, die vom PowerStrip mit Strom versorgt werden, ab. Weitere Informationen zu den physischen Verbindungen zwischen PowerStrips, Geräten und Knoten finden Sie in den Handbüchern für den Schnellstart für RPC und Dominion PX sowie im CC-SG Implementierungshandbuch.
2. Fügen Sie das Verwaltungsgerät zu CC-SG hinzu. Der Vorgang unterscheidet sich für die unterschiedlichen Raritan-Geräte. Sehen Sie im Abschnitt für das Gerät nach, an das der PowerStrip angeschlossen ist:
   - ***PowerStrips, die an KX-, KX2-, KX2-101-, KSX2- und P2SC-Geräte angeschlossen sind, konfigurieren*** (auf Seite 114)
   - ***PowerStrips, die an SX 3.0- und KSX-Geräte angeschlossen sind, konfigurieren*** (auf Seite 115)
   - ***PowerStrips, die an SX 3.1-Geräte angeschlossen sind, konfigurieren*** (auf Seite 118).

3. Konfigurieren Sie Ausgänge. Siehe ***Ausgänge auf einem PowerStrip konfigurieren*** (auf Seite 119).
4. Weisen Sie jedem Ausgang den Knoten zu, der ihn mit Strom versorgt. Siehe ***Schnittstellen für verwaltete Powerstrip-Verbindungen*** (auf Seite 154).

PowerStrips, die an KX-, KX2-, KX2-101-, KSX2- und P2SC-Geräte angeschlossen sind, konfigurieren

CC-SG erkennt automatisch PowerStrips, die an KX-, KX2-, KX2-101-, KSX2- und P2SC-Geräte angeschlossen sind. Sie können in CC-SG die folgenden Aufgaben durchführen, um PowerStrips zu konfigurieren und zu verwalten, die an diese Geräte angeschlossen sind.

- ***PowerStrip-Gerät, das an ein KX-, KX2-, KX2-101-, KSX2- oder P2SC-Gerät angeschlossen ist, hinzufügen*** (auf Seite 114)
- ***PowerStrip eines KX-, KX2-, KX2-101-, KSX2- oder P2SC-Geräts an einen anderen Port bewegen*** (auf Seite 115)
- ***PowerStrip, der an ein KX-, KX2-, KX2-101-, KSX2- oder P2SC-Gerät angeschlossen ist, löschen*** (auf Seite 115)

PowerStrip-Gerät, das an ein KX-, KX2-, KX2-101-, KSX2- oder P2SC-Gerät angeschlossen ist, hinzufügen

Wenn Sie CC-SG ein KX-, KX2-, KX2-101-, KSX2- oder P2SC-Gerät, das an einen PowerStrip angeschlossen ist, hinzufügen, wird der PowerStrip automatisch hinzugefügt. Der PowerStrip wird auf der Registerkarte "Geräte" unter dem Gerät angezeigt, an das er angeschlossen ist.

Nächste Schritte:

1. Konfigurieren Sie Ausgänge. Siehe ***Ausgänge auf einem PowerStrip konfigurieren*** (auf Seite 119).
2. Weisen Sie jedem Ausgang den Knoten zu, der ihn mit Strom versorgt. Siehe ***Schnittstellen für verwaltete Powerstrip-Verbindungen*** (auf Seite 154).

PowerStrip eines KX-, KX2-, KX2-101-, KSX2- oder P2SC-Geräts an einen anderen Port bewegen

Wenn Sie einen PowerStrip physisch von einem KX-, KX2-, KX2-101-, KSX2- oder P2SC-Gerät oder Port zu einem anderen KX-, KX2-, KX2-101-, KSX2- oder P2SC-Gerät oder Port bewegen, erkennt CC-SG automatisch den PowerStrip und aktualisiert seine Zuordnungen auf das richtige Gerät. Sie brauchen CC-SG den PowerStrip nicht separat hinzuzufügen.

Hinweis: Wenn Sie einen PowerStrip von einem P2SC-Port physisch entfernen, diesen PowerStrip aber nicht an einen anderen Port anschließen, entfernt CC-SG den PowerStrip nicht vom alten Port. Sie müssen eine teilweise oder vollständige Datenbankzurücksetzung der UMT-Einheit, an die der PowerStrip angeschlossen ist, durchführen, um den PowerStrip von der Registerkarte Geräte zu entfernen. Siehe ***Raritan P2SC-Benutzerhandbuch****.*

PowerStrip, der an ein KX-, KX2-, KX2-101-, KSX2- oder P2SC-Gerät angeschlossen ist, löschen

Sie können einen PowerStrip, der an ein KX-, KX2-, KX2-101-, KSX2- oder P2SC-Gerät angeschlossen ist, nicht aus CC-SG löschen. Sie müssen den PowerStrip vom Gerät physisch trennen, um den PowerStrip aus CC-SG zu löschen. Nachdem Sie den PowerStrip vom Gerät physisch getrennt haben, werden der PowerStrip und alle konfigurierten Ausgänge nicht mehr auf der Registerkarte "Geräte" angezeigt.

PowerStrips, die an SX 3.0- und KSX-Geräte angeschlossen sind, konfigurieren

Sie können in CC-SG die folgenden Aufgaben durchführen, um PowerStrips zu konfigurieren und zu verwalten, die an SX 3.0- und KSX-Geräte angeschlossen sind.

Hinweis: PowerStrips müssen physisch an den Stromversorgungsport eines KSX-Geräts angeschlossen sein.

- ***PowerStrip, der an ein SX 3.0- oder KSX-Gerät angeschlossen ist, hinzufügen*** (auf Seite 116)
- ***PowerStrip, der an ein SX 3.0- oder KSX-Gerät angeschlossen ist, löschen*** (auf Seite 117)
- ***Geräte- oder Portzuordnung eines PowerStrips ändern (SX 3.0, KSX)*** (auf Seite 117)

PowerStrip, der an ein SX 3.0- oder KSX-Gerät angeschlossen ist, hinzufügen

1. Fügen Sie das SX 3.0- oder KSX-Gerät zu CC-SG hinzu. Siehe ***KVM- oder serielle Geräte hinzufügen*** (auf Seite 64).
2. Wählen Sie "Geräte > Gerätemanager > Gerät hinzufügen".
3. Klicken Sie auf die Dropdown-Liste "Gerätetyp", und wählen Sie "PowerStrip" aus.
4. Geben Sie einen Namen in das Feld "Powerstrip-Name" ein. Halten Sie Ihren Mauszeiger über das Feld, um die für den Namen zulässige Anzahl an Zeichen zu sehen. Leerstellen sind nicht zulässig.
5. Klicken Sie auf das Dropdown-Menü "Anzahl der Ausgänge", und wählen Sie die Anzahl der Ausgänge für den PowerStrip aus.
6. Klicken Sie auf das Dropdown-Menü "Verwaltungsgerät", und wählen Sie dann das SX 3.0- oder KSX-Gerät aus, das an diesen PowerStrip angeschlossen ist.
7. Klicken Sie auf das Dropdown-Menü "Verwaltungsport", und wählen Sie den Port am SX 3.0- oder KSX-Gerät aus, an den dieser PowerStrip angeschlossen ist.
8. Geben Sie eine kurze Beschreibung für diesen PowerStrip in das Feld "Beschreibung" ein. **Optional.**
9. Wählen Sie "Alle Ausgänge konfigurieren", wenn jeder Ausgang dieses PowerStrip automatisch zur Registerkarte "Geräte" hinzugefügt werden soll. Wenn Sie jetzt nicht alle Ausgänge konfigurieren, können Sie die Ausgänge später konfigurieren. Siehe ***Ausgänge auf einem PowerStrip konfigurieren*** (auf Seite 119). **Optional.**
10. Klicken Sie für jede aufgeführte Kategorie auf das Dropdown-Menü "Element", und wählen Sie das Element aus, das auf das Gerät angewendet werden soll. Wählen Sie das leere Element im Feld Element für jede Kategorie aus, die Sie nicht verwenden möchten. Siehe ***Zuordnungen, Kategorien und Elemente*** (auf Seite 49). **Optional.**
11. Wenn Sie mit der Konfiguration des PowerStrip fertig sind, klicken Sie auf "Übernehmen", um dieses Gerät hinzuzufügen und einen neuen, leeren Bildschirm "Gerät hinzufügen" anzuzeigen, in dem Sie weitere Geräte hinzufügen können. Sie können auch auf OK klicken, um diesen PowerStrip hinzuzufügen, ohne einen neuen Bildschirm "Gerät hinzufügen" zu öffnen.

Nächste Schritte:

1. Konfigurieren Sie Ausgänge. Siehe ***Ausgänge auf einem PowerStrip konfigurieren*** (auf Seite 119).

2. Weisen Sie jedem Ausgang den Knoten zu, der ihn mit Strom versorgt. Siehe ***Schnittstellen für verwaltete Powerstrip-Verbindungen*** (auf Seite 154).

PowerStrip, der an ein SX 3.0- oder KSX-Gerät angeschlossen ist, löschen

Sie können einen PowerStrip, der an ein SX 3.0-, KSX- oder P2SC-Gerät angeschlossen ist, sogar dann visuell löschen, wenn der PowerStrip noch immer physisch angeschlossen ist. Wenn Sie den PowerStrip physisch vom SX 3.0-, KSX- oder P2SC-Gerät, dem er zugeordnet ist, trennen, wird der PowerStrip auf der Registerkarte "Geräte" weiterhin unter diesem Gerät angezeigt. Sie müssen den PowerStrip löschen, um ihn aus der Anzeige zu entfernen.

1. Wählen Sie auf der Registerkarte "Geräte" den PowerStrip zum Löschen aus.
2. Wählen Sie "Geräte > Gerätemanager > Gerät löschen".
3. Klicken Sie zum Löschen des PowerStrips auf OK. Eine Meldung wird eingeblendet, wenn der PowerStrip gelöscht wurde. Das PowerStrip-Symbol wird von der Registerkarte "Geräte" entfernt.

Geräte- oder Portzuordnung eines PowerStrips ändern (SX 3.0, KSX)

Wenn ein PowerStrip physisch von einem SX 3.0- oder KSX-Gerät oder Port zu einem anderen SX 3.0- oder KSX-Gerät oder Port bewegt wird, müssen Sie in CC-SG im PowerStrip-Profil die Zuordnung ändern.

1. Wählen Sie auf der Registerkarte "Geräte" den PowerStrip aus, der verschoben wurde.
2. Klicken Sie auf das Dropdown-Menü "Verwaltungsgerät", und wählen Sie dann das SX 3.0- oder KSX-Gerät aus, das an diesen PowerStrip angeschlossen ist.
3. Klicken Sie auf das Dropdown-Menü "Verwaltungsport", und wählen Sie den Port am SX 3.0- oder KSX-Gerät aus, an den dieser PowerStrip angeschlossen ist.
4. Klicken Sie auf OK.

PowerStrips, die an SX 3.1-Geräte angeschlossen sind, konfigurieren

Sie können in CC-SG die folgenden Aufgaben durchführen, um PowerStrips zu konfigurieren und zu verwalten, die an SX 3.1-Geräte angeschlossen sind.

- ***PowerStrip, der an ein SX 3.1-Gerät angeschlossen ist, hinzufügen*** (auf Seite 118)
- ***PowerStrip eines SX 3.1-Geräts an einen anderen Port bewegen*** (auf Seite 119)
- ***PowerStrip, der an ein SX 3.1-Gerät angeschlossen ist, löschen*** (auf Seite 119)

PowerStrip, der an ein SX 3.1-Gerät angeschlossen ist, hinzufügen

Der Vorgang zum Hinzufügen eines PowerStrips, der an ein SX 3.1-Gerät angeschlossen ist, hängt davon ab, ob das SX 3.1-Gerät zu CC-SG hinzugefügt wurde.

Wenn der PowerStrip an das SX 3.1-Gerät angeschlossen ist und das Gerät noch nicht zu CC-SG hinzugefügt wurde:

1. Fügen Sie das SX 3.1-Gerät zu CC-SG hinzu. Siehe ***KVM- oder serielle Geräte hinzufügen*** (auf Seite 64).
2. CC-SG erkennt den PowerStrip und fügt ihn automatisch hinzu. Der PowerStrip wird auf der Registerkarte "Geräte" unter dem SX 3.1-Gerät angezeigt, an das er angeschlossen ist.

Wenn das SX 3.1-Gerät bereits zu CC-SG hinzugefügt wurde und der PowerStrip später an das Gerät angeschlossen wird:

1. Fügen Sie das SX 3.1-Gerät zu CC-SG hinzu. Siehe ***KVM- oder serielle Geräte hinzufügen*** (auf Seite 64).
2. Ports des SX 3.1-Geräts konfigurieren. Siehe ***Ports konfigurieren*** (auf Seite 70).
3. Wählen Sie auf der Registerkarte "Geräte" das SX 3.1-Gerät aus, an das der PowerStrip angeschlossen ist.
4. Klicken Sie auf das Pluszeichen (+) neben dem Gerätesymbol, um die Portliste einzublenden.
5. Klicken Sie mit der rechten Maustaste auf den SX 3.1-Port, an den der PowerStrip angeschlossen ist, und wählen Sie im Popup-Menü die Option "Powerstrip hinzufügen".
6. Geben Sie die Anzahl der Ausgänge ein, die der PowerStrip enthält, und klicken Sie dann auf "OK".

Nächste Schritte:

1. Konfigurieren Sie Ausgänge. Siehe ***Ausgänge auf einem PowerStrip konfigurieren*** (auf Seite 119).
2. Weisen Sie jedem Ausgang den Knoten zu, der ihn mit Strom versorgt. Siehe ***Schnittstellen für verwaltete Powerstrip-Verbindungen*** (auf Seite 154).

PowerStrip eines SX 3.1-Geräts an einen anderen Port bewegen

Wenn Sie einen PowerStrip physisch von einem SX 3.1-Gerät oder Port zu einem anderen SX 3.1-Gerät oder Port bewegen, müssen Sie den PowerStrip vom alten SX 3.1-Port löschen und den PowerStrip dem neuen SX 3.1-Port hinzufügen. Siehe ***PowerStrip, der an ein SX 3.1-Gerät angeschlossen ist, löschen*** (auf Seite 119) und ***PowerStrip, der an ein SX 3.1-Gerät angeschlossen ist, hinzufügen*** (siehe "***PowerStrip, der an ein SX 3.1-Gerät angeschlossen ist, hinzufügen***" auf Seite 118).

PowerStrip, der an ein SX 3.1-Gerät angeschlossen ist, löschen

Sie können einen PowerStrip, der an ein SX 3.1-Gerät angeschlossen ist, sogar dann visuell löschen, wenn der PowerStrip noch immer physisch angeschlossen ist. Wenn Sie den PowerStrip physisch vom SX 3.1-Gerät, dem er zugeordnet ist, trennen, wird der PowerStrip auf der Registerkarte "Geräte" weiterhin unter diesem Gerät angezeigt. Sie müssen den PowerStrip löschen, um ihn aus der Anzeige zu entfernen.

So löschen Sie einen PowerStrip, der an ein SX 3.1-Gerät angeschlossen ist:

1. Wählen Sie auf der Registerkarte "Geräte" den PowerStrip zum Löschen aus.
2. Wählen Sie "Geräte > Gerätemanager > Gerät löschen".
3. Klicken Sie zum Löschen des PowerStrips auf OK. Eine Meldung wird eingeblendet, wenn der PowerStrip gelöscht wurde. Das PowerStrip-Symbol wird von der Registerkarte "Geräte" entfernt.

Ausgänge auf einem PowerStrip konfigurieren

Bevor Sie den PowerStrip-Ausgängen Knoten zuordnen, müssen Sie die Ausgänge konfigurieren, indem Sie dem Knoten die verwaltete PowerStrip-Schnittstelle hinzufügen. Siehe ***Schnittstellen für verwaltete Powerstrip-Verbindungen*** (auf Seite 154).

So konfigurieren Sie Ausgänge im PowerStrip-Profil:

1. Klicken Sie auf der Registerkarte "Geräte" auf das Pluszeichen (+) neben dem Gerät, das an den PowerStrip angeschlossen ist.

2. Wählen Sie den PowerStrip aus, dessen Ausgänge Sie konfigurieren möchten.
3. Wählen Sie im Bildschirm "Geräteprofil: PowerStrip" die Registerkarte "Ausgänge".
4. Markieren Sie das Kontrollkästchen für jeden Ausgang, den Sie konfigurieren möchten, und klicken Sie dann auf "OK".

Die Ausgänge werden auf der Registerkarte "Geräte" unter dem PowerStrip-Symbol angezeigt.

So konfigurieren Sie Ausgänge im Bildschirm Ports konfigurieren:

1. Klicken Sie auf der Registerkarte "Geräte" auf das Pluszeichen (+) neben dem Gerät, das an den PowerStrip angeschlossen ist.
2. Wählen Sie den PowerStrip aus, dessen Ausgänge Sie konfigurieren möchten.
3. Wählen Sie "Geräte > Portmanager > Ports konfigurieren".
   - Wenn Sie mehrere Ausgänge mit den im Bildschirm angezeigten Standardnamen konfigurieren möchten, markieren Sie das Kontrollkästchen für jeden Ausgang, den Sie konfigurieren möchten. Klicken Sie dann auf OK, um jeden Ausgang mit dem Standardnamen zu konfigurieren.
   - Wenn Sie jeden Ausgang individuell konfigurieren möchten, klicken Sie neben dem Ausgang auf die Schaltfläche "Konfigurieren", und geben Sie dann den Namen für den Ausgang in das Feld "Portname" ein. Klicken Sie zum Konfigurieren des Ports auf OK.

So löschen Sie einen Ausgang:

1. Klicken Sie auf der Registerkarte "Geräte" auf das Pluszeichen (+) neben dem Gerät, das an den PowerStrip angeschlossen ist.
2. Klicken Sie auf das Pluszeichen (+) neben dem PowerStrip.
3. Wählen Sie "Geräte > Portmanager > Ports löschen".
4. Markieren Sie das Kontrollkästchen für jeden Ausgang, den Sie löschen möchten, und klicken Sie dann auf "OK", um den Ausgang zu löschen.

Kapitel 8 Knoten, Knotengruppen und Schnittstellen

In diesem Abschnitt wird beschrieben, wie Knoten und die zugewiesenen Schnittstellen angezeigt, konfiguriert und bearbeitet werden. Außerdem wird beschrieben, wie Knotengruppen erstellt werden. Der Verbindungsaufbau zu Knoten wird kurz erläutert. Weitere Informationen zum Verbindungsaufbau zu Knoten finden Sie im **CommandCenter Secure Gateway-Benutzerhandbuch** von Raritan.

In diesem Kapitel

Überblick über Knoten und Schnittstellen 122
Knoten anzeigen.....123
Dienstkonten.....126
Knoten hinzufügen, bearbeiten und löschen 130
Einsatzort und Kontakte zu einem Knotenprofil hinzufügen.....132
Hinweise zu einem Knotenprofil hinzufügen 133
Virtuelle Infrastruktur in CC-SG konfigurieren 133
Virtuelle Infrastruktur mit CC-SG synchronisieren.....145
Virtuellen Host neu starten oder Neustart erzwingen.....146
Zugriff auf die Ansicht für die virtuelle Topologie 147
Verbindung zu Knoten herstellen 147
Knoten anpingen 148
Schnittstellen hinzufügen, bearbeiten und löschen 148
Lesezeichen für Schnittstelle.....161
Direkten Portzugriff auf Knoten konfigurieren 162
Massenkopieren für Knotenzuordnungen, Einsatzort und Kontakte 162
Chat verwenden 163
Knoten per CSV-Dateiimport hinzufügen 164
Bearbeiten von IP-Adressen mit CSV-Datei-Import 178
Knotengruppen hinzufügen, bearbeiten und löschen.....179

Überblick über Knoten und Schnittstellen

Knoten

Jeder Knoten stellt ein Ziel dar, das über CC-SG entweder über In-Band- (direkte IP) oder Out-of Band-Methoden (verbunden mit einem Raritan-Gerät) verfügbar ist. Ein Knoten kann beispielsweise ein Server in einem Gestell, der mit einem Raritan KVM-Gerät über ein IP-Gerät verbunden ist; ein Server mit einer HP iLO-Karte; ein PC in einem Netzwerk mit VNC oder eine Netzwerkinfrastruktureinheit mit einer seriellen Verbindung zur Remoteverwaltung sein.

Sie können CC-SG manuell Knoten hinzufügen, nachdem Sie die Geräte hinzugefügt haben, mit denen sie verbunden sind. Knoten können auch automatisch erstellt werden. Markieren Sie dazu beim Hinzufügen von Geräten im Bildschirm "Gerät hinzufügen" das Kontrollkästchen "Alle Ports konfigurieren". Mithilfe dieser Option kann CC-SG automatisch alle Geräteports hinzufügen und einen Knoten und eine Out-of-Band KVM- oder serielle Schnittstelle für jeden Port hinzufügen. Sie können diese Knoten, Ports und Schnittstellen jederzeit bearbeiten.

Knotennamen

Knotennamen müssen eindeutig sein. CC-SG stellt Vorschläge bereit, wenn Sie manuell einen Knoten mit einem bereits vorhandenen Knotennamen hinzufügen möchten. Wenn CC-SG automatisch Knoten hinzufügt, wird über ein Nummernsystem sichergestellt, dass Knotennamen eindeutig sind.

Weitere Informationen zu den Regeln, die von CC-SG für die Länge von Namen verwendet werden, finden Sie unter ***Benennungskonventionen*** (siehe "***Benennungsregeln***" auf Seite 457).

Schnittstellen

In CC-SG sind Knoten über Schnittstellen verfügbar. Sie müssen jedem neuen Knoten mindestens eine Schnittstelle hinzufügen. Sie können verschiedene Arten von Schnittstellen hinzufügen, um verschiedene Zugriffsarten bereitzustellen. Abhängig vom Knotentyp steht Folgendes zur Verfügung: Out-of-Band-KVM oder seriell, Steuerung der Stromversorgung, In-Band SSH/RSA/VNC, DRAC/RSA/ILO, Web oder Telnet-Zugriff.

Ein Knoten kann über mehrere Schnittstellen verfügen, aber nur über eine serielle Out-of-Band- oder eine KVM-Schnittstelle. Ein Windows Server kann beispielsweise eine Out-of-Band KVM-Schnittstelle für die Tastatur-, Maus- und Monitor-Ports und eine Stromversorgungs-Schnittstelle zum Verwalten des Ausgangs aufweisen, mit dem er verbunden ist.

Einige Schnittstellen funktionieren nur im Direktmodus, obwohl Sie CC-SG für die Verwendung des Proxymodus konfiguriert haben. Zu diesen Schnittstellen gehören ILO, RSA, Microsoft RDP, DRAC, Web Browser und VMware Viewer. Java RDP-Schnittstellen können im Proxymodus verwendet werden. Siehe ***Verbindungsmodi*** (auf Seite 297).

Knoten anzeigen

In CC-SG können Sie alle Knoten auf der Registerkarte "Knoten" anzeigen und einen Knoten zur Ansicht des spezifischen Knotenprofils auswählen.

Registerkarte "Knoten"

Wenn Sie auf die Registerkarte "Knoten" klicken, werden alle Knoten, auf die Sie zugreifen können, in einer Baumstruktur angezeigt.

Knoten werden alphabetisch nach Namen angezeigt oder entsprechend ihrem Verfügbarkeitsstatus aufgeführt. Nach Status aufgeführte Knoten werden innerhalb ihrer Verfügbarkeitsgruppe alphabetisch sortiert. Klicken Sie zum Wechseln der Sortiermethode mit der rechten Maustaste auf die Strukturansicht. Klicken Sie dann auf Knotensortieroptionen, und wählen Sie Nach Knotennamen oder Nach Knotenstatus aus.

Weitere Informationen zu den verschiedenen Anzeigearten der Registerkarte "Knoten" finden Sie unter ***Benutzerdefinierte Ansichten für Geräte und Knoten*** (auf Seite 216).

Knotenprofil

Klicken Sie auf der Registerkarte "Knoten" auf einen Knoten, um die Seite "Knotenprofil" anzuzeigen. Die Seite "Knotenprofil" verfügt über Registerkarten, die Informationen über den Knoten enthalten.

Registerkarte "Schnittstellen"

Die Registerkarte "Schnittstellen" enthält alle Schnittstellen des Knotens. Auf dieser Registerkarte können Sie Schnittstellen hinzufügen, bearbeiten und löschen sowie die Standardschnittstelle auswählen. Knoten, die virtuelle Medien unterstützen, umfassen eine weitere Spalte, in der angezeigt wird, ob die virtuellen Medien aktiviert oder deaktiviert sind.

Registerkarte "Zuordnungen"

Die Registerkarte "Zuordnungen" enthält alle Kategorien und Elemente, die dem Knoten zugeordnet sind. Sie können die Zuordnungen durch eine unterschiedliche Auswahl ändern.

Siehe ***Zuordnungen, Kategorien und Elemente*** (auf Seite 49).

Registerkarte "Einsatzort & Kontakte"

Die Registerkarte "Einsatzort & Kontakte" enthält Informationen zu Einsatzort und Kontakten (z. B. Telefonnummern), die bei der Arbeit mit einem Gerät erforderlich sind. Sie können die Informationen in den Feldern durch Eingabe neuer Informationen ändern.

Siehe ***Einsatzort und Kontakte zu einem Knotenprofil hinzufügen*** (auf Seite 132).

Registerkarte "Hinweise"

Die Registerkarte "Hinweise" enthält ein Tool, mit dem Benutzer anderen Benutzern Hinweise zu einem Gerät hinterlassen können. Alle Hinweise werden mit dem Datum, dem Benutzernamen und der IP-Adresse des Benutzers angezeigt, der den Hinweis hinzugefügt hat.

Wenn Sie über die Berechtigung "Geräte-, Port- und Knotenverwaltung" verfügen, können Sie alle Knoten aus dem Knotenprofil löschen. Klicken Sie auf die Schaltfläche "Löschen".

Siehe ***Hinweise zu einem Knotenprofil hinzufügen*** (auf Seite 133).

Registerkarte "Überwachung"

Sie können den Grund für den Zugriff auf einen Knoten auf der Registerkarte "Überprüfung" anzeigen. Benutzer müssen einen Grund für den Zugriff eingeben, bevor sie eine Verbindung zu einem Knoten herstellen, wenn für die Benutzergruppe eine Knotenüberwachung aktiviert wurde.

Die Registerkarte "Überwachung" ist ausgeblendet, wenn die Funktion deaktiviert ist oder wenn kein Grund für den Zugriff eingegeben wurde.

Siehe ***Zugriffsüberwachung für Benutzergruppen konfigurieren*** (auf Seite 193).

Registerkarte "Daten des Steuerungssystems"

Serverknoten des Steuerungssystems wie das Virtual Center von VMware verfügen über die Registerkarte "Daten des Steuerungssystems". Die Registerkarte "Daten des Steuerungssystems" enthalten Informationen vom Server des Steuerungssystems, die beim Öffnen der Registerkarte aktualisiert werden. Sie können auf eine Topologieansicht der virtuellen Infrastruktur zugreifen, eine Verbindung zu den zugeordneten Knotenprofilen oder zum Steuerungssystem herstellen und die Registerkarte "Übersicht" öffnen.

Registerkarte "Daten des virtuellen Hosts"

Knoten virtueller Hosts wie die ESX-Server von VMware verfügen über die Registerkarte "Daten des virtuellen Hosts". Die Registerkarte "Daten des virtuellen Hosts" enthalten Informationen vom virtuellen Hostserver, die beim Öffnen der Registerkarte aktualisiert werden. Sie können auf eine Topologieansicht der virtuellen Infrastruktur zugreifen, eine Verbindung zu den zugeordneten Knotenprofilen oder zum virtuellen Host herstellen und die Registerkarte "Übersicht" öffnen. Wenn Sie über die Berechtigung "Geräte-, Port- und Knotenverwaltung" verfügen, können Sie den virtuellen Hostserver neu starten oder einen Neustart erzwingen.

Registerkarte "Daten des virtuellen Geräts"

Virtuelle Geräteknoten wie die Virtual Machines von VMware verfügen über die Registerkarte "Daten des virtuellen Geräts". Die Registerkarte "Daten des virtuellen Geräts" enthalten Informationen vom virtuellen Gerät, die beim Öffnen der Registerkarte aktualisiert werden. Sie können auf eine Topologieansicht der virtuellen Infrastruktur zugreifen, eine Verbindung zu den zugeordneten Knotenprofilen oder zum virtuellen Host herstellen und die Registerkarte "Übersicht" öffnen.

Registerkarte "Blades"

Blade-Chassis-Knoten, wie z. B. IBM BladeCenter, enthalten die Registerkarte "Blades". Die Registerkarte "Blades" enthält Informationen zu den Blade-Servern im Blade-Chassis.

Knoten- und Schnittstellensymbole

Knoten verfügen zur leichteren Unterscheidung über unterschiedliche Symbole in der Knotenstrukturansicht. Bewegen Sie den Mauszeiger auf ein Symbol in der Strukturansicht Knoten, um einen Tooltip mit Informationen zum Knoten anzuzeigen.

Symbol	Bedeutung
	Knoten verfügbar: der Knoten verfügt über mindestens eine verfügbare Schnittstelle.
	Knoten nicht verfügbar: der Knoten hat bis jetzt noch keine verfügbare Schnittstelle.

Dienstkonten

Überblick über Dienstkonten

Dienstkonten sind besondere Anmeldeinformationen, die Sie mehreren Schnittstellen zuweisen können. Sie können Zeit sparen, indem Sie einer Gruppe von Schnittstellen, bei denen ein häufiger Kennwortwechsel erforderlich ist, ein Dienstkonto zuweisen. Sie können die Anmeldeinformationen im Dienstkonto aktualisieren. Die Änderung wird anschließend bei jeder Schnittstelle berücksichtigt, die das Dienstkonto verwendet.

Dienstkonten können nicht für Out-of-Band-Schnittstellen oder verwaltete PowerStrip-Schnittstellen verwendet werden.

- Für DRAC-, iLO- und RSA-Schnittstellen gelten die Anmeldeinformationen für die eingebettete Prozessorkarte, nicht für das zugrunde liegende Betriebssystem.
- Für RDP-, SSH- und Telnet-Schnittstellen gelten die Anmeldeinformationen für das Betriebssystem.
- Für VNC-Schnittstellen gelten die Anmeldeinformationen für den VNC-Server.
- Für Webbrowser-Schnittstellen gelten die Anmeldeinformationen für das Formular, das unter dem in der Schnittstelle angegebenen URL verfügbar ist.

So zeigen Sie Dienstkonten an:

- Wählen Sie "Knoten > Dienstkonten". Die Seite "Dienstkonten" wird angezeigt.
- Klicken Sie auf die Spaltenüberschrift, um die Tabelle in aufsteigender Reihenfolge nach diesem Attribut zu sortieren. Klicken Sie erneut auf die Spaltenüberschrift, um die Tabelle in absteigender Reihenfolge zu sortieren. **Optional.**

FELD	Beschreibung
Dienstkontoname	Dieser Name kennzeichnet das Dienstkonto in den Dialogfeldern für die Schnittstelle und auf der Seite "Dienstkonten zuweisen".
Benutzername	Dieser Benutzername wird als Bestandteil der Anmeldeinformationen verwendet, wenn das Dienstkonto einer Schnittstelle zugewiesen wird.
Kennwort	Dieses Kennwort wird als Bestandteil der Anmeldeinformationen verwendet, wenn das Dienstkonto einer Schnittstelle zugewiesen wird.
Kennwort erneut eingeben	Mit diesem Feld wird sichergestellt, dass das Kennwort richtig eingegeben wurde.
Beschreibung	Diese Beschreibung kann zusätzliche Informationen zum Dienstkonto enthalten, die Sie hinzufügen möchten.

Dienstkonten hinzufügen, bearbeiten und löschen

So fügen Sie ein Dienstkonto hinzu:

1. Wählen Sie "Knoten > Dienstkonten". Die Seite "Dienstkonten" wird angezeigt.
2. Klicken Sie auf das Symbol zum Einfügen einer neuen Zeile , um eine neue Zeile in die Tabelle einzufügen.
3. Geben Sie einen Namen für dieses Dienstkonto im Feld "Dienstkontoname" ein.
4. Geben Sie den Benutzernamen im Feld "Benutzername" ein.
5. Geben Sie das Kennwort im Feld "Kennwort" ein.
6. Geben Sie das Kennwort noch einmal im Feld "Kennwort erneut eingeben" ein.
7. Geben Sie eine Beschreibung dieses Dienstkontos im Feld "Beschreibung" ein.
8. Klicken Sie auf OK.

So bearbeiten Sie ein Dienstkonto:

1. Wählen Sie "Knoten > Dienstkonten". Die Seite "Dienstkonten" wird angezeigt.
2. Suchen Sie das Dienstkonto, das Sie bearbeiten möchten.
3. Bearbeiten Sie die Felder. Der Dienstkontoname kann nicht bearbeitet werden.

Hinweis: CC-SG aktualisiert alle Schnittstellen, die das Dienstkonto verwenden, sodass bei einer Änderung des Benutzernamens oder des Kennworts die neuen Anmeldeinformationen verwendet werden.

4. Klicken Sie auf OK.

So löschen Sie ein Dienstkonto:

1. Wählen Sie "Knoten > Dienstkonten". Die Seite "Dienstkonten" wird angezeigt.
2. Wählen Sie das Dienstkonto aus, das gelöscht werden soll.
3. Klicken Sie auf die Schaltfläche zum Löschen von Zeilen.
4. Klicken Sie auf OK.

Kennwort für ein Dienstkonto ändern

So ändern Sie das Kennwort für ein Dienstkonto:

1. Wählen Sie "Knoten > Dienstkonten". Die Seite "Dienstkonten" wird angezeigt.
2. Suchen Sie das Dienstkonto, dessen Kennwort Sie ändern möchten.
3. Geben Sie das neue Kennwort im Feld "Kennwort" ein.
4. Geben Sie das Kennwort noch einmal im Feld "Kennwort erneut eingeben" ein.
5. Klicken Sie auf OK.

Hinweis: CC-SG aktualisiert alle Schnittstellen, die das Dienstkonto verwenden, sodass bei einer Änderung des Benutzernamens oder des Kennworts die neuen Anmeldeinformationen verwendet werden.

Schnittstellen Dienstkonten zuweisen

Sie können ein Dienstkonto mehreren Schnittstellen zuweisen. Jede Schnittstelle, die dem Dienstkonto zugewiesen wird, verwendet dieselben Anmeldeinformationen für Verbindungen.

CC-SG aktualisiert alle Schnittstellen, die das Dienstkonto verwenden, sodass bei einer Änderung des Benutzernamens oder des Kennworts die neuen Anmeldeinformationen verwendet werden.

Beim Konfigurieren einer Schnittstelle können Sie auch ein Dienstkonto auswählen. Siehe ***Schnittstellen hinzufügen, bearbeiten und löschen*** (auf Seite 148).

Sie müssen über die Berechtigung "Geräte-, Port- und Knotenverwaltung" verfügen, um Schnittstellen Dienstkonten zuweisen zu können. Siehe ***Benutzergruppen hinzufügen, bearbeiten und löschen*** (auf Seite 188).

So weisen Sie Schnittstellen ein Dienstkonto zu:

1. Wählen Sie "Knoten > Dienstkonten zuweisen". Die Seite "Dienstkonten zuweisen" wird angezeigt.
2. Wählen Sie im Feld "Dienstkontoname" das Dienstkonto aus, das Sie den Knoten zuweisen möchten.
3. Wählen Sie in der Liste "Verfügbar" die Schnittstellen aus, die Sie dem Dienstkonto zuweisen möchten. Klicken Sie bei gedrückter Strg- oder Umschalttaste, um mehrere Schnittstellen auf einmal auszuwählen.

   Tipp: Geben Sie einen Knotennamen im Feld "Knoten suchen" ein, um ihn in der Liste zu markieren. Geben Sie ein Sternchen (*) hinter einem Teilnamen ein, um alle ähnlichen Namen in der Liste zu markieren.

   Klicken Sie auf die Spaltenüberschriften, um die Listen alphabetisch zu sortieren.

4. Klicken Sie auf "Hinzufügen", um die ausgewählten Schnittstellen in die Liste "Ausgewählt" zu verschieben.
5. Klicken Sie auf OK. Das Dienstkonto wird allen Knoten in der Liste "Ausgewählt" zugewiesen.

Hinweis: CC-SG aktualisiert alle Schnittstellen, die das Dienstkonto verwenden, sodass bei einer Änderung des Benutzernamens oder des Kennworts die neuen Anmeldeinformationen verwendet werden.

Knoten hinzufügen, bearbeiten und löschen

Knoten hinzufügen

So fügen Sie CC-SG einen Knoten hinzu:

1. Klicken Sie auf die Registerkarte "Knoten".
2. Wählen Sie "Knoten > Knoten hinzufügen".
3. Geben Sie den Namen des neuen Knotens im Feld Knotenname ein. Alle Knotennamen in CC-SG müssen eindeutig sein. Weitere Informationen zu den Regeln, die von CC-SG für die Länge von Namen verwendet werden, finden Sie unter ***Benennungskonventionen*** (siehe "***Benennungsregeln***" auf Seite 457).
4. Geben Sie eine kurze Beschreibung für diesen Knoten im Feld "Beschreibung" ein. **Optional.**
5. Sie müssen mindestens eine Schnittstelle konfigurieren. Klicken Sie im Bereich "Schnittstelle" des Bildschirms "Knoten hinzufügen" auf "Hinzufügen", um eine Schnittstelle hinzuzufügen. Siehe ***Schnittstellen hinzufügen*** (auf Seite 148).
6. Sie können eine Liste mit Kategorien und Elementen konfigurieren, um diesen Knoten besser beschreiben und verwalten zu können. Siehe ***Zuordnungen, Kategorien und Elemente*** (auf Seite 49). **Optional.**
   - Klicken Sie für jede aufgeführte Kategorie auf das Dropdown-Menü Element. Wählen Sie dann das Element zum Anwenden auf den Knoten in der Liste aus.

   Hinweis: Standardmäßig verwendet CC-SG die Standardkategorienamen für "Systemtyp" und "US-Bundesstaaten und -Staatsgebiete" in Englisch.

   - Wählen Sie das leere Element im Feld Element für jede Kategorie aus, die Sie nicht verwenden möchten.
   - Wenn die Werte für "Kategorie" oder "Element", die Sie verwenden möchten, nicht angezeigt werden, können Sie diese über das Menü "Zuordnungen" hinzufügen. Siehe ***Zuordnungen, Kategorien und Elemente*** (auf Seite 49).
7. Klicken Sie zum Speichern der Änderungen auf OK. Der Knoten wird der Knotenliste hinzugefügt.

Wichtig: Wenn Sie den Dominion-Geräteport eines Blade-Chassis ändern, gehen Benutzeroberflächen, die dem Blade-Chassis-Knoten in CC-SG hinzugefügt wurden, für CC-SG verloren. Alle weiteren Informationen bleiben erhalten.

Durch das Konfigurieren von Ports erstellte Knoten

Beim Konfigurieren der Ports eines Geräts wird automatisch ein Knoten für jeden Port erstellt. Für jeden Knoten wird auch eine Schnittstelle erstellt.

Wird ein Knoten automatisch erstellt, wird ihm der gleiche Name wie dem Port gegeben, dem er zugewiesen ist. Wenn dieser Knotenname bereits vorhanden ist, wird dem Knotennamen eine Erweiterung hinzugefügt. Ein Beispiel ist Kanal1(1). Die Erweiterung ist die Zahl in Klammern. Diese Erweiterung ist bei der Zeichenanzahl des Knotennamens nicht eingeschlossen. Wenn Sie den Knotennamen bearbeiten, ist der neue Name auf die maximale Anzahl an Zeichen beschränkt. Siehe ***Benennungskonventionen*** (siehe "***Benennungsregeln***" auf Seite 457).

Knoten bearbeiten

Sie können einen Knoten bearbeiten, um den Namen, die Beschreibung, die Schnittstellen, die Standardschnittstelle oder die Zuordnungen zu ändern.

So bearbeiten Sie einen Knoten:

1. Klicken Sie auf die Registerkarte "Knoten", und wählen Sie den Knoten zum Bearbeiten aus. Das Knotenprofil wird angezeigt.
2. Bearbeiten Sie bei Bedarf die Felder.
3. Klicken Sie zum Speichern der Änderungen auf OK.

Hinweis 1: Wenn Sie den Knotennamen eines Blade-Chassis ändern, wird der Chassis-Name nicht geändert. Um den Chassis-Namen zu ändern, müssen Sie ihn im Bildschirm "Geräteprofil" bearbeiten. Siehe **Blade-Chassis-Gerät bearbeiten** *(auf Seite 79).*

Hinweis 2: Durch Änderung des Knotennamens eines virtuellen Host-Knotens oder virtuellen Steuersystemknotens wird auch der Name in der Virtualisierungstabelle geändert.

Knoten löschen

Wenn Sie einen Knoten löschen, wird dieser von der Registerkarte "Knoten" entfernt. Benutzer können nicht mehr auf den Knoten zugreifen. Wenn Sie einen Knoten löschen, werden alle Schnittstellen, Zuordnungen und zugeordneten Ports gelöscht.

So löschen Sie einen Knoten:

1. Wählen Sie auf der Registerkarte "Knoten" den Knoten zum Löschen aus.

2. Wählen Sie "Knoten > Knoten löschen". Das Fenster "Knoten löschen" wird angezeigt.
3. Klicken Sie zum Löschen des Knotens auf OK.
4. Klicken Sie auf "Ja", um zu bestätigen, dass durch das Löschen des Knotens auch alle Schnittstellen und zugewiesenen Ports gelöscht werden. Nach dem Löschvorgang wird eine Liste aller gelöschten Elemente angezeigt.

Einsatzort und Kontakte zu einem Knotenprofil hinzufügen

Geben Sie Details zum Einsatzort des Knotens sowie Kontaktinformationen für die Personen ein, die den Knoten verwalten oder verwenden.

So fügen Sie einen Einsatzort und Kontakte zu einem Knotenprofil hinzu:

1. Wählen Sie einen Knoten auf der Registerkarte "Knoten". Die Seite "Knotenprofil" wird angezeigt.
2. Klicken Sie auf die Registerkarte "Einsatzort & Kontakte".
3. Geben Sie Informationen zum Einsatzort ein.
   - Abteilung: Maximal 64 Zeichen.
   - Standort: Maximal 64 Zeichen.
   - Speicherort: Maximal 128 Zeichen.
4. Geben Sie Kontaktinformationen ein.
   - "Erster Ansprechpartner" und "Zweiter Ansprechpartner": Maximal 64 Zeichen.
   - "Telefonnummer" und "Mobilfunknummer": Maximal 32 Zeichen.
5. Klicken Sie zum Speichern der Änderungen auf OK.

Hinweise zu einem Knotenprofil hinzufügen

Sie können auf der Registerkarte "Hinweise" Hinweise zu einem Knoten für andere Benutzer hinzufügen. Alle Hinweise werden mit dem Datum, dem Benutzernamen und der IP-Adresse des Benutzers angezeigt, der den Hinweis hinzugefügt hat.

Wenn Sie über die Berechtigung "Geräte-, Port- und Knotenverwaltung" verfügen, können Sie alle auf der Registerkarte "Hinweise" angezeigten Hinweise löschen.

So fügen Sie Hinweise zum Knotenprofil hinzu:

1. Wählen Sie einen Knoten auf der Registerkarte "Knoten". Die Seite "Knotenprofil" wird angezeigt.
2. Klicken Sie auf die Registerkarte "Hinweise".
3. Geben Sie den Hinweis im Feld "Neuer Hinweis" ein.
4. Klicken Sie auf "Hinzufügen". Ihr Hinweis wird in der Liste "Hinweise" angezeigt.

So löschen Sie alle Knoten:

1. Klicken Sie auf die Registerkarte "Hinweise".
2. Klicken Sie auf "Hinweise löschen".
3. Klicken Sie zum Bestätigen auf "Ja". Alle Hinweise werden aus der Registerkarte "Hinweise" gelöscht.

Virtuelle Infrastruktur in CC-SG konfigurieren

Terminologie zur virtuellen Infrastruktur

CC-SG verwendet die folgende Terminologie für Komponenten der virtuellen Infrastruktur.

Begriff	Definition	Beispiel
Steuerungssystem	Das Steuerungssystem ist der Verwaltungsserver. Das Steuerungssystem verwaltet mindestens einen virtuellen Host.	Virtual Center von VMware
Virtueller Host	Der virtuelle Host ist die physische Hardware, die mindestens ein virtuelles Gerät enthält.	ESX von VMware
Virtuelles Gerät	Ein virtuelles Gerät ist ein virtueller "Server" auf einem virtuellen Host. Ein virtuelles Gerät kann von einem virtuellen Host auf einen anderen virtuellen Host verschoben werden.	Virtual Machine oder VM von VMware

Begriff	Definition	Beispiel
VI-Client-Schnittstelle	Knoten des Steuerungssystems und Knoten virtueller Hosts haben eine VI-Client-Schnittstelle, die Zugriff auf die Infrastruktur-Clientanwendung des Virtualisierungssystems bereitstellt.	Virtual Infrastructure Web Access von VMware
VMW-Viewer-Schnittstelle	Virtuelle Geräteknoten haben eine VMW-Viewer-Schnittstelle, die Zugriff auf die Viewer-Anwendung des virtuellen Geräts bereitstellt.	Virtual Machine Remote Console von VMware
VMW-Stromversorgungs-Schnittstelle	Virtuelle Geräteknoten haben eine VMW-Stromversorgungs-Schnittstelle, die eine Stromversorgungssteuerung für den Knoten über CC-SG bereitstellt.	Nicht zutreffend

Überblick über virtuelle Knoten

Sie können Ihre virtuelle Infrastruktur für den Zugriff in CC-SG konfigurieren. Die Seite "Virtualisierung" bietet zwei Assistenten, den Assistenten "Steuerungssystem hinzufügen" und den Assistenten "Virtuellen Host hinzufügen", mit denen Sie Steuerungssysteme, virtuelle Hosts und ihre virtuellen Geräte ordnungsgemäß hinzufügen können.

Nachdem Sie die Konfiguration beendet haben, kann in CC-SG auf alle Steuerungssysteme, virtuellen Hosts und virtuellen Geräte als Knoten zugegriffen werden. Jeder Typ eines virtuellen Knotens wird mit einer Schnittstellen für den Zugriff und einer Schnittstelle für die Stromversorgung konfiguriert.

- Die Knoten des Steuerungssystems und die Knoten des virtuellen Hosts werden mit einer VI-Client-Schnittstelle konfiguriert. Die VI-Client-Schnittstelle stellt Zugriff auf den Infrastruktur-Client des Virtualisierungssystems bereit. Bei VMware-Kontrollzentren bietet die VI-Client-Schnittstelle über VMware Virtual Infrastructure Web Access Zugriff auf den Server des Kontrollzentrums. Bei VMware ESX-Servern bietet die VI-Client-Schnittstelle über VMware Virtual Infrastructure Web Access Zugriff auf den ESX-Server.
- Virtuelle Geräteknoten werden mit einer VMW-Viewer-Schnittstelle und einer VMW-Stromversorgungs-Schnittstelle konfiguriert. Die VMW-Viewer-Schnittstelle bietet Zugriff auf die Viewer-Anwendung des virtuellen Geräts. Bei virtuellen Geräten von VMware bietet die VMW-Viewer-Schnittstelle Zugriff auf die Remotekonsole des virtuellen Geräts. Die VMW-Stromversorgungs-Schnittstelle stellt über CC-SG eine Stromversorgungssteuerung für den Knoten bereit.
- Ab CC-SG 5.0 ist das Menü "Geräte" der VMWare-Remotekonsole für vSphere 4.0-Knoten zugänglich, auf die über CC-SG zugegriffen wird. So werden Verbindungen zwischen Geräten und Abbildern und dem virtuellen Knoten ermöglicht.
- CC-SG kann keine virtuellen ESXi-Knoten verwalten, die eine Lizenz für eine kostenlose Testversion des VMware-Produkts verwenden. Ein Zugriff auf solche Knoten ist ebenfalls nicht möglich.

Steuerungssystem mit virtuellen Hosts und virtuellen Geräten hinzufügen

Beim Hinzufügen eines Steuerungssystems werden Sie von einem Assistenten durch das Hinzufügen der virtuellen Hosts und der virtuellen Geräte geführt, die im Steuerungssystem enthalten sind.

So fügen Sie ein Steuerungssystem mit virtuellen Hosts und virtuellen Geräten hinzu:

1. Wählen Sie "Knoten > Virtualisierung".
2. Klicken Sie auf "Steuerungssystem hinzufügen".

3. IP-Adresse/Hostname: Geben Sie die IP-Adresse bzw. den Hostnamen des Steuerungssystems ein. Maximal 64 Zeichen.
4. Verbindungsprotokoll: Geben Sie HTTP oder HTTPS als Übertragungsprotokoll zwischen dem Steuerungssystem und CC-SG an.
5. TCP-Port: Geben Sie den TCP-Port ein. Der Standardport lautet 443.
6. Überprüfungsintervall (Sekunden): Geben Sie die Zeit in Sekunden ein, die vergehen soll, bevor ein Zeitüberschreitungsfehler zwischen dem Steuerungssystem und CC-SG auftritt.
7. Geben Sie Authentifizierungsinformationen ein:
   - Um ein Dienstkonto zur Authentifizierung zu verwenden, markieren Sie das Kontrollkästchen "Dienstkontoinformationen verwenden". Wählen Sie das gewünschte Dienstkonto im Menü "Dienstkontoname".

     Oder
   - Geben Sie einen Benutzernamen und ein Kennwort für die Authentifizierung ein. Für jede Angabe maximal 64 Zeichen.
8. Damit sich Benutzer, die auf dieses Steuerungssystem zugreifen, automatisch an der VI-Client-Schnittstelle anmelden können, markieren Sie das Kontrollkästchen "Einzelanmeldung für VI-Client aktivieren". **Optional.**
9. Klicken Sie auf "Weiter". CC-SG erkennt die virtuellen Hosts und die virtuellen Geräte des Steuerungssystems.
   - Klicken Sie auf die Spaltenüberschrift, um die Tabelle in aufsteigender Reihenfolge nach diesem Attribut zu sortieren. Klicken Sie erneut auf die Spaltenüberschrift, um die Tabelle in absteigender Reihenfolge zu sortieren. **Optional.**
10. Fügen Sie CC-SG neue virtuelle Geräte hinzu. Für jedes virtuelle Gerät wird ein Knoten erstellt. Jeder zugehörige virtuelle Host wird ebenfalls konfiguriert. Es wird nur ein Knoten für den virtuellen Host hinzugefügt, selbst wenn der virtuelle Host mehreren virtuellen Geräten zugewiesen ist.
    - So fügen Sie ein virtuelles Gerät hinzu:
      - Markieren Sie das Kontrollkästchen "Konfigurieren" neben dem virtuellen Gerät, das Sie hinzufügen möchten.
      - Um dem Knoten für den virtuellen Host und dem virtuellen Geräteknoten eine VNC-, RDP- oder SSH-Schnittstelle hinzuzufügen, markieren Sie die Kontrollkästchen neben dem virtuellen Gerät. **Optional.**
    - So fügen Sie alle virtuellen Geräte hinzu:

- Markieren Sie das oberste Kontrollkästchen in der Spalte "Konfigurieren", um alle virtuellen Geräte auszuwählen.
- Um allen Knoten für den virtuellen Host und allen virtuellen Geräteknoten eine VNC-, RDP- oder SSH-Schnittstelle hinzuzufügen, markieren Sie die obersten Kontrollkästchen in den Spalten "VNC", "RDP" oder "SSH". **Optional.**

- So fügen Sie mehrere virtuelle Geräte hinzu:
  - Klicken Sie bei gedrückter Strg- oder Umschalttaste, um mehrere virtuelle Geräte auszuwählen, die Sie hinzufügen möchten.
  - Markieren Sie im Bereich "Zeilen markieren bzw. Markierung aufheben" das Kontrollkästchen "Virtuelles Gerät".
  - Um den Knoten des virtuellen Hosts und den Knoten des virtuellen Geräts, die erstellt werden, eine VNC-, RDP- oder SSH-Schnittstelle hinzuzufügen, markieren Sie im Bereich "Zeilen markieren bzw. Markierung aufheben" die Kontrollkästchen "VNC", "RDP" oder "SSH". **Optional.**
  - Klicken Sie auf "Markieren".

11. Klicken Sie auf "Weiter". CC-SG zeigt eine Liste der Schnittstellentypen an, die hinzugefügt werden. Sie können für jeden Typ Namen und Anmeldeinformationen hinzufügen.
12. Geben Sie für jeden Schnittstellentyp einen Namen und Anmeldeinformationen ein. Der Name und die Anmeldeinformationen werden von allen Schnittstellen verwendet, die jedem konfigurierten virtuellen Geräteknoten und jedem konfigurierten Knoten des virtuellen Hosts hinzugefügt wurden. **Optional.**

Lassen Sie diese Felder leer, wenn Sie jeder Schnittstelle einzeln Namen und Anmeldeinformationen hinzufügen möchten.

Die Schnittstelle übernimmt den Namen des Knotens, wenn das Feld leer gelassen wird.

---

a. Geben Sie Namen für Schnittstellen ein. Maximal 32 Zeichen.
   - VI-Client-Schnittstellen für virtuellen Host
   - VMware-Viewer-Schnittstellen
   - Virtuelle Stromversorgungs-Schnittstellen
   - RDP-, VNC- und SSH-Schnittstellen, sofern angegeben

b. Geben Sie bei Bedarf Anmeldeinformationen ein. Bei manchen Schnittstellentypen sind keine Anmeldeinformationen erforderlich.

- Um ein Dienstkonto zu verwenden, markieren Sie das Kontrollkästchen "Dienstkontoinformationen verwenden", und wählen Sie den Namen des Dienstkontos.

Oder

- Geben Sie einen Benutzernamen und ein Kennwort für den Schnittstellentyp ein. Für jede Angabe maximal 64 Zeichen.

13. Klicken Sie auf OK.

CC-SG erstellt Folgendes:

- Einen Knoten für jedes virtuelle Gerät. Jeder virtuelle Geräteknoten hat eine VMW-Viewer-Schnittstelle, eine VMW-Stromversorgungs-Schnittstelle sowie weitere von Ihnen angegebene In-Band-Schnittstellen. Virtuelle Hostsysteme weisen virtuellen Geräteknoten den Namen ihres virtuellen Geräts zu.
- Einen Knoten für jeden virtuellen Host. Jeder Knoten für einen virtuellen Host verfügt über eine VI-Client-Schnittstelle. Knoten für virtuelle Hosts wird ihre IP-Adresse oder ihr Hostname als Name zugewiesen.
- Einen Knoten für das Steuerungssystem. Der Knoten des Steuerungssystems verfügt über eine VI-Client-Schnittstelle. Knoten für Steuerungssysteme wird der Name "Virtual Center" plus IP-Adresse zugewiesen (z. B. "Virtual Center 192.168.10.10.").

Virtuellen Host mit virtuellen Geräten hinzufügen

Beim Hinzufügen eines virtuellen Hosts werden Sie beim Hinzufügen der virtuellen Geräte, die im virtuellen Host enthalten sind, von einem Assistenten unterstützt.

So fügen Sie einen virtuellen Host mit virtuellen Geräten hinzu:

1. Wählen Sie "Knoten > Virtualisierung".
2. Klicken Sie auf "Virtuellen Host hinzufügen".
3. Wählen Sie "Knoten > Virtualisierung".
4. Klicken Sie auf "Virtuellen Host hinzufügen".
5. IP-Adresse/Hostname: Geben Sie die IP-Adresse bzw. den Hostnamen des virtuellen Hosts ein. Maximal 64 Zeichen.
6. Verbindungsprotokoll: Geben Sie HTTP oder HTTPS als Übertragungsprotokoll zwischen dem virtuellen Host und CC-SG an.
7. TCP-Port: Geben Sie den TCP-Port ein. Der Standardport lautet 443.

8. Überprüfungsintervall (Sekunden): Geben Sie die Zeit in Sekunden ein, die vergehen soll, bevor ein Zeitüberschreitungsfehler zwischen dem virtuellen Host und CC-SG auftritt.
9. Geben Sie Authentifizierungsinformationen ein:
   - Um ein Dienstkonto zur Authentifizierung zu verwenden, markieren Sie das Kontrollkästchen "Dienstkontoinformationen verwenden". Wählen Sie das gewünschte Dienstkonto im Menü "Dienstkontoname".

     Oder
   - Geben Sie einen Benutzernamen und ein Kennwort für die Authentifizierung ein. Für jede Angabe maximal 64 Zeichen.
10. Damit sich Benutzer, die auf diesen virtuellen Host zugreifen, automatisch an der VI-Client-Schnittstelle anmelden können, markieren Sie das Kontrollkästchen "Einzelanmeldung für VI-Client aktivieren". **Optional.**
11. Klicken Sie auf "Weiter". CC-SG erkennt die virtuellen Geräte des virtuellen Hosts.
    - Klicken Sie auf die Spaltenüberschrift, um die Tabelle in aufsteigender Reihenfolge nach diesem Attribut zu sortieren. Klicken Sie erneut auf die Spaltenüberschrift, um die Tabelle in absteigender Reihenfolge zu sortieren. **Optional.**
12. Fügen Sie CC-SG neue virtuelle Geräte hinzu. Für jedes virtuelle Gerät wird ein Knoten erstellt. Jeder zugehörige virtuelle Host wird ebenfalls konfiguriert. Es wird nur ein Knoten für den virtuellen Host hinzugefügt, selbst wenn der virtuelle Host mehreren virtuellen Geräten zugewiesen ist.
    - So fügen Sie ein virtuelles Gerät hinzu:
      - Markieren Sie das Kontrollkästchen "Konfigurieren" neben dem virtuellen Gerät, das Sie hinzufügen möchten.
      - Um dem Knoten für den virtuellen Host und dem virtuellen Geräteknoten eine VNC-, RDP- oder SSH-Schnittstelle hinzuzufügen, markieren Sie die Kontrollkästchen neben dem virtuellen Gerät. **Optional.**
    - So fügen Sie alle virtuellen Geräte hinzu:
      - Markieren Sie das oberste Kontrollkästchen in der Spalte "Konfigurieren", um alle virtuellen Geräte auszuwählen.
      - Um allen Knoten für den virtuellen Host und allen virtuellen Geräteknoten eine VNC-, RDP- oder SSH-Schnittstelle hinzuzufügen, markieren Sie die obersten Kontrollkästchen in den Spalten "VNC", "RDP" oder "SSH". **Optional.**
    - So fügen Sie mehrere virtuelle Geräte hinzu:

- Klicken Sie bei gedrückter Strg- oder Umschalttaste, um mehrere virtuelle Geräte auszuwählen, die Sie hinzufügen möchten.
- Markieren Sie im Bereich "Zeilen markieren bzw. Markierung aufheben" das Kontrollkästchen "Virtuelles Gerät".
- Um den Knoten des virtuellen Hosts und den Knoten des virtuellen Geräts, die erstellt werden, eine VNC-, RDP- oder SSH-Schnittstelle hinzuzufügen, markieren Sie im Bereich "Zeilen markieren bzw. Markierung aufheben" die Kontrollkästchen "VNC", "RDP" oder "SSH". **Optional.**
- Klicken Sie auf "Markieren".

13. Klicken Sie auf "Weiter". CC-SG zeigt eine Liste der Schnittstellentypen an, die hinzugefügt werden. Sie können für jeden Typ Namen und Anmeldeinformationen hinzufügen.
14. Geben Sie für jeden Schnittstellentyp einen Namen und Anmeldeinformationen ein. Der Name und die Anmeldeinformationen werden von allen Schnittstellen verwendet, die jedem konfigurierten virtuellen Geräteknoten und jedem konfigurierten Knoten des virtuellen Hosts hinzugefügt wurden. **Optional.**

Lassen Sie diese Felder leer, wenn Sie jeder Schnittstelle einzeln Namen und Anmeldeinformationen hinzufügen möchten.

Die Schnittstelle übernimmt den Namen des Knotens, wenn das Feld leer gelassen wird.

---

a. Geben Sie Namen für Schnittstellen ein. Maximal 32 Zeichen.
   - VI-Client-Schnittstellen
   - VMware-Viewer-Schnittstellen
   - Virtuelle Stromversorgungs-Schnittstellen
   - RDP-, VNC- und SSH-Schnittstellen, sofern angegeben

b. Geben Sie bei Bedarf Anmeldeinformationen ein. Bei manchen Schnittstellentypen sind keine Anmeldeinformationen erforderlich.
   - Um ein Dienstkonto zu verwenden, markieren Sie das Kontrollkästchen "Dienstkontoinformationen verwenden", und wählen Sie den Namen des Dienstkontos.

   Oder

   - Geben Sie einen Benutzernamen und ein Kennwort für den Schnittstellentyp ein. Für jede Angabe maximal 64 Zeichen.

15. Klicken Sie auf OK.

CC-SG erstellt Folgendes:

- Einen Knoten für jedes virtuelle Gerät. Jeder virtuelle Geräteknoten hat eine VMW-Viewer-Schnittstelle, eine VMW-Stromversorgungs-Schnittstelle sowie weitere von Ihnen angegebene In-Band-Schnittstellen. Virtuelle Hostsysteme weisen virtuellen Geräteknoten den Namen ihres virtuellen Geräts zu.
- Einen Knoten für jeden virtuellen Host. Jeder Knoten für einen virtuellen Host verfügt über eine VI-Client-Schnittstelle. Knoten für virtuelle Hosts wird ihre IP-Adresse oder ihr Hostname als Name zugewiesen.

Steuerungssysteme, virtuelle Hosts und virtuelle Geräte bearbeiten

Sie können die Eigenschaften von in CC-SG konfigurierten Steuerungssystemen, virtuellen Hosts und virtuellen Geräten ändern. Sie können virtuelle Geräteknoten aus CC-SG löschen, indem Sie das Kontrollkästchen "Konfigurieren" für das virtuelle Gerät deaktivieren.

Hinweis: Um den Knotennamen eines virtuellen Host-Knotens oder Steuersystemknotens zu ändern, bearbeiten die den Knoten. Siehe **Knoten bearbeiten** *(auf Seite 131). Die Namensänderung wird auch in der Virtualisierungstabelle angezeigt.*

So bearbeiten Sie Steuerungssysteme, virtuelle Hosts und virtuelle Geräte:

1. Wählen Sie "Knoten > Virtualisierung".
2. Klicken Sie auf die Spaltenüberschrift, um die Tabelle in aufsteigender Reihenfolge nach diesem Attribut zu sortieren. Klicken Sie erneut auf die Spaltenüberschrift, um die Tabelle in absteigender Reihenfolge zu sortieren. **Optional.**
3. Wählen Sie das Steuerungssystem oder den virtuellen Host, das bzw. den Sie bearbeiten möchten.
4. Klicken Sie auf "Bearbeiten".
5. Ändern Sie die Informationen nach Bedarf. Eine ausführliche Beschreibung der Felder finden Sie unter ***Steuerungssystem mit virtuellen Hosts und virtuellen Geräten hinzufügen*** (auf Seite 135) und ***Virtuellen Host mit virtuellen Geräten hinzufügen*** (auf Seite 138).
6. Klicken Sie auf "Weiter".
7. Löschen Sie mindestens ein virtuelles Gerät aus CC-SG.
   - Um ein virtuelles Gerät zu löschen, deaktivieren Sie das Kontrollkästchen "Konfigurieren".

- Um mehrere virtuelle Geräte zu löschen, klicken Sie bei gedrückter Strg- oder Umschalttaste, um mehrere virtuelle Geräte auszuwählen. Markieren Sie anschließend das Kontrollkästchen "Virtuelles Gerät" im Bereich "Zeilen markieren bzw. Markierung aufheben", und klicken Sie auf "Markierung aufheben".

8. Um dem Knoten für den virtuellen Host und dem virtuellen Geräteknoten VNC-, RDP- oder SSH-Schnittstellen hinzuzufügen, markieren Sie die Kontrollkästchen neben jedem virtuellen Gerät.

   Auf dieser Seite können Sie keine SSH-, VNC- und RDP-Schnittstellen aus Knoten virtueller Geräte oder aus Knoten virtueller Hosts entfernen. Sie müssen die Schnittstelle aus dem Knotenprofil löschen. Siehe **Schnittstellen löschen** *(auf Seite 160).*

9. Klicken Sie auf "Weiter". Wenn Sie virtuelle Geräte löschen, wird eine Warnung angezeigt.
10. Geben Sie für jeden Schnittstellentyp einen Namen und Anmeldeinformationen ein. Der Name und die Anmeldeinformationen werden von allen Schnittstellen verwendet, die jedem konfigurierten virtuellen Geräteknoten und jedem konfigurierten Knoten des virtuellen Hosts hinzugefügt wurden. **Optional.** Sie können diese Felder leer lassen, wenn Sie jeder Schnittstelle einzeln Namen und Anmeldeinformationen hinzufügen möchten.
    a. Geben Sie Namen für Schnittstellen ein (maximal 32 Zeichen).
       - VI-Client-Schnittstellen für virtuellen Host
       - VMware-Viewer-Schnittstellen
       - Virtuelle Stromversorgungs-Schnittstellen
       - RDP-, VNC- und SSH-Schnittstellen, sofern angegeben
    b. Geben Sie Anmeldeinformationen ein:
       - Um ein Dienstkonto zu verwenden, markieren Sie das Kontrollkästchen "Dienstkontoinformationen verwenden", und wählen Sie den Namen des Dienstkontos.

       Oder

       - Geben Sie einen Benutzernamen und ein Kennwort für den Schnittstellentyp ein. Für jede Angabe maximal 64 Zeichen.
11. Klicken Sie auf OK.

Steuerungssysteme und virtuelle Hosts löschen

Sie können Steuerungssysteme und virtuelle Hosts aus CC-SG löschen.

Wenn Sie ein Steuerungssystem löschen, werden die damit verknüpften virtuellen Hosts und virtuellen Geräte nicht gelöscht.

Wenn Sie einen virtuellen Host löschen, werden die damit verknüpften Steuerungssysteme und virtuellen Geräte nicht gelöscht.

Virtuelle Geräteknoten werden nicht automatisch gelöscht, wenn ihre verknüpften Steuerungssysteme oder virtuellen Hosts gelöscht werden. Siehe ***Virtuellen Geräteknoten löschen*** (auf Seite 143).

So löschen Sie Steuerungssysteme und virtuelle Hosts:

1. Wählen Sie "Knoten > Virtualisierung".
2. Wählen Sie die zu löschenden Steuerungssysteme und virtuellen Hosts aus der Liste aus. Klicken Sie bei gedrückter Strg-Taste, um mehrere Elemente auszuwählen.
3. Klicken Sie auf "Löschen".

Virtuellen Geräteknoten löschen

Virtuelle Geräteknoten können auf zwei Arten gelöscht werden:

- Verwenden Sie die Funktion "Knoten löschen". Siehe ***Knoten löschen*** (auf Seite 131).
- Deaktivieren Sie das Kontrollkästchen "Konfigurieren" für das virtuelle Gerät. Siehe ***Steuerungssysteme, virtuelle Hosts und virtuelle Geräte bearbeiten*** (auf Seite 141).

Virtuelle Infrastruktur löschen

Führen Sie die folgenden Schritte aus, um eine ganze virtuelle Infrastruktur aus CC-SG zu löschen, einschließlich Steuerungssystem, virtuelle Hosts und virtuelle Geräte.

So löschen Sie eine virtuelle Infrastruktur:

1. Löschen Sie alle virtuellen Geräteknoten, indem Sie das Kontrollkästchen "Konfigurieren" für jedes virtuelle Gerät deaktivieren. Siehe ***Steuerungssysteme, virtuelle Hosts und virtuelle Geräte bearbeiten*** (auf Seite 141).
2. Löschen Sie das Steuerungssystem und die virtuellen Hosts. Siehe ***Steuerungssysteme und virtuelle Hosts löschen*** (auf Seite 143)

   Alle Komponenten der virtuellen Infrastruktur werden gelöscht, einschließlich der Knoten des Steuerungssystems, der Knoten der virtuellen Hosts, der virtuellen Geräteknoten sowie deren Schnittstellen.

vSphere 4-Benutzer müssen ein neues Plug-In installieren

Wenn Sie Ihre virtuelle Umgebung von einer früheren Version auf vSphere 4 aktualisieren, müssen Sie das Plug-In VMware Remote Console aus dem Browser entfernen. Nach dem Entfernen des Plug-Ins wird das korrekte Plug-In für vSphere 4 installiert, wenn Sie das nächste Mal aus CCSG eine Verbindung zu einem virtuellen Gerät herstellen.

So entfernen Sie das alte Plug-In im Internet Explorer:

1. Wählen Sie "Extras > Add-Ons verwalten > Add-Ons aktivieren bzw. deaktivieren".
2. Wählen Sie "Von Internet Explorer verwendete Add-Ons" in der Liste "Anzeigen".
3. Blättern Sie bis zum "VMware Remote Console Plug-In", und wählen Sie es aus.
4. Die Schaltfläche "ActiveX löschen" sollte aktiv werden. Klicken Sie zum Löschen des alten Plug-Ins auf die Schaltfläche.
   - Wenn die Schaltfläche "Löschen" nicht aktiv ist, wählen Sie "Systemsteuerung > Programme hinzufügen/entfernen" und suchen Sie nach einem älteren VI-Client. Wenn VI-Client 2.5 installiert ist, deinstallieren Sie diesen. Nach der Deinstallation von VI-Client 2.5 wird das Plug-In entfernt.

So entfernen Sie das alte Plug-In in Firefox:

1. Wählen Sie "Extras > Add-Ons".
2. Klicken Sie auf die Registerkarte "Plugins".
3. Wählen Sie das alte Plug-In aus, und klicken Sie auf "Deaktivieren".

So installieren Sie das neue Plug-In:

1. Melden Sie sich nach dem Entfernen des alten Plug-Ins bei CCSG an, und stellen Sie eine Verbindung zu einem virtuellen Gerät her.
2. Sie werden aufgefordert, das Plug-In für vSphere 4 zu installieren.

Virtuelle Infrastruktur mit CC-SG synchronisieren

Eine Synchronisierung stellt sicher, dass CC-SG über die neuesten Informationen zu Ihrer virtuellen Infrastruktur besitzt. Bei der Synchronisierung werden die Informationen zu jedem virtuellen Geräteknoten sowie die Topologieinformationen zur virtuellen Infrastruktur aktualisiert.

Sie können eine automatische tägliche Synchronisierung aller konfigurierten Steuerungssysteme und virtuellen Hosts konfigurieren. Sie können jederzeit auch bestimmte Steuerungssysteme und virtuelle Hosts synchronisieren.

Virtuelle Infrastruktur synchronisieren

Sie können CC-SG mit Ihrer virtuellen Infrastruktur synchronisieren.

Wenn Sie ein Steuerungssystem zur Synchronisierung auswählen, werden die zugehörigen virtuellen Hosts ebenfalls synchronisiert, unabhängig davon, ob Sie die virtuellen Hosts ausgewählt haben.

So synchronisieren Sie die virtuelle Infrastruktur:

1. Wählen Sie "Knoten > Virtualisierung".
2. Wählen Sie in der Liste mit Knoten die Knoten aus, die synchronisiert werden sollen. Klicken Sie bei gedrückter Strg-Taste, um mehrere Elemente auszuwählen.
3. Klicken Sie auf "Synchronisieren". Falls die virtuelle Infrastruktur seit der letzten Synchronisierung geändert wurde, werden die Informationen in CC-SG aktualisiert.
   - Die Spalte "Konfiguriert in Secure Gateway" zeigt die Anzahl der virtuellen Geräte oder Hosts, die in CC-SG konfiguriert sind.
   - Das Datum der letzten Synchronisierung zeigt das Datum und die Uhrzeit der Synchronisierung.
   - Die Spalte "Knotenstatus" zeigt den Status des virtuellen Knotens.

Tägliche Synchronisierung der virtuellen Infrastruktur aktivieren oder deaktivieren

Sie können eine automatische Synchronisierung von CC-SG mit Ihrer virtuellen Infrastruktur konfigurieren. Die automatische Synchronisierung findet täglich zur angegebenen Zeit statt.

So aktivieren Sie die tägliche Synchronisierung der virtuellen Infrastruktur:

1. Wählen Sie "Knoten > Virtualisierung".

2. Markieren Sie das Kontrollkästchen "Tägliche automatische Synchronisierung aktivieren".
3. Geben Sie die Uhrzeit, zu der die tägliche Synchronisierung stattfinden soll, im Feld "Startzeit" ein.
4. Klicken Sie auf "Aktualisieren".

So deaktivieren Sie die tägliche Synchronisierung der virtuellen Infrastruktur:

1. Wählen Sie "Knoten > Virtualisierung".
2. Deaktivieren Sie das Kontrollkästchen "Tägliche automatische Synchronisierung aktivieren".
3. Klicken Sie auf "Aktualisieren".

Virtuellen Host neu starten oder Neustart erzwingen

Sie können den virtuellen Hostserver neu starten oder den Neustart des virtuellen Hostservers erzwingen. Bei einem Neustart wird ein normaler Neustart des virtuellen Hostservers durchgeführt, wenn er sich im Wartungsmodus befindet. Bei einem erzwungenen Neustart wird der virtuelle Hostserver zu einem Neustart gezwungen, selbst wenn sich der Server nicht im Wartungsmodus befindet.

Um auf diese Befehle zugreifen zu können, benötigen Sie die Berechtigung "In-Band-Zugriff für Knoten" und "Stromversorgungssteuerung für Knoten". Sie müssen außerdem zu einer Benutzergruppe gehören, der eine Richtlinie für den Zugriff auf den Knoten zugewiesen wurde, der neu gestartet oder für den ein Neustart erzwungen werden soll.

So starten Sie den Knoten eines virtuellen Hosts neu oder erzwingen einen Neustart:

1. Wählen Sie den Knoten des virtuellen Hosts aus, den Sie neu starten oder für den Sie einen Neustart erzwingen möchten.
2. Klicken Sie auf die Registerkarte "Daten des virtuellen Hosts".
3. Klicken Sie auf "Neustart" oder "Erzwungener Neustart".

Zugriff auf die Ansicht für die virtuelle Topologie

Die Topologieansicht ist eine Baumstruktur, die die Beziehung zwischen dem Steuerungssystem, virtuellen Hosts und virtuellen Geräten zeigt, die mit dem ausgewählten Knoten verknüpft sind.

Zum Öffnen der Topologieansicht benötigen Sie die Berechtigung "Geräte-, Port- und Knotenverwaltung".

Öffnen Sie die Topologieansicht über das Profil des virtuellen Knotens:

1. Klicken Sie im Knotenprofil auf die Registerkarte, die Virtualisierungsinformationen über den Knoten enthält: Je nach Knotentyp ist das die Registerkarte "Daten des virtuellen Geräts", die Registerkarte "Daten des virtuellen Hosts" oder die Registerkarte "Steuerungssystem".
2. Klicken Sie auf den Link "Topologieansicht". Die Topologieansicht wird in einem neuen Fenster geöffnet. Virtuelle Knoten, die in CC-SG konfiguriert sind, wenden als Links angezeigt.
   - Doppelklicken Sie auf den Link eines Knotens, um das Knotenprofil für den virtuellen Knoten zu öffnen.
   - Doppelklicken Sie auf einen Schnittstellenlink, um eine Verbindung zum Knoten herzustellen.
   - Doppelklicken Sie auf den Link für eine virtuelle Stromversorgungs-Schnittstelle, um die Seite "Stromversorgungssteuerung" für den Knoten zu öffnen.

Verbindung zu Knoten herstellen

Nachdem ein Knoten mit einer Schnittstelle verknüpft ist, haben Sie verschiedene Möglichkeiten, eine Verbindung zu diesem Knoten über die Schnittstelle herzustellen. Informationen dazu finden Sie im **CommandCenter Secure Gateway-Benutzerhandbuch** von Raritan.

So stellen Sie eine Verbindung mit einem Knoten her:

1. Klicken Sie auf die Registerkarte "Knoten".
2. Wählen Sie den Knoten aus, zu dem Sie eine Verbindung herstellen möchten. Führen Sie außerdem Folgendes durch:
   - Klicken Sie in der Tabelle "Schnittstellen" auf den Namen der Schnittstelle, über die Sie die Verbindung herstellen möchten.

   Oder

- Erweitern Sie auf der Registerkarte "Knoten" die Liste der Schnittstellen unter dem Knoten, mit dem Sie eine Verbindung herstellen möchten. Doppelklicken Sie auf den Namen der Schnittstelle, zu der Sie eine Verbindung herstellen möchten, oder klicken Sie mit der rechten Maustaste auf die Schnittstelle, und wählen Sie "Verbinden".

Firefox-Benutzer des Zugriffs-Clients müssen JNLP-Datei herunterladen

Firefox-Benutzer des Zugriffs-Clients werden bei jeder Out-of-Band-KVM-Portverbindung aufgefordert, eine .JNLP-Datei herunterzuladen.

Aktivieren Sie das Kontrollkästchen "Do this automatically for files like this from now on" (Dies von nun an automatisch für Dateien wie diese ausführen), sodass Firefox die Datei für künftige Verbindungen automatisch herunterladen kann.

Knoten anpingen

Sie können einen Knoten über CC-SG anpingen, um sicherzustellen, dass die Verbindung aktiv ist.

So pingen Sie einen Knoten an:

1. Klicken Sie auf die Registerkarte "Knoten", und wählen Sie den Knoten zum Anpingen aus.
2. Wählen Sie "Knoten > Knoten anpingen". Die Ergebnisse des Pingvorgangs werden angezeigt.

Schnittstellen hinzufügen, bearbeiten und löschen

Schnittstellen hinzufügen

Hinweis: Schnittstellen für virtuelle Knoten wie das Steuerungssystem, virtuelle Hosts und virtuelle Geräte können nur mit den Virtualisierungstools unter "Knoten" > "Virtualisierung" hinzugefügt werden. Siehe **Virtuelle Infrastruktur in CC-SG konfigurieren** *(auf Seite 133).*

So fügen Sie eine Schnittstelle hinzu:

1. Bei einem vorhandenen Knoten: Klicken Sie auf die Registerkarte "Knoten", und wählen Sie den Knoten aus, dem Sie eine Schnittstelle hinzufügen möchten. Klicken Sie im Bereich "Schnittstellen" des Bildschirms "Knotenprofil" auf "Hinzufügen".

Beim Hinzufügen von neuen Knoten: Klicken Sie im Bereich "Schnittstellen" des Bildschirms "Knoten hinzufügen" auf "Hinzufügen".

Das Fenster "Schnittstelle hinzufügen" wird angezeigt.

2. Klicken Sie auf das Dropdown-Menü "Schnittstellentyp", und wählen Sie die Verbindungsart für den Knoten aus:

In-Band-Verbindungen:

- In-Band - DRAC KVM: Wählen Sie diese Option aus, um eine KVM-Verbindung zu einem Dell DRAC-Server über eine DRAC-Schnittstelle herzustellen. Sie müssen auch eine DRAC-Stromversorgungs-Schnittstelle konfigurieren.
- In-Band - iLO Processor KVM: Wählen Sie diese Option aus, um eine KVM-Verbindung zu einem HP-Server über eine iLO- oder RILOE-Schnittstelle herzustellen.
- In-Band - RDP: Wählen Sie diese Option aus, um eine KVM-Verbindung zu einem Knoten über Java oder Microsoft Remote Desktop Protocol herzustellen.
- In-Band - RSA KVM: Wählen Sie diese Option aus, um eine KVM-Verbindung zu einem IBM RSA-Server über eine RSA-Schnittstelle herzustellen. Sie müssen auch eine RSA-Stromversorgungs-Schnittstelle konfigurieren.
- In-Band - SSH: Wählen Sie diese Option aus, um eine SSH-Verbindung zu einem Knoten herzustellen.
- In-Band - VNC: Wählen Sie diese Option aus, um eine KVM-Verbindung zu einem Knoten über eine VNC-Serversoftware herzustellen.

  Siehe ***Schnittstellen für In-Band-Verbindungen*** (auf Seite 151).

Out-of-Band-Verbindungen:

- Out-of-Band - KVM: Wählen Sie diese Option aus, um eine KVM-Verbindung zu einem Knoten über ein Raritan KVM-Gerät (KX, KX101, KSX, IP-Reach, Paragon II) herzustellen.
- Out-of-Band - Seriell: Wählen Sie diese Option aus, um eine serielle Verbindung zu einem Knoten über ein serielles Raritan-Gerät (SX, KSX) herzustellen.

  Siehe ***Schnittstellen für Out-of-Band KVM-, Out-of-Band serielle Verbindungen*** (auf Seite 152).

Stromversorgungsverbindungen:

- Stromversorgungssteuerung - DRAC: Wählen Sie diese Option aus, um eine Stromversorgungsverbindung zu einem Dell DRAC-Server zu erstellen.

- Stromversorgungssteuerung - iLO Processor: Wählen Sie diese Option aus, um eine Stromversorgungsverbindung zu einem HP iLO/RILOE-Server zu erstellen.
- Stromversorgungssteuerung - IPMI: Wählen Sie diese Option aus, um eine Stromversorgungsverbindung zu einem Knoten mit einer IPMI-Verbindung herzustellen.
- Stromversorgungssteuerung – Integrity ILO2: Wählen Sie diese Option aus, um eine Stromversorgungsverbindung zu einem HP Integrity-Server oder sonstigen Servern, die Integrity ILO2 unterstützen, zu erstellen.
- Stromversorgungssteuerung – Power IQ Proxy: Wählen Sie diese Option aus, um eine Stromversorgungsverbindung zu einem Power IQ IT-Gerät zu erstellen.
- Stromversorgungssteuerung - RSA: Wählen Sie diese Option aus, um eine Stromversorgungsverbindung zu einem RSA-Server zu erstellen.

  Siehe ***Schnittstellen für DRAC-Stromversorgungsverbindungen*** (auf Seite 153)

  Schnittstellen für ILO Processor-, Integrity ILO2- und RSA-Stromversorgungsverbindungen (auf Seite 153)

  Schnittstellen für Power IQ Proxy-Stromversorgungsverbindungen (auf Seite 156)

Verwaltete PowerStrip-Verbindungen:

- Verwalteter Powerstrip: Wählen Sie diese Option aus, um eine Stromversorgungsverbindung zu einem Knoten herzustellen, der über einen Raritan-PowerStrip oder ein Dominion PX-Gerät versorgt wird.

  Siehe ***Schnittstellen für verwaltete Powerstrip-Verbindungen*** (auf Seite 154).

Webbrowserverbindungen:

- Webbrowser: Wählen Sie diese Option aus, um eine Verbindung zu einem Gerät mit einem eingebetteten Webserver herzustellen.

  Siehe ***Webbrowser-Schnittstelle*** (auf Seite 157).

3. Im Feld "Name" wird ein Standardname angezeigt. Dies ist davon abhängig, welchen Schnittstellentyp Sie auswählen. Sie können den Namen ändern. Dieser Name wird neben der Schnittstelle in der Knotenliste angezeigt. Weitere Informationen zu den Regeln, die von CC-SG für die Länge von Namen verwendet werden, finden Sie unter ***Benennungskonventionen*** (siehe "***Benennungsregeln***" auf Seite 457).

Schnittstellen für In-Band-Verbindungen

Zu den In-Band-Verbindungen gehören RDP, VNC, SSH, RSA KVM, iLO Processor KVM, DRAC KVM und TELNET.

Telnet ist keine sichere Zugriffsmethode. Alle Benutzernamen und Kennwörter sowie der gesamte Verkehr werden als Klartext übertragen.

So fügen Sie eine Schnittstelle für In-Band-Verbindungen hinzu:

1. Geben Sie die IP-Adresse oder den Hostnamen dieser Schnittstelle in das Feld IP-Adresse/Hostname ein.
2. Geben Sie einen TCP-Port für diese Verbindung in das Feld "TCP-Port" ein. **Optional.**
3. Wählen Sie für RDP-Schnittstellen Java oder Windows und anschließend "Konsole" oder "Remotebenutzer" aus. Wenn ein Konsolenbenutzer auf einen Knoten zugreift, werden alle anderen Benutzer getrennt. Mehrere Remotebenutzer können gleichzeitig auf einen Knoten zugreifen.
4. Geben Sie Authentifizierungsinformationen ein:
   - Um ein Dienstkonto zur Authentifizierung zu verwenden, markieren Sie das Kontrollkästchen "Dienstkontoinformationen verwenden". Wählen Sie das gewünschte Dienstkonto im Menü "Dienstkontoname".

   Oder

   - Geben Sie einen Benutzernamen und ein Kennwort für die Authentifizierung ein. Für VNC-Schnittstellen ist nur ein Kennwort erforderlich.
5. Wählen Sie das Tastaturlayout für Ihre Sprache. Diese Option ist für Microsoft RDP-Schnittstellen nicht verfügbar.
6. Geben Sie eine Beschreibung für die Schnittstelle in das Feld "Beschreibung" ein. **Optional.**
7. Klicken Sie zum Speichern der Änderungen auf OK.

DRAC 5-Verbindungsdetails

Wenn Sie den Internet Explorer verwenden und eine Verbindung zu DRAC 5-Servern herstellen, müssen Sie über ein gültiges installiertes Zertifikat auf DRAC 5 verfügen, ansonsten wird vom Internet Explorer eine Fehlermeldung ausgegeben.

Wenn das Zertifikat nicht von einer vertrauenswürdigen Zertifizierungsstelle signiert wurde, speichern Sie dasselbe Zertifikat zusätzlich unter den vertrauenswürdigen Stammzertifizierungsstellen des Browsers.

Microsoft RDP-Verbindungsdetails

- Wenn Sie einen Windows XP-Client verwenden, müssen Sie Terminal Server Client 6.0 oder höher nutzen, um eine Verbindung von CC-SG zu einer Microsoft RDP-Schnittstelle herzustellen. Über den folgenden Link können Sie den Terminal Server Client auf Version 6.0 aktualisieren: http://support.microsoft.com/kb/925876.
- Nur Internet Explorer.
- Microsoft RDP kann nicht für Verbindungen im Proxymodus verwendet werden. Siehe ***Verbindungsmodi*** (auf Seite 297).
- Zu den unterstützten Zielgeräten zählen: Vista, Win2008 Server und Windows 7 sowie alle vorherigen Windows-Versionen einschließlich Windows XP- und Windows 2003-Ziele.
- Weitere Informationen zu Microsoft RDP, einschließlich Nutzungsinformationen finden Sie unter: http://www.microsoft.com/downloads/details.aspx?FamilyID=469eee3a-45b4-4b40-b695-b678646a728b&displaylang=en

Java RDP-Verbindungsdetails

- Die Java RDP-Schnittstelle unterstützt Windows XP- und Windows 2003-Ziele.
- Java RDP kann für Verbindungen im Proxymodus verwendet werden. Siehe ***Verbindungsmodi*** (auf Seite 297).

Schnittstellen für Out-of-Band KVM-, Out-of-Band serielle Verbindungen

So fügen Sie eine Schnittstelle für Out-of-Band KVM- oder Out-of-Band serielle Verbindungen hinzu:

1. Anwendungsname: Wählen Sie in der Liste die Anwendung aus, mit der Sie über die Schnittstelle eine Verbindung zum Konten herstellen möchten.
   - CC-SG wählt die Anwendung basierend auf Ihrem Browser automatisch aus, wenn Sie Automatisch erkennen markieren.
   - Um Active KVM Client nutzen zu können, sind bestimmte Voraussetzungen erforderlich. Siehe ***Voraussetzungen bei der Nutzung von AKC*** (siehe "***Voraussetzungen für die Verwendung des AKC***" auf Seite 286) und ***AKC-Download-Serverzertifikatsvalidierung aktivieren*** (siehe "***Aktivieren der AKC-Download-Serverzertifikat-Validierung***" auf Seite 300).
2. Raritan-Gerätename: Wählen Sie das Raritan-Gerät aus, das den Zugriff auf diesen Knoten bereitstellt. Sie müssen zunächst ein Gerät zu CC-SG hinzufügen, bevor es in der Liste angezeigt werden kann.

3. Raritan-Portname: Wählen Sie den Port auf dem Raritan-Gerät aus, das den Zugriff auf diesen Knoten bereitstellt. Der Port muss in CC-SG konfiguriert werden, bevor er in der Liste angezeigt wird. Bei seriellen Verbindungen werden die Werte für Baudrate, Parität und Flusssteuerung anhand der Portkonfiguration ausgefüllt.
4. Geben Sie eine Beschreibung für die Schnittstelle in das Feld "Beschreibung" ein. **Optional.**
5. Klicken Sie zum Speichern der Änderungen auf OK.

Schnittstellen für DRAC-Stromversorgungsverbindungen

So fügen Sie eine Schnittstelle für DRAC-Stromversorgungsverbindungen hinzu:

1. Geben Sie die IP-Adresse oder den Hostnamen dieser Schnittstelle in das Feld IP-Adresse/Hostname ein.
2. Geben Sie einen TCP-Port für diese Verbindung in das Feld "TCP-Port" ein. **Nur DRAC 5.** Für DRAC 4 ist kein TCP-Port erforderlich**.**
3. Geben Sie Authentifizierungsinformationen ein:
   - Um ein Dienstkonto zur Authentifizierung zu verwenden, markieren Sie das Kontrollkästchen "Dienstkontoinformationen verwenden". Wählen Sie das gewünschte Dienstkonto im Menü "Dienstkontoname".

   Oder

   - Geben Sie einen Benutzernamen und ein Kennwort für die Authentifizierung ein.
4. Geben Sie eine Beschreibung für die Schnittstelle in das Feld "Beschreibung" ein. **Optional.**
5. Klicken Sie zum Speichern der Änderungen auf OK.

Schnittstellen für ILO Processor-, Integrity ILO2- und RSA-Stromversorgungsverbindungen

So fügen Sie eine Schnittstelle für ILO Processor-, Integrity ILO2- und RSA-Stromversorgungsverbindungen hinzu:

1. Geben Sie die IP-Adresse oder den Hostnamen dieser Schnittstelle in das Feld IP-Adresse/Hostname ein.
2. Geben Sie Authentifizierungsinformationen ein:
   - Um ein Dienstkonto zur Authentifizierung zu verwenden, markieren Sie das Kontrollkästchen "Dienstkontoinformationen verwenden". Wählen Sie das gewünschte Dienstkonto im Menü "Dienstkontoname".

   Oder

- Geben Sie einen Benutzernamen und ein Kennwort für die Authentifizierung ein.

3. Geben Sie eine Beschreibung für die Schnittstelle in das Feld "Beschreibung" ein. **Optional.**
4. Klicken Sie zum Speichern der Änderungen auf OK.

Details zur RSA-Schnittstelle

Wenn Sie eine In-Band-RSA KVM- oder Stromversorgungs-Schnittstelle erstellen, werden der der Schnittstelle zugewiesene Benutzername und das Kennwort von CC-SG verworfen und zwei Benutzerkonten auf dem RSA-Server erstellt. So erhalten Sie gleichzeitigen KVM- und Stromversorgungszugriff auf den RSA-Server.

Neue Benutzernamen:

- cc_kvm_user
- cc_power_user

Diese Benutzernamen ersetzen den Benutzernamen, den Sie beim Erstellen der Schnittstellen eingegeben haben. CC-SG verwendet diese neuen Benutzerkonten zur Verbindungsherstellung mit dem RSA-Server über die Schnittstellen.

Die Kennwörter dieser Benutzerkonten auf dem RSA-Server dürfen nicht gelöscht, bearbeitet oder geändert werden, andernfalls kann von CC-SG keine Verbindung unter Verwendung der Schnittstellen mehr hergestellt werden.

Wenn Sie zum Erstellen der Schnittstellen ein Dienstkonto verwendet haben, erstellt CC-SG auf dem RSA-Server keine Benutzerkonten. Wenn Sie für die Schnittstellen ein Dienstkonto verwenden, haben Sie keinen gleichzeitigen KVM- und Stromversorgungszugriff auf den RSA-Server.

RSA-Kompatibilität mit JRE

IBM RSA II Version 1.14 ist mit JRE Version 1.6.0_10 und 1.6.0_11 kompatibel.

CC-SG unterstützt auch höhere JRE-Versionen, aber höhere JRE-Versionen arbeiten mit IBM RSA II-Karten nicht gut zusammen.

Schnittstellen für verwaltete Powerstrip-Verbindungen

Wenn Sie eine verwaltete Powerstrip-Schnittstelle erstellen, die ein KX-Gerät als Verwaltungsgerät festlegt, wird der von Ihnen festgelegte Ausgang in den Namen des zugewiesenen Knotens umbenannt.

So fügen Sie eine Schnittstelle für verwaltete Powerstrip-Verbindungen hinzu:

1. Verwaltungsgerät:

- Wählen Sie das Raritan-Gerät aus, an das der PowerStrip angeschlossen ist. Das Gerät muss zu CC-SG hinzugefügt werden.

Oder

- Wählen Sie "Dominion PX", wenn diese Stromversorgungs-Steuerungsschnittstelle ein PX-Gerät im IP-Netzwerk verwendet, das nicht an ein anderes Raritan-Gerät angeschlossen ist.

2. Verwaltungsport: Wählen Sie den Port am Raritan-Gerät aus, an den der PowerStrip angeschlossen ist. Dieses Feld ist deaktiviert, wenn Sie PX als Verwaltungsgerät auswählen.
3. Powerstrip-Name:* Wählen Sie den Powerstrip oder das PX-Gerät aus, der bzw. das den Knoten mit Strom versorgt. Der Powerstrip oder das PX-Gerät muss in CC-SG konfiguriert werden, bevor er bzw. es in der Liste angezeigt wird.
4. Ausgangsname:* Wählen Sie den Namen des Ausgangs aus, an den der Knoten angeschlossen ist. **Optional.**
5. Geben Sie eine Beschreibung für die Schnittstelle in das Feld "Beschreibung" ein.
6. Klicken Sie zum Speichern der Änderungen auf OK.

Hinweis: Sie können einem Blade-Chassis-Knoten, jedoch nicht einem Blade-Server-Knoten, eine Schnittstelle für einen verwalteten Powerstrip hinzufügen.

Schnittstellen für IPMI-Stromversorgungsverbindungen

So fügen Sie eine Schnittstelle für IPMI-Stromversorgungsverbindungen hinzu:

1. Geben Sie die IP-Adresse oder den Hostnamen dieser Schnittstelle in das Feld IP-Adresse/Hostname ein.
2. Geben Sie eine UDP-Portnummer für diese Schnittstelle in das Feld "UDP-Port" ein.
3. Authentifizierung: Wählen Sie ein Authentifizierungsschema für die Verbindung zu dieser Schnittstelle aus.
4. Geben Sie für diese Schnittstelle ein Überprüfungsintervall im Feld Überprüfungsintervall (Sekunden) ein.
5. Geben Sie Authentifizierungsinformationen ein:

   - Um ein Dienstkonto zur Authentifizierung zu verwenden, markieren Sie das Kontrollkästchen "Dienstkontoinformationen verwenden". Wählen Sie das gewünschte Dienstkonto im Menü "Dienstkontoname".

   Oder

- Geben Sie einen Benutzernamen und ein Kennwort für die Authentifizierung ein. **Optional.**

6. Geben Sie eine Beschreibung für die Schnittstelle in das Feld "Beschreibung" ein. **Optional.**
7. Klicken Sie zum Speichern der Änderungen auf OK.

Einzelheiten zur IBM IMM-Modulverbindung

Über CD-SG für Stromversorgungs-Steuerungsvorgänge und eine IPMI-Stromversorgungsverbindung können Sie eine Verbindung zur Standardversion eines IBM IMM-Moduls herstellen. Funktionen zum Einschalten, Ausschalten sowie Aus- und Einschalten werden unterstützt.

Siehe ***Schnittstellen für IPMI-Stromversorgungsverbindungen*** (auf Seite 155).

Hinweis: KVM-Zugriff auf IBM IMM-Module ist über CC-SG nicht möglich.

Schnittstellen für Power IQ Proxy-Stromversorgungsverbindungen

Fügen Sie eine Power IQ Proxy-Schnittstelle zur Stromversorgungssteuerung hinzu, wenn Sie CC-SG zur Stromversorungssteuerung eines Power IQ-IT-Geräts verwenden, das Sie als Knoten zu CC-SG hinzugefügt haben. Hiermit können Sie die Stromversorgung von Knoten steuern, die mit nicht durch CC-SG verwalteten PDUs verbunden sind.

So fügen Sie eine Schnittstelle für Power IQ Proxy-Stromversorgungsverbindungen hinzu:

1. Geben Sie den externen Schlüssel des IT-Geräts ein. Der externe Schlüssel muss für Power IQ und CC-SG gleich lauten. Maximal 255 Zeichen. Kommas sind nicht zulässig. Als Standardwert gilt der Knotenname. Sie können diesen Wert ändern.
   - Wenn das IT-Gerät bereits zu Power IQ hinzugefügt wurde, suchen Sie den externen Schlüssel auf der Seite des IT-Geräts auf der Registerkarte "Data Center" (Rechenzentrum) und geben Sie anschließend den Text in das Feld "Extenal Key" (Externer Schlüssel) ein.
   - Wenn das IT-Gerät noch nicht zu Power IQ hinzugefügt wurde, akzeptieren Sie den Standardwert für den externen Schlüssel oder ändern Sie ihn, aber stellen Sie sicher, dass beim Hinzufügen des IT-Geräts zu Power IQ derselbe Wert verwendet wird. Durch einen Export können Sie auf schnelle Weise eine Datei mit allen Knoten- und Schnittstelleninformationen erstellen. Siehe ***Knoten exportieren*** (auf Seite 177).

2. Wählen Sie im Feld "Verwaltungsgerät" das Power IQ-Gerät aus, das das IT-Gerät verwaltet. Bevor das Power IQ-Gerät in diesem Feld angezeigt wird, müssen Sie Informationen über das Gerät in CC-SG hinzufügen. Siehe ***Power IQ-Dienste konfigurieren*** (auf Seite 400).
3. Geben Sie eine Beschreibung für die Schnittstelle in das Feld "Beschreibung" ein.
4. Klicken Sie zum Speichern der Änderungen auf OK.

Webbrowser-Schnittstelle

Sie können eine Webbrowser-Schnittstelle hinzufügen, um eine Verbindung zu einem Gerät mit einem eingebetteten Webserver, z. B. Dominion PX, zu erstellen. Siehe ***Beispiel: Webbrowser-Schnittstelle zu einem PX-Knoten hinzufügen*** (auf Seite 159). Einem Blade-Chassis mit integriertem KVM-Switch wird automatisch eine Webbrowser-Schnittstelle hinzugefügt, sofern Sie diesem Blade-Chassis eine URL- oder IP-Adresse auf dem KX2-Gerät zugewiesen haben.

Mit einer Webbrowser-Schnittstelle kann auch eine Verbindung zu einer Webanwendung, z. B. der Webanwendung, die einer RSA-, DRAC- oder iLO Processor-Karte zugewiesen ist, hergestellt werden.

Eine Webbrowser-Schnittstelle lässt eventuell keine automatische Anmeldung zu, wenn die Webanwendung weitere Informationen als den Benutzernamen und das Kennwort benötigt, z. B. eine Sitzungs-ID.

Benutzer müssen über die Berechtigung "In-Band-Zugriff für Knoten" verfügen, um auf eine Webbrowser-Schnittstelle zugreifen zu können.

Nur wenn DNS konfiguriert wurde, werden URLs aufgelöst. DNS muss nicht für IP-Adressen konfiguriert sein.

So fügen Sie eine Webbrowser-Schnittstelle hinzu:

1. Der Standardname für eine Webbrowser-Schnittstelle ist Webbrowser. Sie können den Namen im Feld "Name" ändern. Weitere Informationen zu den Regeln, die von CC-SG für die Länge von Namen verwendet werden, finden Sie unter ***Benennungskonventionen*** (siehe "***Benennungsregeln***" auf Seite 457).
2. Geben Sie einen TCP-Port für diese Verbindung in das Feld "TCP-Port" ein. Wenn Sie HTTPS im URL verwenden, müssen Sie den TCP-Port auf 443 festsetzen. **Optional.**
3. Geben Sie den URL oder Domänennamen der Webanwendung in das Feld URL ein. Beachten Sie, dass Sie den URL eingeben müssen, bei dem die Webanwendung erwartet, den Benutzernamen und das Kennwort zu lesen. Die Höchstanzahl sind 120 Zeichen. Beachten Sie diese Beispiele für die richtigen Formate:
   - http(s)://192.168.1.1/login.asp

- http(s)://www.Beispiel.com/cgi/login
- http(s)://Beispiel.com/home.html

4. Geben Sie Authentifizierungsinformationen ein: **Optional.**
   - Um ein Dienstkonto zur Authentifizierung zu verwenden, markieren Sie das Kontrollkästchen "Dienstkontoinformationen verwenden". Wählen Sie das gewünschte Dienstkonto im Menü "Dienstkontoname".

   Oder

   - Geben Sie einen Benutzernamen und ein Kennwort für die Authentifizierung ein. Geben Sie die Kombination von Benutzername und Kennwort ein, die den Zugriff auf diese Schnittstelle zulässt.

   Hinweis: Geben Sie keine Authentifizierungsinformationen für DRAC-, ILO- und RSA-Webanwendungen ein, weil die Verbindung sonst fehlschlägt.

5. Geben Sie die Feldnamen der Felder für den Benutzernamen und das Kennwort, die im Anmeldebildschirm für die Webanwendung verwendet werden, in das Feld für Benutzername und im Feld für Kennwort ein. Sie müssen den HTML-Quelltext des Anmeldebildschirms anzeigen, um die Feldnamen zu suchen. Verwechseln Sie die Feldnamen nicht mit den Feldbeschriftungen. Siehe ***Tipps für das Hinzufügen einer Webbrowser-Schnittstelle*** (auf Seite 158).
6. Geben Sie eine Beschreibung für die Schnittstelle in das Feld "Beschreibung" ein. **Optional.**
7. Klicken Sie zum Speichern der Änderungen auf OK.

Tipps für das Hinzufügen einer Webbrowser-Schnittstelle

Zum Konfigurieren der Webbrowser-Schnittstelle müssen Sie einige Informationen aus dem HTML-Quelltext zusammentragen, um die tatsächlichen Feldnamen der Felder Benutzername und Kennwort zu identifizieren. Alle Anbieter implementieren diese Authentifizierungsfelder unterschiedlich. Außerdem variieren die Namen dieser Felder von Gerät zu Gerät sowie zwischen den Firmwareversionen einzelner Geräte. Aus diesem Grund gibt es nicht nur eine Methode zum Suchen dieser Feldnamen. Eine mögliche Methode ist im Folgenden beschrieben.

Ein Softwaretechniker oder Systemadministrator kann Ihnen bei der Suche und Identifizierung der entsprechenden Feldnamen helfen.

Tipp zum Suchen der Feldnamen:

1. Suchen Sie im HTML-Quelltext der Anmeldeseite für die Webanwendung nach der Beschriftung des Felds, z. B. Benutzername und Kennwort.

2. Wenn Sie die Feldbeschriftung gefunden haben, suchen Sie im angrenzenden Code nach einem Tag, der so ähnlich aussieht wie `name="user"`.

   Das Wort in Anführungszeichen ist der Feldname.

Beispiel: Webbrowser-Schnittstelle zu einem PX-Knoten hinzufügen

Ein PowerStrip, der von einem Dominion PX verwaltet wird, kann als Knoten zu CC-SG hinzugefügt werden. Sie können dem Knoten dann eine Webbrowser-Schnittstelle hinzufügen, über die Benutzer auf die webbasierte Verwaltungsanwendung des Dominion PX-Geräts zugreifen können.

Verwenden Sie die folgenden Werte, um eine Webbrowser-Schnittstelle für einen Dominion PX-Knoten hinzuzufügen:

URL: <`DOMINION PX-IP-ADRESSE`>`/auth.asp`

TCP-Port: 80

Benutzername: Der Benutzername des Dominion PX-Administrators.

Kennwort: Das Kennwort des Dominion PX-Administrators.

Feld für Benutzername = `login`

Feld für Kennwort = `password`

Ergebnisse nach dem Hinzufügen von Schnittstellen

Wenn Sie einem Knoten eine Schnittstelle hinzufügen, wird die Schnittstelle in der Tabelle "Schnittstellen" und dem Dropdown-Menü "Standardschnittstelle" des Bildschirms "Knoten hinzufügen" oder "Knotenprofil" angezeigt. Sie können auf das Dropdown-Menü klicken, um die Standardschnittstelle auszuwählen, die für Verbindungen zu Knoten verwendet werden soll.

Nachdem Sie die Änderungen im Bildschirm "Knoten hinzufügen" oder "Knotenprofil" gespeichert haben, werden die Namen der Schnittstellen auch in den Knotenlisten verschachtelt unter dem Knoten angezeigt, für den sie den Zugriff bereitstellen.

Wenn Sie eine verwaltete Powerstrip-Schnittstelle hinzufügen, die ein KX-Gerät als Verwaltungsgerät festlegt, wird der von Ihnen festgelegte Ausgang in den Namen des zugewiesenen Knotens umbenannt.

Schnittstellen bearbeiten

So bearbeiten Sie eine Schnittstelle:

1. Klicken Sie auf die Registerkarte "Knoten", und wählen Sie den Knoten mit der zu bearbeitenden Schnittstelle aus. Die Seite "Knotenprofil" wird angezeigt.
2. Wählen Sie auf der Registerkarte "Schnittstellen" die Schnittstellenzeile aus, die Sie bearbeiten möchten.
3. Klicken Sie auf "Bearbeiten".
4. Bearbeiten Sie bei Bedarf die Felder. Weitere Informationen zu den Feldern finden Sie unter ***Schnittstellen hinzufügen*** (auf Seite 148). Manche Felder sind schreibgeschützt.
5. Klicken Sie zum Speichern der Änderungen auf OK.

Schnittstellen löschen

Sie können jede Schnittstelle, ausgenommen der folgenden Schnittstellen, aus einem Knoten löschen:

- Eine VMW-Viewer-Schnittstelle oder eine VMW-Stromversorgungs-Schnittstelle auf einem virtuellen Geräteknoten.
- Eine Webbrowser-Schnittstelle auf einem Blade-Chassis mit integriertem KVM-Switch, wenn ein URL oder eine IP-Adresse auf dem KX2-Gerät zugewiesen wurde.

So löschen Sie eine Schnittstelle eines Knotens:

1. Klicken Sie auf die Registerkarte "Knoten".
2. Klicken Sie auf den Knoten mit der Schnittstelle, die Sie löschen möchten.
3. Wählen Sie in der Tabelle "Schnittstellen" die Schnittstellenzeile aus, die Sie löschen möchten.
4. Klicken Sie auf "Löschen". Eine Bestätigungsmeldung wird angezeigt.
5. Klicken Sie auf "Ja", um die Schnittstelle zu löschen.

Lesezeichen für Schnittstelle

Wenn Sie häufig über eine bestimmte Schnittstelle auf einen Knoten zugreifen, können Sie ein Lesezeichen für diese Schnittstelle in Ihrem Browser erstellen, d. h. die Schnittstelle Ihren Favoriten hinzufügen.

So erstellen Sie ein Lesezeichen für eine Schnittstelle in Ihrem Browser:

1. Wählen Sie auf der Registerkarte "Knoten" die Schnittstelle aus, für die ein Lesezeichen erstellt werden soll. Sie müssen den Knoten erweitern, um die Schnittstellen anzuzeigen.
2. Wählen Sie "Knoten > Lesezeichen für Knotenschnittstelle".
3. Wählen Sie "URL in Zwischenablage kopieren".
4. Klicken Sie auf OK. Der URL wird in die Zwischenablage kopiert.
5. Öffnen Sie ein neues Browserfenster, und fügen Sie den URL in die Adresszeile ein.
6. Drücken Sie die Eingabetaste, um eine Verbindung zum URL herzustellen.
7. Fügen Sie den URL als Lesezeichen (Favorit) in Ihrem Browser hinzu.

So erstellen Sie ein Lesezeichen für eine Schnittstelle in Internet Explorer bzw. so fügen Sie eine Schnittstelle den Favoriten hinzu:

1. Wählen Sie auf der Registerkarte "Knoten" die Schnittstelle aus, für die ein Lesezeichen erstellt werden soll. Sie müssen den Knoten erweitern, um die Schnittstellen anzuzeigen.
2. Wählen Sie "Knoten > Lesezeichen für Knotenschnittstelle".
3. Wählen Sie "Lesezeichen hinzufügen (nur IE)".
4. Im Feld "Lesezeichenname" wird ein Standardname für das Lesezeichen angezeigt. Sie können den Namen ändern, der im Internet Explorer in der Liste "Favoriten" angezeigt wird.
5. Klicken Sie auf OK. Das Fenster "Zu Favoriten hinzufügen" wird angezeigt.
6. Klicken Sie auf OK, um das Lesezeichen der Liste "Favoriten" hinzuzufügen.

So greifen Sie auf eine mit einem Lesezeichen versehene Schnittstelle zu:

1. Öffnen Sie ein Browserfenster.
2. Wählen Sie die Schnittstelle in der Liste der Lesezeichen (Favoriten) im Browser aus.

3. Wenn der CC-SG-Zugriffs-Client angezeigt wird, melden Sie sich als ein Benutzer an, der Zugriff auf die Schnittstelle hat. Die Verbindung zur Schnittstelle wird hergestellt.

So erstellen Sie Lesezeichen-URLs für alle Knoten:

- Sie können Lesezeichen-URLs für alle Knoten im Knotenanlagebericht erstellen. Siehe ***Knotenanlagebericht*** (auf Seite 258).

Direkten Portzugriff auf Knoten konfigurieren

Sie können mit der Funktion "Lesezeichen für Knotenschnittstelle" einen direkten Portzugriff auf einen Knoten konfigurieren.

Siehe ***Lesezeichen für Schnittstelle*** (auf Seite 161).

Massenkopieren für Knotenzuordnungen, Einsatzort und Kontakte

Mit dem Befehl "Massenkopieren" können Sie Kategorien, Elemente, Einsatzort und Kontaktinformationen von einem Knoten auf mehrere andere Knoten mittels Kopieren übertragen. Die ausgewählten Informationen sind die einzigen bei diesem Vorgang kopierten Eigenschaften. Wenn dieselben Informationstypen bereits auf einem ausgewählten Knoten vorhanden sind, werden mit dem Befehl "Massenkopieren" die vorhandenen Daten durch die neuen zugeordneten Informationen ÜBERSCHRIEBEN.

So führen Sie das Massenkopieren von Knotenzuordnungen, Einsatzort und Kontaktinformationen aus:

1. Klicken Sie auf die Registerkarte "Knoten", und wählen Sie einen Knoten aus.
2. Wählen Sie "Knoten > Massenkopieren".
3. Wählen Sie in der Liste "Available Nodes" (Verfügbare Knoten) die Knoten aus, auf die Sie die Zuordnungen, Einsatzort und Kontaktinformationen des im Feld "Knotenname" angezeigten Knotens kopieren möchten.
4. Klicken Sie auf > (Pfeil nach rechts), um der Liste "Ausgewählte Knoten" einen Knoten hinzuzufügen.
5. Wählen Sie den gewünschten Knoten aus, und klicken Sie auf < (Pfeil nach links), um ihn aus der Liste "Ausgewählte Knoten" zu entfernen.
6. Markieren Sie auf der Registerkarte "Zuordnungen" das Kontrollkästchen "Knotenzuordnungen kopieren", um alle Kategorien und Elemente des Knotens zu kopieren.

- Sie können auf dieser Registerkarte beliebige Daten ändern, hinzufügen oder löschen. Die geänderten Daten werden auf mehrere Knoten in der Liste "Ausgewählte Knoten" sowie auf den Knoten kopiert, der aktuell im Feld "Knotenname" angezeigt wird. **Optional.**

7. Markieren Sie auf der Registerkarte "Einsatzort und Kontakte" das Kontrollkästchen für die zu kopierenden Informationen.
   - Markieren Sie das Kontrollkästchen "Standortinformationen kopieren", um die Standortinformationen zu kopieren, die im Bereich "Einsatzort" angezeigt werden.
   - Markieren Sie das Kontrollkästchen "Kontaktinformationen kopieren", um die Kontaktinformationen zu kopieren, die im Bereich "Kontakte" angezeigt werden.
   - Sie können auf dieser Registerkarte beliebige Daten ändern, hinzufügen oder löschen. Die geänderten Daten werden auf mehrere Knoten in der Liste "Ausgewählte Knoten" sowie auf den Knoten kopiert, der aktuell im Feld "Knotenname" angezeigt wird. **Optional.**
8. Klicken Sie zum Massenkopieren auf OK. Eine Meldung wird eingeblendet, nachdem die ausgewählten Informationen kopiert wurden.

Chat verwenden

Chat bietet Benutzern, die mit einem Knoten verbunden sind, die Möglichkeit, miteinander zu kommunizieren. Sie müssen mit einem Knoten verbunden sein, um eine Chatsitzung für den Knoten zu starten. Nur Benutzer an demselben Knoten können miteinander chatten.

So starten Sie eine Chatsitzung:

1. Wählen Sie "Knoten > Chat > Chatsitzung starten".
2. Geben Sie im unteren linken Feld eine Nachricht ein, und klicken Sie auf "Senden". Die Nachricht wird im oberen linken Feld für alle Benutzer angezeigt.

So treten Sie einer verfügbaren Chatsitzung bei:

- Wählen Sie "Knoten > Chat > Chatsitzung anzeigen".

So beenden Sie eine Chatsitzung:

1. Klicken Sie in der Chatsitzung auf "Schließen". Eine Bestätigungsmeldung wird angezeigt.
   - Klicken Sie auf "Ja", um die Chatsitzung für alle Teilnehmer zu schließen.

- Klicken Sie auf "Nein", um die Chatsitzung zu verlassen, für andere Teilnehmer jedoch nicht zu schließen.

Knoten per CSV-Dateiimport hinzufügen

Sie können Knoten und Schnittstellen zu CC-SG hinzufügen, indem Sie eine CSV-Datei, in der die Werte enthalten sind, importieren.

Sie benötigen die Berechtigungen für Geräte-, Port- und Knotenverwaltung sowie CC-Setup und -Steuerung, um Knoten importieren bzw. exportieren zu können.

Ihnen muss eine Richtlinie zugewiesen sein, mit der Sie auf alle relevanten Geräte und Knoten zugreifen können. Hierfür wird eine Richtlinie mit vollständigem Zugriff auf alle Knoten und alle Geräte empfohlen.

Ihnen muss eine Richtlinie zugewiesen sein, mit der Sie auf alle relevanten Geräte zugreifen können, um Out-of-Band-KVM- oder Out of Band serielle Schnittstellen sowie Stromversorgungsschnittstellen zu importieren oder exportieren.

Virtuelle Infrastrukturknoten und -schnittstellen wie Steuerungssysteme, virtuelle Hosts und virtuelle Geräte werden nicht exportiert oder importiert.

Anforderungen an CSV-Dateien – Knoten

Durch die CSV-Datei für Knoten werden die Knoten, Schnittstellen sowie deren Informationen, die zum Hinzufügen zu CC-SG erforderlich sind, definiert.

- Knotennamen müssen eindeutig sein. Wenn Sie doppelte Knotennamen eingeben, fügt CC-SG eine Nummer in Klammern zum Namen hinzu, um diesen eindeutig zu kennzeichnen, und fügt anschließend den Knoten hinzu. Wenn Sie den Knoten in der CSV-Datei auch Kategorien und Elemente zuweisen und doppelte Knotennamen vorhanden sind, werden die Kategorien und Elemente möglicherweise den falschen Knoten zugewiesen. Um dies zu vermeiden, vergeben Sie für jeden Knoten einen eindeutigen Namen. Sie können auch zunächst die Knoten importieren, deren Namen in CC-SG überprüfen und anschließend eine separate Datei importieren, um Kategorien und Elemente den richtigen Knotennamen zuzuweisen.
- Um Out-of-Band-Schnittstellen hinzuzufügen, muss der zugewiesene Port nicht in CC-SG konfiguriert sein.
- Sie können keine virtuellen Infrastrukturknoten und -schnittstellen importieren. Nutzen Sie die Optionen unter "Nodes > Virtualization" (Knoten > Virtualisierung).
- Die erste Schnittstelle in der CSV-Datei nach dem Befehl ADD NODE (Knoten hinzufügen) ist als Standardschnittstelle des Knotens festgelegt.
- Exportieren Sie eine Datei aus CC-SG, um die Kommentare anzuzeigen. Diese enthalten alle Tags und Parameter, die zum Erstellen einer gültigen CSV-Datei erforderlich sind. Siehe ***Knoten exportieren*** (auf Seite 177).
- Erfüllen Sie die zusätzlichen Anforderungen für alle CSV-Dateien. Siehe ***Häufige Anforderungen an CSV-Dateien*** (siehe "***Häufige Anforderungen für CSV-Dateien***" auf Seite 434).

So fügen Sie einen Knoten zur CSV-Datei hinzu:

Spaltennummer	Tag oder Wert	Details
1	`ADD (Hinzufügen)`	Die erste Spalte für alle Tags ist der Befehl `ADD` (Hinzufügen).
2	`NODE (Knoten)`	Geben Sie das Tag wie beschrieben ein. Bei Tags wird die Groß- und Kleinschreibung nicht berücksichtigt.
3	Knotenname	Erforderliches Feld.
4	Beschreibung	Optional.

So fügen Sie eine Out-of-Band-KVM-Schnittstelle zur CSV-Datei hinzu:

Spaltennummer	Tag oder Wert	Details
1	`ADD (Hinzufügen)`	Die erste Spalte für alle Tags ist der Befehl `ADD` (Hinzufügen).
2	`NODE-OOBKVM-INTERFACE (Knoten Out-of-Band-KVM-Schnittstelle)`	Geben Sie das Tag wie beschrieben ein. Bei Tags wird die Groß- und Kleinschreibung nicht berücksichtigt.
3	Knotenname	Geben Sie denselben Wert wie für den Raritan-Portnamen ein.
4	Raritan-Gerätename:	Erforderliches Feld. Das Gerät muss bereits zu CC-SG hinzugefügt worden sein.
5	Portnummer	Erforderliches Feld.
6	Blade-Slot/KVM-Switch-Port	Wenn der Knoten einem Blade zugewiesen ist, geben Sie die Slotnummer ein. Wenn der Knoten mit einem mehrschichtigen generischen analogen KVM-Switch verknüpft ist, geben Sie die Portnummer ein.
7	Raritan-Portname:	Wenn keine Angaben gemacht werden, verwendet CC-SG den bestehenden Portnamen des Geräts. Wenn Sie einen neuen Namen eingeben, wird dieser, mit Ausnahme von SX-Geräten, für das Gerät übernommen.
8	Schnittstellenname	Geben Sie denselben Wert wie für den Raritan-Portnamen ein.
9	Beschreibung	Optional.

So fügen Sie eine Out-of-Band serielle Schnittstelle zur CSV-Datei hinzu:

Spaltennummer	Tag oder Wert	Details
1	`ADD (Hinzufügen)`	Die erste Spalte für alle Tags ist der Befehl `ADD` (Hinzufügen).

Spaltennummer	Tag oder Wert	Details
2	`NODE-OOBSERIAL-INTERFACE (Knoten Out-of-Band serielle Schnittstelle)`	Geben Sie das Tag wie beschrieben ein. Bei Tags wird die Groß- und Kleinschreibung nicht berücksichtigt.
3	Knotenname	Geben Sie denselben Wert wie für den Raritan-Portnamen ein.
4	Raritan-Gerätename:	Erforderliches Feld.
5	Portnummer	Erforderliches Feld.
6	Raritan-Portname:	Wenn keine Angaben gemacht werden, verwendet CC-SG den bestehenden Portnamen des Geräts. Wenn Sie einen neuen Namen eingeben, wird dieser, mit Ausnahme von SX-Geräten, für das Gerät übernommen.
7	Schnittstellenname	Geben Sie denselben Wert wie für den Raritan-Portnamen ein.
8	Baudrate	Nur gültig für SX-Ports.
9	Parität	Nur gültig für SX-Ports.
10	Flusssteuerung	Nur gültig für SX-Ports.
11	Beschreibung	Optional.

So fügen Sie eine RDP-Schnittstelle zur CSV-Datei hinzu:

Spaltennummer in der CSV-Datei	Tag oder Wert	Details
1	`ADD (Hinzufügen)`	Die erste Spalte für alle Tags ist der Befehl "ADD" (Hinzufügen).
2	`NODE-RDP-INTERFACE (Knoten RDP-Schnittstelle)`	Geben Sie das Tag wie beschrieben ein. Bei Tags wird die Groß- und Kleinschreibung nicht berücksichtigt.
3	Knotenname	Erforderliches Feld.
4	Schnittstellenname	Erforderliches Feld.
5	IP-Adresse oder Hostname	Erforderliches Feld.
6	TCP-Port	Der Standardwert ist 3389.
7	Dienstkontoname	Optional.

Spaltennummer in der CSV-Datei	Tag oder Wert	Details
8	Benutzername	Optional.
9	Kennwort	Optional.
10	Benutzertyp	`REMOTE` oder `CONSOLE` (Konsole) Der Standardwert lautet `REMOTE`.
11	Tastaturtyp	`USA`, `Großbritannien`, `Arabisch`, `Dänisch`, `Deutsch`, `Spanisch`, `Finnisch`, `Französisch`, `Belgisch`, `Kroatisch`, `Italienisch`, `Japanisch`, `Litauisch`, `Lettisch`, `Mazedonisch`, `Norwegisch`, `Polnisch`, `Portugiesisch`, `Brasilianisch`, `Russisch`, `Slowenisch`, `Schwedisch` oder `Türkisch` Die Standardeinstellung ist `USA`.
12	Beschreibung	Optional.
13	RDP-Typ	`Java` oder `Microsoft` Die Standardeinstellung ist `Java`.

So fügen Sie eine SSH- oder TELNET-Schnittstelle zur CSV-Datei hinzu:

Spaltennummer	Tag oder Wert	Details
1	`ADD (Hinzufügen)`	Die erste Spalte für alle Tags ist der Befehl `ADD` (Hinzufügen).
2	`NODE-SSH-INTERFACE` (Knoten SSH-Schnittstelle) für SSH-Schnittstellen `NODE-TELNET-INTERFACE` (Knoten Telnet-Schnittstelle) für TELNET-Schnittstellen	Geben Sie das Tag wie beschrieben ein. Bei Tags wird die Groß- und Kleinschreibung nicht berücksichtigt.
3	Knotenname	Erforderliches Feld.
4	Schnittstellenname	Erforderliches Feld.

Spaltennummer	Tag oder Wert	Details
5	IP-Adresse oder Hostname	Erforderliches Feld.
6	TCP-Port	Der Standardwert für SSH ist 22. Der Standardwert für TELNET ist 23.
7	Dienstkontoname	Optional. Lassen Sie das Feld leer, wenn Sie einen Benutzernamen und ein Kennwort angeben.
8	Benutzername	Optional. Lassen Sie das Feld leer, wenn Sie ein Dienstkonto angeben.
9	Kennwort	Optional.
10	Beschreibung	Optional.

So fügen Sie eine VNC-Schnittstelle zur CSV-Datei hinzu:

Spaltennummer	Tag oder Wert	Details
1	`ADD (Hinzufügen)`	Die erste Spalte für alle Tags ist der Befehl `ADD` (Hinzufügen).
2	`NODE-VNC-INTERFACE (Knoten VNC-Schnittstelle)`	Geben Sie das Tag wie beschrieben ein. Bei Tags wird die Groß- und Kleinschreibung nicht berücksichtigt.
3	Knotenname	Erforderliches Feld.
4	Schnittstellenname	Erforderliches Feld.
5	IP-Adresse oder Hostname	Erforderliches Feld.
6	TCP-Port	Der Standardwert ist 5900.
7	Dienstkontoname	Optional. Lassen Sie das Feld leer, wenn Sie ein Kennwort angeben.
8	Kennwort	Optional. Lassen Sie das Feld leer, wenn Sie ein Dienstkonto angeben.
9	Beschreibung	Optional.

So fügen Sie eine DRAC-KVM-, DRAC-Stromversorgungs-, ILO-KVM-, ILO-Stromversorgungs-, Integrity ILO2-Stromversorgungs- oder RSA-Stromversorgungs-Schnittstelle zur CSV-Datei hinzu:

Beim Importieren von DRAC-, ILO- und RSA-Schnittstellen müssen Sie sowohl die KVM- als auch die Stromversorgungs-Schnittstelle angeben. Ansonsten können Sie den Import nicht durchführen.

Spaltennummer	Tag oder Wert	Details
1	`ADD (Hinzufügen)`	Die erste Spalte für alle Tags ist der Befehl `ADD` (Hinzufügen).
2	`NODE-DRAC-KVM-INTERFACE` (Knoten DRAC-KVM-Schnittstelle) für DRAC-KVM-Schnittstellen `NODE-DRAC-POWER-INTERFACE` (Knoten DRAC-Stromversorgungsschnittstelle) für DRAC-Stromversorgungsschnittstellen `NODE-ILO-KVM-INTERFACE` (Knoten ILO-KVM-Schnittstelle) für ILO-KVM-Schnittstellen `NODE-ILO-POWER-INTERFACE` (Knoten iLO-Stromversorgungsschnittstelle) für iLO-Stromversorgungsschnittstellen `NODE-INT-ILO2-POWER-INTERFACE` (Knoten Integrity iLO2-Stromversorgungsschnittstelle) für Integrity iLO2-Stromversorgungsschnittstellen `NODE-RSA-POWER-INTERFACE` (Knoten RSA-Stromversorgungsschnittstelle) für RSA-Stromversorgungsschnittstellen	Geben Sie das Tag wie beschrieben ein. Bei Tags wird die Groß- und Kleinschreibung nicht berücksichtigt.

Spaltennummer	Tag oder Wert	Details
3	Knotenname	Erforderliches Feld.
4	Schnittstellenname	Erforderliches Feld.
5	IP-Adresse oder Hostname	Erforderliches Feld.
6	Dienstkontoname	Sie müssen entweder ein Dienstkonto oder einen Benutzernamen und ein Kennwort eingeben. Lassen Sie das Feld leer, wenn Sie einen Benutzernamen und ein Kennwort angeben.
7	Benutzername	Sie müssen entweder ein Dienstkonto oder einen Benutzernamen und ein Kennwort eingeben. Lassen Sie das Feld leer, wenn Sie ein Dienstkonto angeben.
8	Kennwort	Sie müssen entweder ein Dienstkonto oder einen Benutzernamen und ein Kennwort eingeben. Lassen Sie das Feld leer, wenn Sie ein Dienstkonto angeben.
9	Beschreibung	Optional.
10*	TCP-Port	*Nur bei `NODE-DRAC-POWER-INTERFACE` (Knoten DRAC-Stromversorgungsschnittstelle): Geben Sie einen TCP-Port an. Der Standardwert ist 22.

So fügen Sie eine RSA-KVM-Schnittstelle zur CSV-Datei hinzu:

Beim Importieren von DRAC-, ILO- und RSA-Schnittstellen müssen Sie sowohl die KVM- als auch die Stromversorgungs-Schnittstelle angeben. Ansonsten können Sie den Import nicht durchführen.

Spaltennummer	Tag oder Wert	Details
1	`ADD (Hinzufügen)`	Die erste Spalte für alle Tags ist der Befehl `ADD` (Hinzufügen).

Spaltennummer	Tag oder Wert	Details
2	`NODE-RSA-KVM-INTERFACE (Knoten RSA-KVM-Schnittstelle)`	Geben Sie das Tag wie beschrieben ein. Bei Tags wird die Groß- und Kleinschreibung nicht berücksichtigt.
3	Knotenname	Erforderliches Feld.
4	Schnittstellenname	Erforderliches Feld.
5	IP-Adresse oder Hostname	Erforderliches Feld.
6	TCP-Port	Der Standardwert ist 2000.
7	Dienstkontoname	Lassen Sie das Feld leer, wenn Sie einen Benutzernamen und ein Kennwort angeben.
8	Benutzername	Lassen Sie das Feld leer, wenn Sie ein Dienstkonto angeben.
9	Kennwort	Lassen Sie das Feld leer, wenn Sie ein Dienstkonto angeben.
10	Beschreibung	Optional.

So fügen Sie eine IPMI-Schnittstelle zur Stromversorgungssteuerung zur CSV-Datei hinzu:

Spaltennummer	Tag oder Wert	Details
1	`ADD (Hinzufügen)`	Die erste Spalte für alle Tags ist der Befehl `ADD` (Hinzufügen).
2	`NODE-IPMI-INTERFACE (Knoten IPMI-Schnittstelle)`	Geben Sie das Tag wie beschrieben ein. Bei Tags wird die Groß- und Kleinschreibung nicht berücksichtigt.
3	Knotenname	Erforderliches Feld.
4	Schnittstellenname	Erforderliches Feld.
5	IP-Adresse oder Hostname	Erforderliches Feld.
6	UDP-Port	Der Standardwert ist 623.
7	Authentifizierung	`MD5`, `None` (Keine), `OEM` oder `PASSWORD` (Kennwort) Die Standardeinstellung lautet `PASSWORD` (Kennwort).

Spaltennummer	Tag oder Wert	Details
8	Intervall	Geben Sie das Überprüfungsintervall in Sekunden ein. Der Standardwert ist 550.
9	Dienstkontoname	Lassen Sie das Feld leer, wenn Sie einen Benutzernamen und ein Kennwort angeben.
10	Benutzername	Lassen Sie das Feld leer, wenn Sie ein Dienstkonto angeben.
11	Kennwort	Lassen Sie das Feld leer, wenn Sie ein Dienstkonto angeben.
12	Beschreibung	Optional.

So fügen Sie eine verwaltete Powerstrip-Schnittstelle zur CSV-Datei hinzu:

Spaltennummer	Tag oder Wert	Details
1	`ADD (Hinzufügen)`	Die erste Spalte für alle Tags ist der Befehl `ADD` (Hinzufügen).
2	`NODE-POWER-INTERFACE (Knoten Stromversorgungsschnittstelle)`	Geben Sie das Tag wie beschrieben ein. Bei Tags wird die Groß- und Kleinschreibung nicht berücksichtigt.
3	Knotenname	Erforderliches Feld.
4	Schnittstellenname	Erforderliches Feld.
5	Powerstrip-Name	Erforderliches Feld.
6	Ausgang	Erforderliches Feld.
7	Verwaltungsgerät	Der Name des Geräts, an das der Powerstrip angeschlossen ist. Erforderliches Feld für alle Powerstrips außer Dominion PX.
8	Verwaltungsport	Der Name des Ports auf dem Gerät, an den der Powerstrip angeschlossen ist. Erforderliches Feld für alle Powerstrips außer Dominion PX.
9	Beschreibung	Optional.

So fügen Sie eine Webbrowser-Schnittstelle zur CSV-Datei hinzu:

Spaltennummer	Tag oder Wert	Details
1	`ADD (Hinzufügen)`	Die erste Spalte für alle Tags ist der Befehl `ADD` (Hinzufügen).
2	`NODE-WEB-INTERFACE (Knoten Web-Schnittstelle)`	Geben Sie das Tag wie beschrieben ein. Bei Tags wird die Groß- und Kleinschreibung nicht berücksichtigt.
3	Knotenname	Erforderliches Feld.
4	Schnittstellenname	Erforderliches Feld.
5	URL	Erforderliches Feld.
6	TCP-Port	Der Standardwert ist 80.
7	Dienstkontoname	Optional. Lassen Sie das Feld leer, wenn Sie einen Benutzernamen und ein Kennwort angeben.
8	Benutzername	Optional. Lassen Sie das Feld leer, wenn Sie ein Dienstkonto angeben.
9	Kennwort	Optional. Lassen Sie das Feld leer, wenn Sie ein Dienstkonto angeben.
10	Feld für Benutzername	Optional. Siehe ***Tipps für das Hinzufügen einer Webbrowser-Schnittstelle*** (auf Seite 158).
11	Feld für Kennwort	Optional. Siehe ***Tipps für das Hinzufügen einer Webbrowser-Schnittstelle*** (auf Seite 158).
12	Beschreibung	Optional.

So fügen Sie eine Power IQ Proxy-Schnittstelle zur Stromversorgungssteuerung zur CSV-Datei hinzu:

Weitere Informationen zum Konfigurieren dieses Schnittstellentyps finden Sie unter ***Stromversorgungssteuerung von Power IQ-IT-Geräten*** (auf Seite 399).

Spaltennummer	Tag oder Wert	Details
1	`ADD (Hinzufügen)`	Die erste Spalte für alle Tags ist der Befehl "ADD" (Hinzufügen).
2	`NODE-POWER-PIQ-INTERFACE (Knoten PIQ-Stromversorgungsschnittstelle)`	Geben Sie das Tag wie beschrieben ein. Bei Tags wird die Groß- und Kleinschreibung nicht berücksichtigt.
3	Knotenname	Erforderliches Feld.
4	Schnittstellenname	Erforderliches Feld.
5	Externer Schlüssel	▪ Wenn das IT-Gerät bereits zu Power IQ hinzugefügt wurde, suchen Sie den externen Schlüssel auf der Seite des IT-Geräts auf der Registerkarte "Data Center" (Rechenzentrum) und geben Sie anschließend den Text in das Feld ein. ▪ Wenn das IT-Gerät noch nicht zu Power IQ hinzugefügt wurde, geben Sie einen Textwert ein, aber stellen Sie sicher, dass beim Hinzufügen des IT-Geräts zu Power IQ derselbe Wert verwendet wird. Durch einen Export können Sie auf schnelle Weise eine Datei mit allen Knoten- und Schnittstelleninformationen erstellen. Siehe ***Knoten exportieren*** (auf Seite 177).
6	Name des verwaltenden Power IQ-Geräts	Geben Sie den Namen des Power IQ-Geräts ein, das das IT-Gerät verwaltet. Der Name muss mit dem Wert im Power IQ-Gerätenamensfeld im Dialogfeld "Access > Power IQ Services > "Power IQ Device Name" Configuration" (Zugriff > Power IQ-Dienste > "Power IQ-Gerätename" Konfiguration) übereinstimmen.

Spaltennummer	Tag oder Wert	Details
		Siehe ***Power IQ-Dienste konfigurieren*** (auf Seite 400).
7	Beschreibung	Optional.

So weisen Sie Kategorien oder Elemente einem Knoten in der CSV-Datei zu:

Kategorien und Elemente müssen bereits in CC-SG erstellt worden sein.

Sie können einem Knoten in der CSV-Datei mehrere Elemente derselben Kategorie zuweisen.

Spaltennummer	Tag oder Wert	Details
1	`ADD (Hinzufügen)`	Die erste Spalte für alle Tags ist der Befehl `ADD` (Hinzufügen).
2	`NODE-CATEGORYELEMENT (Knotenkategorie-Element)`	Geben Sie das Tag wie beschrieben ein. Bei Tags wird die Groß- und Kleinschreibung nicht berücksichtigt.
3	Knotenname	Erforderliches Feld.
4	Kategoriename	Erforderliches Feld.
5	Elementname	Erforderliches Feld.

Beispiel-CSV-Datei für Knoten

ADD (Hinzufügen), NODE (Knoten), NJSomersetEmailServer, Physischer Server

ADD (Hinzufügen), NODE-OOBKVM-INTERFACE (Knoten Out-of-Band-KVM-Schnittstelle), NJSomersetEmailServer, NJSomersetEmailServer, DKX2-NY-Rack7, NJSomersetEmailServer

ADD (Hinzufügen), NODE-RDP-INTERFACE (Knoten RDP-Schnittstelle), NJSomersetEmailServer,,192.168.53.42,,admins,,,,,

ADD (Hinzufügen), NODE-POWER-INTERFACE (Knoten Stromversorgungsschnittstelle), NJSomersetEmailServer, Power,,,,Rack17,4

ADD (Hinzufügen), NODE-CATEGORYELEMENT (Knotenkategorie-Element), NJSomersetEmailServer, Position, Somerset

Knoten importieren

Wenn Sie die CSV-Datei erstellt haben, überprüfen Sie sie auf Fehler und importieren Sie sie anschließend.

Doppelte Einträge werden übersprungen und somit nicht hinzugefügt.

1. Wählen Sie "Administration > Importieren >Knoten importieren".
2. Klicken Sie auf "Durchsuchen" und wählen Sie die zu importierende CSV-Datei aus. Klicken Sie auf "Öffnen".
3. Klicken Sie auf Überprüfen. Die Dateiinhalte werden im Bereich "Analysebericht" angezeigt.
   - Wenn die Datei ungültig ist, wird eine Fehlermeldung angezeigt. Klicken Sie auf "OK". Im Bereich "Probleme" auf der Seite wird eine Beschreibung der Dateiprobleme aufgeführt. Klicken Sie auf "In Datei speichern", um die Liste der Probleme zu speichern. Korrigieren Sie die CSV-Datei und versuchen Sie sie anschließend erneut zu validieren. Siehe ***Problembehebung bei CSV-Dateien*** (auf Seite 436).
4. Klicken Sie auf "Importieren".
5. Die Ergebnisse des Imports werden im Bereich "Aktionen" angezeigt. Erfolgreich importierte Elemente werden grün dargestellt. Nicht erfolgreich importierte Elemente werden rot dargestellt. Elemente, die aufgrund eines bereits vorhandenen oder bereits importierten Duplikats nicht erfolgreich importiert wurden, werden ebenso rot dargestellt.
6. Um weitere Details zu den Importergebnissen anzuzeigen, rufen Sie den Überwachungslistenbericht auf. Siehe ***Einträge in der Überwachungsliste für Importe*** (auf Seite 435).

Knoten exportieren

In der Exportdatei sind als erstes Kommentare enthalten, die jedes Element in der Datei beschreiben. Die Kommentare können als Anweisungen zum Erstellen einer Datei oder zum Importieren verwendet werden.

So exportieren Sie Knoten:

1. Wählen Sie "Administration > Exportieren >Knoten exportieren".
2. Klicken Sie auf "In Datei exportieren".
3. Geben Sie einen Namen für die Datei ein, und wählen Sie den Speicherort aus.
4. Klicken Sie auf Speichern.

Bearbeiten von IP-Adressen mit CSV-Datei-Import

Bearbeiten Sie IP-Adressen, die sich geändert haben, indem Sie die neuen IP-Adressen in einem CSV-Datei-Import hochladen.

Diese Methode eignet sich am besten für eine schnelle Aktualisierung vieler IP-Adressen.

So bearbeiten Sie IP-Adressen mit dem CSV-Datei-Import:

1. Exportieren Sie die Knoten-CSV-Datei. Siehe ***Knoten exportieren*** (auf Seite 177).
2. Öffnen Sie die exportierte Datei in einem Tabellenkalkulationsprogramm, wie z. B. Microsoft Excel. Speichern Sie die Datei sofort als .csv, um sicherzustellen, dass sie über den korrekten Dateityp verfügt.
3. Suchen Sie Zeilen, die zu ändernde IP-Adressen enthalten. Geben Sie die neuen IP-Adressen in die Zellen ein.
4. Löschen Sie in der ersten Zelle jeder zu ändernden Zeile den Befehl "ADD", und geben Sie stattdessen den Befehl "MODIFY" ein.
5. Löschen Sie alle Zeilen mit Informationen, die Sie nicht ändern möchten.
6. Speichern Sie die Datei als .csv.
7. Importieren Sie die .csv-Datei. Siehe ***Knoten importieren*** (auf Seite 177).

Knotengruppen hinzufügen, bearbeiten und löschen

Überblick über Knotengruppen

Knotengruppen werden zur Verwaltung von mehreren Knoten verwendet. Die Knotengruppe dient als Basis für eine Richtlinie, die den Zugriff auf diese Knotengruppe zulässt oder verweigert. Siehe ***Richtlinien hinzufügen*** (auf Seite 211). Knoten können manuell mit der Methode "Auswählen" oder durch Erstellen eines booleschen Ausdrucks gruppiert werden, der eine Gruppe gemeinsamer Attribute mithilfe der Methode "Beschreiben" beschreibt.

Wenn Sie den Setup-Assistenten zum Erstellen von Kategorien und Elementen für Knoten verwenden, werden einige Mittel zum Verwalten von Konten mit gemeinsamen Attributen erstellt. CC-SG erstellt automatisch Zugriffsrichtlinien basierend auf diesen Elementen. Ausführliche Informationen zum Erstellen von Kategorien und Elementen finden Sie unter ***Zuordnungen, Kategorien und Elemente*** (auf Seite 49).

So zeigen Sie Knotengruppen an:

- Wählen Sie "Zuordnungen > Knotengruppen". Das Fenster "Knotengruppenmanager" wird angezeigt. Die Liste der vorhandenen Knotengruppen wird links angezeigt, und Details der ausgewählten Knotengruppe werden im Hauptfenster angezeigt.
  - Eine Liste der vorhandenen Knotengruppen wird links angezeigt. Klicken Sie auf eine Knotengruppe, um die Details dieser Gruppe im Knotengruppenmanager anzuzeigen.
  - Die Gruppe wurde willkürlich zusammengestellt. Die Registerkarte "Knoten auswählen" wird mit jeweils einer Liste der Knoten angezeigt, die der Gruppe angehören oder nicht angehören.
  - Wurde die Gruppe basierend auf gemeinsamen Attributen gebildet, werden auf der Registerkarte "Knoten beschreiben" die Regeln angezeigt, die die Auswahl der Knoten für die Gruppe bestimmt haben.
  - Geben Sie zur Suche eines Knotens in der Knotengruppenliste unten in der Liste einen Suchbegriff in das Feld Suchen ein. Klicken Sie dann auf Suchen. Die Suchmethode wird über den Bildschirm Mein Profil konfiguriert. Siehe ***Benutzer und Benutzergruppen*** (auf Seite 185).
  - Wenn Sie eine Gruppe anzeigen, die auf Attributen basiert, können Sie über Knoten anzeigen eine Liste der Knoten anzeigen, die der Knotengruppe zugeordnet sind. Im Fenster "Knoten in der Knotengruppe" werden die Knoten und ihre Attribute angezeigt.

Knotengruppen hinzufügen

So fügen Sie eine Knotengruppe hinzu:

1. Wählen Sie "Zuordnungen > Knotengruppe". Das Fenster "Knotengruppenmanager" wird angezeigt.
2. Wählen Sie "Gruppen > Neu". Eine Vorlage einer Knotengruppe wird angezeigt.
3. Geben Sie in das Feld "Gruppenname" einen Namen für die Knotengruppe ein, die Sie erstellen möchten. Weitere Informationen zu den Regeln, die von CC-SG für die Länge von Namen verwendet werden, finden Sie unter ***Benennungskonventionen*** (siehe "***Benennungsregeln***" auf Seite 457).
4. Sie haben zwei Möglichkeiten, Knoten einer Gruppe hinzuzufügen: Knoten auswählen und Knoten beschreiben. Über Knoten auswählen können Sie willkürlich bestimmen, welche Knoten der Gruppe zugeordnet werden sollen. Wählen Sie die Knoten dazu einfach in der Liste der verfügbaren Knoten aus. Mithilfe der Methode Knoten beschreiben können Sie Regeln zum Beschreiben von Knoten festlegen. Knoten, die der Beschreibung entsprechen, werden der Gruppe hinzugefügt.

Methode "Beschreiben" und Methode "Auswählen"

Verwenden Sie die Methode "Beschreiben", wenn Ihre Gruppe auf einem Attribut des Knotens oder der Geräte basieren soll, z. B. den Kategorien und Elementen. Der Vorteil dieser Methode besteht darin, dass Geräte oder Knoten automatisch in die Gruppe aufgenommen werden, wenn Sie mehrere Geräte oder Knoten mit denselben beschriebenen Attributen hinzufügen.

Verwenden Sie die Methode "Auswählen", wenn Sie lediglich eine Gruppe bestimmter Knoten manuell erstellen möchten. Neue Knoten und Geräte, die zu CC-SG hinzugefügt werden, werden nicht automatisch in diese Gruppen eingefügt. Sie müssen die neuen Knoten bzw. Geräte manuell hinzufügen, nachdem Sie sie zu CC-SG hinzugefügt haben.

Diese beiden Methoden können nicht kombiniert werden.

Nachdem eine Gruppe mit einer Methode erstellt wurde, müssen Sie diese mit derselben Methode bearbeiten. Bei einem Methodenwechsel werden die aktuellen Gruppeneinstellungen überschrieben.

Knoten auswählen

So fügen Sie eine Knotengruppe mit der Option "Knoten auswählen":

1. Klicken Sie auf die Registerkarte "Knoten auswählen".

2. Klicken Sie auf das Dropdown-Menü "Gerätename", und wählen Sie ein Gerät aus, wenn Sie die Liste "Verfügbar" nach den Knoten durchsuchen möchten, die über Schnittstellen zu diesem Gerät verfügen.
3. Wählen Sie in der Liste "Verfügbar" den Knoten aus, den Sie der Gruppe hinzufügen möchten, und klicken Sie dann auf "Hinzufügen", um den Knoten in die Liste "Ausgewählt" zu verschieben. Knoten in der Liste "Ausgewählt" werden der Gruppe hinzugefügt.
   - Wählen Sie zum Entfernen eines Knotens aus der Gruppe den Knotennamen in der Liste "Ausgewählt" aus, und klicken Sie auf "Entfernen".
   - Sie können den Knoten in der Liste "Verfügbar" oder "Ausgewählt" suchen. Geben Sie den Suchbegriff in das Feld unter der Liste ein, und klicken Sie auf Los.
4. Wenn Sie eine Richtlinie erstellen möchten, die jederzeit Zugriff auf die Knoten dieser Gruppe erlaubt, markieren Sie "Richtlinie mit unbeschränktem Zugriff für Gruppe erstellen".
5. Wenn Sie alle Knoten zur Gruppe hinzugefügt haben, klicken Sie auf OK, um die Knotengruppe zu erstellen. Die Gruppe wird der Liste der Knotengruppen links hinzugefügt.

Knoten beschreiben

So fügen Sie eine Knotengruppe mit der Option "Knoten beschreiben":

1. Klicken Sie auf die Registerkarte "Knoten auswählen".
2. Klicken Sie auf das Symbol "Neue Zeile einfügen" , um eine Zeile in die Tabelle für eine neue Regel einzufügen. Regeln nehmen die Form eines Ausdrucks an, der mit Knoten verglichen werden kann.
3. Doppelklicken Sie auf jede Spalte in der Zeile, um für die entsprechende Zeile ein Dropdown-Menü anzuzeigen. Wählen Sie dann den entsprechenden Wert für jede Komponente aus:
   - Präfix: Feld leer lassen oder NOT auswählen. Wenn NOT ausgewählt ist, sucht diese Regel nach Werten, die dem Ausdruck nicht entsprechen.
   - Kategorie: Wählen Sie ein Attribut aus, das in der Regel bewertet wird. Es sind alle Kategorien verfügbar, die Sie im Zuordnungsmanager erstellt haben. Außerdem sind Knotenname und Schnittstelle enthalten. Wenn ein Blade-Chassis im System konfiguriert wurde, ist standardmäßig eine Blade-Chassis-Kategorie verfügbar.

- Operator: Wählen Sie einen Vergleichsvorgang, der zwischen Kategorien und Elementen durchgeführt werden soll. Es stehen drei Operatoren zur Verfügung: = (ist gleich), LIKE (zum Suchen des Elements in einem Namen) und <> (ist nicht gleich).
- Element: Wählen Sie einen Wert für das Kategorieattribut zum Vergleich aus. Hier werden nur Elemente dargestellt, die der ausgewählten Kategorie zugewiesen sind. (Beispiel: wenn eine Kategorie "Abteilung" bewertet wird, werden Elemente mit der Bezeichnung "Einsatzort" nicht angezeigt).
- Regelname: Der Name, der der Regel in dieser Zeile zugewiesen wurde. Sie können diese Werte nicht bearbeiten. Verwenden Sie diese Werte, um Beschreibungen im Feld "Kurzer Ausdruck" einzugeben.

  Die Beispielregel Abteilung = Technik beschreibt alle Knoten, bei denen die Kategorie „Abteilung“ auf „Technik“ eingestellt ist. Dies geschieht genau dann, wenn Sie die Zuordnungen während des Vorgangs Knoten hinzufügen konfigurieren.

4. Wenn Sie eine weitere Regel hinzufügen möchten, klicken Sie auf das Symbol "Neue Zeile einfügen", und nehmen Sie die entsprechenden Konfigurationen vor. Wenn Sie mehrere Regeln konfigurieren, können Sie genauere Beschreibungen anfertigen, indem Sie mehrere Kriterien zur Bewertung von Knoten bereitstellen.
   - Zum Entfernen von Regeln markieren Sie die zu löschenden Regeln in der Tabelle, und klicken Sie auf das Symbol "Zeile(n) entfernen" .
5. Die Tabelle mit Regeln stellt Kriterien zur Bewertung von Knoten bereit. Definieren Sie eine Beschreibung für die Knotengruppe, indem Sie die Regeln nach Regelname zum Feld "Kurzer Ausdruck" hinzufügen. Erfordert die Beschreibung nur eine Regel, geben Sie den Namen der Regel in das Feld ein. Werden mehrere Regeln bewertet, geben Sie die Regeln in das Feld mithilfe logischer Operatoren ein, um die Regeln in ihrer Beziehung zueinander zu beschreiben:
   - &: der UND-Operator. Ein Knoten muss die Regeln auf beiden Seiten dieses Operators für die Beschreibung (oder den Abschnitt einer Beschreibung) erfüllen, um als wahr bewertet zu werden.
   - | - der ODER Operator. Ein Knoten muss nur eine Regel auf einer Seite dieses Operators für die Beschreibung (oder den Abschnitt einer Beschreibung) erfüllen, um als wahr bewertet zu werden.

- (und) – Gruppierungsoperatoren. Die Beschreibung wird in einen Unterabschnitt aufgeteilt, der in Klammern steht. Der Abschnitt innerhalb der Klammern wird bewertet, bevor die restliche Beschreibung mit dem Knoten verglichen wird. Gruppen in Klammern können in einer anderen Gruppe in Klammern verschachtelt werden.

  Beispiel 1: Wenn Sie Knoten beschreiben möchten, die zur Technikabteilung gehören, muss die Regel wie folgt aussehen: Abteilung = Technik. Dies wird als Regel0 bezeichnet. Geben Sie dann Regel0 in das Feld "Kurzer Ausdruck" ein.

  Beispiel 2: Wenn Sie eine Gerätegruppe beschreiben möchten, die zur Technikabteilung gehört oder den Standort "Philadelphia" aufweist, und festlegen möchten, dass alle Geräte mindestens über 1 GB Speicher verfügen müssen, dann müssen Sie drei Regeln erstellen. Abteilung = Technik (Regel0) Standort = Philadelphia (Regel1) Speicher = 1GB (Regel2). Diese Regeln müssen in Relation zueinander gesetzt werden. Da das Gerät entweder der Technikabteilung angehören oder den Standort "Philadelphia" aufweisen kann, verwenden Sie den ODER Operator |, um die beiden zu verbinden: Regel0 | Regel1. Lassen Sie diesen Vergleich zuerst durchführen, indem Sie ihn in Klammern einschließen: (Regel0 | Regel1). Da die Geräte beide diesen Vergleich erfüllen UND 1 GB Speicher aufweisen müssen, wird der UND-Operator & verwendet, um diesen Abschnitt mit Regel2 zu verbinden: (Regel0 | Regel1) & Regel2. Geben Sie diesen Ausdruck in das Feld "Kurzer Ausdruck" ein.

Hinweis: Vor und nach den Operatoren muss ein Leerzeichen sowie das Zeichen | vorhanden sein. Andernfalls wird der Wert im Feld "Kurzer Ausdruck" auf den Standardausdruck zurückgesetzt, d. h. Regel0 & Regel1 & Regel2 usw., wenn Sie eine Regel aus der Tabelle löschen.

6. Klicken Sie auf "Überprüfen", wenn eine Beschreibung im Feld "Kurzer Ausdruck" enthalten ist. Wurde die Beschreibung fehlerhaft gebildet, wird ein Warnhinweis angezeigt. Wurde die Beschreibung richtig gebildet, wird eine normalisierte Form des Ausdrucks im Feld "Normalisierter Ausdruck" angezeigt.
7. Klicken Sie auf Knoten anzeigen, um anzuzeigen, welche Knoten diese Anforderungen erfüllen. Ein Ergebnisfenster "Knoten in der Knotengruppe" wird mit den Knoten angezeigt, die durch den aktuellen Ausdruck gruppiert werden. Sie können dadurch prüfen, ob die Beschreibung richtig geschrieben wurde. Ist dies nicht der Fall, können Sie zur Regeltabelle oder dem Feld "Kurzer Ausdruck" wechseln, um Anpassungen vorzunehmen.
8. Wenn Sie wissen, dass Sie eine Richtlinie erstellen möchten, die jederzeit Zugriff auf die Knoten dieser Gruppe erlaubt, markieren Sie das Kontrollkästchen "Richtlinie mit unbeschränktem Zugriff für Gruppe erstellen".

9. Wenn Sie alle Knoten der Gruppe beschrieben haben, klicken Sie auf OK, um die Knotengruppe zu erstellen. Die Gruppe wird der Liste der Knotengruppen links hinzugefügt.

Knotengruppen bearbeiten

Sie können eine Knotengruppe bearbeiten, um die Mitgliedschaft oder Beschreibung der Gruppe zu ändern.

So bearbeiten Sie eine Knotengruppe:

1. Wählen Sie "Zuordnungen > Knotengruppe". Das Fenster "Knotengruppenmanager" wird angezeigt.
2. Klicken Sie in der Knotengruppenliste auf den Knoten, den Sie bearbeiten möchten. Die Details des Knotens werden im Fenster "Knotengruppen" angezeigt.
3. Weitere Informationen zum Konfigurieren von Knotengruppen finden Sie in den Abschnitten "Knoten auswählen" oder "Knoten beschreiben".
4. Klicken Sie zum Speichern der Änderungen auf OK.

Knotengruppen löschen

So löschen Sie eine Knotengruppe:

1. Wählen Sie "Zuordnungen > Knotengruppe". Das Fenster "Knotengruppenmanager" wird angezeigt.
2. Wählen Sie in der Knotengruppenliste links den Knoten aus, den Sie löschen möchten.
3. Wählen Sie "Gruppen > Löschen".
4. Der Fensterbereich "Knotengruppe löschen" wird angezeigt. Klicken Sie auf "Löschen".
5. Klicken Sie in der Bestätigungsmeldung auf "Ja".

Kapitel 9 Benutzer und Benutzergruppen

Benutzerkonten werden erstellt, damit Benutzern ein Benutzername und Kennwort für den Zugriff auf CC-SG zugeordnet werden kann.

Eine "Benutzergruppe" definiert mehrere Berechtigungen für ihre Mitglieder. Sie können nur den Benutzergruppen und nicht den eigentlichen Benutzern Berechtigungen zuordnen. Alle Benutzer müssen mindestens einer Benutzergruppe angehören.

CC-SG verwaltet eine zentralisierte Benutzerliste und Benutzergruppenliste zur Authentifizierung und Autorisierung.

Sie können CC-SG auch so konfigurieren, dass eine externe Authentifizierung verwendet wird. Siehe ***Remoteauthentifizierung*** (auf Seite 225).

Sie müssen außerdem Zugriffsrichtlinien erstellen, die Sie Benutzergruppen zuweisen können. Siehe ***Richtlinien für die Zugriffssteuerung*** (auf Seite 210).

In diesem Kapitel

Registerkarte "Benutzer" 186
Standardbenutzergruppen 187
Benutzergruppen hinzufügen, bearbeiten und löschen 188
Anzahl an KVM-Sitzungen pro Benutzer einschränken 192
Zugriffsüberwachung für Benutzergruppen konfigurieren 193
Benutzer hinzufügen, bearbeiten und löschen 194
Benutzer einer Gruppe zuordnen 197
Benutzer aus einer Gruppe löschen 198
Benutzer per CSV-Dateiimport hinzufügen 198
Ihr Benutzerprofil 206
Benutzer abmelden 207
Massenkopieren von Benutzern 208

Registerkarte "Benutzer"

Klicken Sie auf die Registerkarte "Benutzer", um alle Benutzergruppen und Benutzer in CC-SG anzuzeigen.

Benutzer sind unter den Benutzergruppen angeordnet, denen sie zugewiesen sind. Benutzergruppen mit zugeordneten Benutzern werden in der Liste mit dem Symbol + angezeigt. Klicken Sie auf das Pluszeichen (+), um die Liste ein- oder auszublenden. Aktive Benutzer: Die Benutzer, die zurzeit bei CC-SG angemeldet sind, werden in Fettdruck dargestellt.

Mithilfe der Registerkarte "Benutzer" können Sie in der Struktur nach Benutzern suchen.

Standardbenutzergruppen

In CC-SG sind drei Standardbenutzergruppen konfiguriert: CC-Superuser, Systemadministratoren und CC Users.

Die CC-Superuser-Gruppe

Die CC-Superuser-Gruppe verfügt über alle Verwaltungs- und Zugriffsberechtigungen. Nur ein Benutzer kann Mitglied dieser Gruppe sein. Der Standard-Benutzername lautet `admin`. Sie können den Standard-Benutzernamen ändern. Die CC-Superuser-Gruppe kann nicht gelöscht werden. Sie können die der CC-Superuser-Gruppe zugeordneten Berechtigungen nicht ändern, keine weiteren Mitglieder hinzufügen oder den einzigen Benutzer der Gruppe löschen. Für das Mitglied der CC-Superuser-Gruppe sind immer sichere Kennwörter aktiviert. Die Anforderungen für sichere Kennwörter sind:

- Kennwörter müssen mindestens einen kleingeschriebenen Buchstaben enthalten.
- Kennwörter müssen mindestens einen großgeschriebenen Buchstaben enthalten.
- Kennwörter müssen mindestens eine Zahl enthalten.
- Kennwörter müssen mindestens ein Sonderzeichen (zum Beispiel ein Ausrufezeichen oder kaufmännisches Und) enthalten.

Hinweis: Sie können über den CSV-Dateiimport keine Änderungen an der CC-Superuser-Gruppe vornehmen.

Systemadministratorgruppe

Die Systemadministratorgruppe verfügt über alle Verwaltungs- und Zugriffsberechtigungen. Die Berechtigungen können nicht geändert werden. Sie können Mitglieder hinzufügen oder löschen.

CC Users-Gruppe

Die CC Users-Gruppe verfügt über In-Band- und Out-of-Band-Knotenzugriff. Sie können die Berechtigungen ändern und Mitglieder hinzufügen oder löschen.

Wichtig: Viele Menüelemente können nur ausgewählt werden, wenn zuvor die entsprechende Benutzergruppe oder der Benutzer ausgewählt wurde.

Benutzergruppen hinzufügen, bearbeiten und löschen

Benutzergruppen hinzufügen

Wenn Sie zunächst Benutzergruppen erstellen, können Sie Benutzer beim Hinzufügen einfacher organisieren. Beim Erstellen einer Benutzergruppe wird dieser Benutzergruppe ein Satz an Berechtigungen zugeordnet. Benutzer, die der Gruppe zugeordnet werden, erben diese Berechtigungen. Wenn Sie beispielsweise eine Gruppe erstellen und dieser die Berechtigung "Benutzermanagement" zuweisen, können alle Benutzer dieser Gruppe die Befehle im Menü "Benutzermanager" anzeigen und ausführen. Siehe ***Benutzergruppenberechtigungen*** (auf Seite 421).

Das Konfigurieren von Benutzergruppen umfasst vier Schritte:

- Name und Beschreibung für die Gruppe eingeben
- Berechtigungen für die Benutzergruppe auswählen
- Schnittstellentypen auswählen, die Benutzer für den Zugriff auf Knoten verwenden können
- Richtlinien auswählen, die festlegen, auf welche Knoten die Benutzergruppe zugreifen kann

So fügen Sie eine Benutzergruppe hinzu:

1. Wählen Sie "Benutzer > Benutzergruppenmanager > Benutzergruppe hinzufügen". Das Fenster "Benutzergruppe hinzufügen" wird angezeigt.
2. Geben Sie einen neuen Benutzergruppennamen in das Feld "Benutzergruppenname" ein. Benutzergruppennamen müssen eindeutig sein. Weitere Informationen zu den Regeln, die von CC-SG für die Länge von Namen verwendet werden, finden Sie unter ***Benennungskonventionen*** (siehe "***Benennungsregeln***" auf Seite 457).
3. Geben Sie eine kurze Beschreibung für die Gruppe im Feld "Beschreibung" ein. **Optional.**

4. Um für den Zugriff auf Geräte, auf denen diese Funktion aktiviert ist, eine maximal mögliche Anzahl an KVM-Sitzungen pro Benutzer dieser Benutzergruppe festzulegen, aktivieren Sie das Kontrollkästchen "Limit Number of KVM Sessions per Device" (Einschränken der Anzahl an KVM-Sitzungen pro Gerät) und wählen Sie im Feld "Max KVM Sessions (1-8)" (Max. KVM-Sitzungen (1-8)) die zulässige Anzahl an Sitzungen aus. **Optional.** Weitere Informationen finden Sie unter ***Anzahl an KVM-Sitzungen pro Benutzer einschränken*** (auf Seite 192).
5. Klicken Sie auf die Registerkarte "Berechtigungen".
6. Markieren Sie die Kontrollkästchen für die Berechtigungen, die Sie der Benutzergruppe zuordnen möchten.
7. Unter der Berechtigungstabelle wird der Bereich "Knotenzugriff" mit Berechtigungen für drei Arten des Knotenzugriffs angezeigt: Out-of-Band-Zugriff für Knoten, In-Band-Zugriff für Knoten und Stromversorgungssteuerung für Knoten. Markieren Sie das Kontrollkästchen für die Art des Knotenzugriffs, die Sie der Benutzergruppe zuordnen möchten.
8. Klicken Sie auf die Registerkarte "Geräte-/Knotenrichtlinien". Eine Tabelle mit Richtlinien wird angezeigt.

   In der Tabelle "Alle Richtlinien" werden alle Richtlinien für CC-SG angezeigt. Jede Richtlinie stellt eine Regel dar, die den Zugriff auf eine Knotengruppe zulässt oder verweigert. Ausführliche Informationen zu Richtlinien und deren Erstellung finden Sie unter ***Richtlinien für die Zugriffssteuerung*** (auf Seite 210).
9. Wählen Sie in der Liste "Alle Richtlinien" die Richtlinie aus, die Sie der Benutzergruppe zuweisen möchten, und klicken Sie auf "Hinzufügen", um die Richtlinie in die Liste "Ausgewählte Richtlinien" zu verschieben. Richtlinien in der Liste "Ausgewählte Richtlinien" gewähren oder verweigern den Zugriff auf die Knoten oder Geräte, die durch die Richtlinie gesteuert werden. Weitere Informationen zur Interaktion von Richtlinien finden Sie unter ***Richtlinien Benutzergruppen zuordnen*** (auf Seite 215).

   Wiederholen Sie diesen Schritt, um der Benutzergruppe weitere Richtlinien zuzuweisen.

   - Wenn Sie dieser Gruppe den Zugriff auf alle verfügbaren Knoten gewähren möchten, wählen Sie in der Liste "Alle Richtlinien" die Option "Richtlinie mit unbeschränktem Zugriff" aus, und klicken Sie auf "Hinzufügen".
   - Wählen Sie zum Löschen einer Richtlinie in der Benutzergruppe den Namen der Richtlinie in der Liste "Ausgewählte Richtlinien" aus, und klicken Sie auf "Löschen".

10. Wenn Sie die Konfiguration der Richtlinien für diese Gruppe abgeschlossen haben, klicken Sie zum Speichern dieser Gruppe und Erstellen einer weiteren auf "Übernehmen". Wiederholen Sie die Schritte in diesem Abschnitt, um Benutzergruppen hinzuzufügen. **Optional.**
11. Klicken Sie zum Speichern der Änderungen auf OK.

Benutzergruppen bearbeiten

Bearbeiten Sie eine Benutzergruppe, um die vorhandenen Berechtigungen und Richtlinien der Gruppe zu ändern.

Hinweis: Sie können die Berechtigungen oder Richtlinien der CC-Superuser-Gruppe nicht bearbeiten.

So bearbeiten Sie eine Benutzergruppe:

1. Klicken Sie auf die Registerkarte "Benutzer".
2. Klicken Sie auf der Registerkarte "Benutzer" auf eine Benutzergruppe. Das Benutzergruppenprofil wird angezeigt.
3. Geben Sie einen neuen Benutzergruppennamen in das Feld "Benutzergruppenname" ein. **Optional.**
4. Geben Sie eine neue Beschreibung für diese Benutzergruppe in das Feld "Beschreibung" ein. **Optional.**
5. Um für den Zugriff auf Geräte, auf denen diese Funktion aktiviert ist, eine maximal mögliche Anzahl an KVM-Sitzungen pro Benutzer dieser Benutzergruppe festzulegen, aktivieren Sie das Kontrollkästchen "Limit Number of KVM Sessions per Device" (Einschränken der Anzahl an KVM-Sitzungen pro Gerät) und wählen Sie im Feld "Max KVM Sessions (1-8)" (Max. KVM-Sitzungen (1-8)) die zulässige Anzahl an Sitzungen aus. **Optional.** Weitere Informationen finden Sie unter ***Anzahl an KVM-Sitzungen pro Benutzer einschränken*** (auf Seite 192).
6. Klicken Sie auf die Registerkarte "Berechtigungen".
7. Markieren Sie die Kontrollkästchen für die Berechtigungen, die Sie der Benutzergruppe zuordnen möchten. Heben Sie die Markierung einer Berechtigung auf, um sie aus der Gruppe zu entfernen.
8. Klicken Sie im Bereich "Knotenzugriff" auf das Dropdown-Menü jeder Schnittstelle, über die diese Gruppe zugreifen darf, und wählen Sie "Steuerung" aus.
9. Klicken Sie auf das Dropdown-Menü jeder Schnittstelle, über die diese Gruppe nicht zugreifen darf, und wählen Sie "Ablehnen" aus.
10. Klicken Sie auf die Registerkarte "Richtlinien". Es werden zwei Tabellen mit Richtlinien angezeigt.

11. Wählen Sie jede Richtlinie, die Sie der Gruppe hinzufügen möchten, unter "Alle Richtlinien" aus, und klicken Sie auf "Hinzufügen", um sie in die Liste "Ausgewählte Richtlinien" zu verschieben. Mithilfe von Richtlinien in der Liste "Ausgewählte Richtlinien" erhalten Benutzer Zugriff auf den Knoten (oder auf Geräte), die durch diese Richtlinie gesteuert werden, oder der Zugriff wird verweigert.
12. Wählen Sie zum Löschen einer Richtlinie aus der Benutzergruppe den Namen der Richtlinie in der Liste "Ausgewählte Richtlinien" aus, und klicken Sie auf "Entfernen".
13. Klicken Sie zum Speichern der Änderungen auf OK.

Benutzergruppen löschen

Sie können eine Benutzergruppe löschen, wenn sie keine Mitglieder enthält.

So löschen Sie eine Benutzergruppe:

1. Klicken Sie auf die Registerkarte "Benutzer".
2. Klicken Sie auf die Benutzergruppe, die Sie löschen möchten.
3. Wählen Sie "Benutzer > Benutzergruppenmanager > Benutzergruppe löschen".
4. Klicken Sie zum Löschen der Benutzergruppe auf OK.

Anzahl an KVM-Sitzungen pro Benutzer einschränken

Sie können die Anzahl an zulässigen KVM-Sitzungen pro Benutzer für Sitzungen mit Dominion KXII-, KSXII- und KX (KX1)-Geräten begrenzen. Dadurch wird verhindert, dass einzelne Benutzer alle verfügbaren Kanäle gleichzeitig verwenden.

Wenn ein Benutzer eine Verbindung zu einem Knoten herstellen möchte, durch die die maximal zulässige Anzahl überschritten würde, wird eine Warnmeldung mit Informationen zu den aktuellen Sitzungen angezeigt. Das Ereignis wird im Zugriffsbericht unter der Meldung *Connection Denied* (Verbindung nicht hergestellt) protokolliert. Bevor eine weitere neue Sitzung begonnen werden kann, muss der Benutzer eine Sitzung auf dem Gerät beenden.

Vollständiger Meldungstext:

Connection Denied: Exceeds the allotted number of sessions for the KVM switch this node is attached to. If possible, please disconnect an existing session to the same KVM switch (Verbindung nicht hergestellt: Die zugewiesene Anzahl an Sitzungen für den KVM-Switch, mit dem dieser Knoten verbunden ist, wurde überschritten. Trennen Sie nach Möglichkeit eine vorhandene Sitzung über denselben KVM-Switch).

Die Meldung enthält eine Liste der aktiven Verbindungen zum KVM-Switch.

Hinweis: Sie können den Zugriffsbericht nach Meldungstext filtern, um festzustellen, welche Geräte über hohen Datenverkehr verfügen. Siehe **Zugriffsbericht** *(auf Seite 252).*

Beschränkungen der Anzahl an KVM-Sitzungen werden pro Benutzergruppe festgelegt. Sie können Beschränkungen beim manuellen Hinzufügen oder Bearbeiten von Benutzergruppen, über den Setup-Assistenten oder per CSV-Import aktivieren. Siehe ***Benutzergruppen hinzufügen*** (auf Seite 188).

NUR bei Dominion KXII-Geräten: Diese Geräte geben außerdem eine Warnung aus, wenn die maximale Anzahl an Verbindungen für das Gerät erreicht wurde. Das Ereignis wird im Zugriffsbericht unter der Meldung *Connection Denied* (Verbindung nicht hergestellt) protokolliert.

Vollständiger Meldungstext:

Connection Denied: Exceeds the number of available video channels on the KVM switch this node is attached to. (Verbindung nicht hergestellt: Die zugewiesene Anzahl an Videokanälen für den KVM-Switch, mit dem dieser Knoten verbunden ist, wurde überschritten).

Zugriffsüberwachung für Benutzergruppen konfigurieren

Sie können festlegen, dass die Mitglieder einer Benutzergruppe den Grund für den Zugriff auf den Knoten angeben müssen, bevor ihnen Zugriff gestattet wird. Allen Benutzern der Benutzergruppe, die Sie auswählen, wird ein Dialogfeld angezeigt. Benutzer müssen den Grund für den Zugriff eingeben, bevor eine Verbindung zum Knoten hergestellt wird. Diese Funktion gilt für alle Arten von Zugriff mit allen Schnittstellentypen, einschließlich der Stromversorgungssteuerung.

Der Grund für den Zugriff wird in der Überwachungsliste und auf der Registerkarte "Überwachung" des Knotenprofils protokolliert.

So konfigurieren Sie die Zugriffsüberwachung für Benutzergruppen:

1. Wählen Sie "Benutzer > Knotenüberwachung".
2. Markieren Sie das Kontrollkästchen "Benutzer müssen beim Zugriff auf einen Knoten Zugriffsinformationen eingeben".
3. Geben Sie im Feld "Meldung an Benutzer" eine Meldung ein, die Benutzern angezeigt wird, wenn sie auf einen Knoten zuzugreifen versuchen. Es wird eine Standardmeldung bereitgestellt. Maximal 256 Zeichen.
4. Verschieben Sie die Benutzergruppen durch Klicken auf die Pfeilschaltflächen in die Liste "Ausgewählt", um die Zugriffsüberwachung für die Gruppen zu aktivieren. Klicken Sie bei gedrückter Strg-Taste, um mehrere Elemente auszuwählen.

   Tipp: Geben Sie den Namen einer Benutzergruppe im Feld "Benutzergruppe suchen" ein, um sie in der Liste zu markieren. Geben Sie ein Sternchen (*) hinter einem Teilnamen ein, um alle ähnlichen Namen in der Liste zu markieren.

   Klicken Sie auf die Spaltenüberschriften, um die Listen alphabetisch zu sortieren.

5. Klicken Sie auf "Aktualisieren".

Benutzer hinzufügen, bearbeiten und löschen

Benutzer hinzufügen

Wenn Sie zu CC-SG einen Benutzer hinzufügen, müssen Sie eine Benutzergruppe festlegen, um dem Benutzer die Zugriffsberechtigungen zu geben, die der Benutzergruppe zugeordnet sind.

So fügen Sie einen Benutzer hinzu:

1. Wählen Sie auf der Registerkarte "Benutzer" die Gruppe aus, zu der Sie einen Benutzer hinzufügen möchten.
2. Wählen Sie "Benutzer > Benutzermanager > Benutzer hinzufügen".
3. Geben Sie im Feld "Benutzername" den Benutzernamen des Benutzer ein, der hinzugefügt werden soll. Dieser Name wird für die Anmeldung bei CC-SG verwendet. Weitere Informationen zu den Regeln, die von CC-SG für die Länge von Namen verwendet werden, finden Sie unter ***Benennungskonventionen*** (siehe "***Benennungsregeln***" auf Seite 457).
4. Geben Sie im Feld "Vollständiger Name" den vollständigen Vor- und Nachnamen des Benutzers ein. Weitere Informationen zu den Regeln, die von CC-SG für die Länge von Namen verwendet werden, finden Sie unter ***Benennungskonventionen*** (siehe "***Benennungsregeln***" auf Seite 457).
5. Markieren Sie das Kontrollkästchen "Anmeldung aktiviert", wenn der Benutzer über die Anmeldeberechtigung für CC-SG verfügen soll.
6. Markieren Sie das Kontrollkästchen "Remoteauthentifizierung" nur, wenn der Benutzer mithilfe eines externen Servers wie TACACS+, RADIUS, LDAP oder AD authentifiziert werden soll. Wenn Sie die Remoteauthentifizierung verwenden, benötigen Sie kein Kennwort, und die Felder "Neues Kennwort" und "Neues Kennwort erneut eingeben" sind deaktiviert.
7. Geben Sie in die Felder "Neues Kennwort" und "Neues Kennwort erneut eingeben" das Kennwort ein, das der Benutzer zur Anmeldung in CC-SG verwenden soll.

Hinweis: Weitere Informationen zu den Regeln, die von CC-SG für die Länge von Namen verwendet werden, finden Sie unter **Benennungskonventionen** *(siehe "***Benennungsregeln***" auf Seite 457).*

Sind sichere Kennwörter aktiviert, muss das eingegebene Kennwort den definierten Regeln entsprechen. In der Informationszeile oben im Bildschirm wird eine Nachricht mit den Kennwortanforderungen angezeigt. Ausführliche Informationen zu sicheren Kennwörtern finden Sie unter **Erweiterte Administration** *(auf Seite 282).*

8. Markieren Sie das Kontrollkästchen "Änderung des Kennworts bei der nächsten Anmeldung erzwingen", wenn der Benutzer gezwungen werden soll, das zugewiesene Kennwort bei der nächsten Anmeldung zu ändern.
9. Markieren Sie das Kontrollkästchen "Änderung des Kennworts periodisch erzwingen", wenn Sie festlegen möchten, wie oft der Benutzer zur Kennwortänderung gezwungen werden soll.
10. Falls das Feld "Gültigkeitsdauer (in Tagen)" markiert ist, geben Sie die Anzahl von Tagen ein, die der Benutzer dasselbe Kennwort verwenden kann, bevor eine Änderung erzwungen wird.
11. Geben Sie die E-Mail-Adresse des Benutzers in das Feld "E-Mail-Adresse" ein. Sie wird zum Senden der Benutzerbenachrichtigungen verwendet.
12. Geben Sie in das Feld "Telefonnummer" die Telefonnummer des Benutzers ein.
13. Klicken Sie auf das Dropdown-Menü "Benutzergruppen", und wählen Sie die Gruppe aus, zu der der Benutzer hinzugefügt wird.
    - Abhängig von der ausgewählten Benutzergruppe, kann das Kontrollkästchen "Benutzer muss beim Zugriff auf einen Knoten Zugriffsinformationen eingeben" markiert sein oder nicht. Ist dieses Kontrollkästchen markiert, muss der Benutzer beim Zugriff auf einen Knoten die entsprechenden Informationen eingeben. Siehe ***Zugriffsüberwachung für Benutzergruppen konfigurieren*** (auf Seite 193).
14. Wenn Sie die Konfiguration dieses Benutzers abgeschlossen haben, klicken Sie auf "Übernehmen", um diesen Benutzer hinzuzufügen und einen weiteren zu erstellen. Sie können auch auf OK klicken, um den Benutzer hinzuzufügen ohne weitere zu erstellen. Die erstellten Benutzer werden auf der Registerkarte "Benutzer" unter den Benutzergruppen angezeigt, denen sie zugewiesen sind.

Benutzer bearbeiten

Durch das Bearbeiten eines Benutzers können Sie die Gruppe, der dieser Benutzer angehört, nicht ändern. Siehe ***Benutzer einer Gruppe zuordnen*** (auf Seite 197).

So bearbeiten Sie einen Benutzer:

1. Klicken Sie auf der Registerkarte "Benutzer" auf das Pluszeichen (+), um die Benutzergruppe einzublenden, die einen Benutzer enthält, den Sie bearbeiten möchten. Wählen Sie dann den Benutzer aus. Das Benutzerprofil wird angezeigt.
2. Deaktivieren Sie das Kontrollkästchen "Anmeldung aktiviert", damit sich dieser Benutzer nicht an CC-SG anmelden kann. Aktivieren Sie das Kontrollkästchen "Anmeldung aktiviert", damit sich dieser Benutzer an CC-SG anmelden kann.

3. Markieren Sie das Kontrollkästchen "Remoteauthentifizierung" nur, wenn der Benutzer mithilfe eines externen Servers wie TACACS+, RADIUS, LDAP oder AD authentifiziert werden soll. Wenn Sie die Remoteauthentifizierung verwenden, benötigen Sie kein Kennwort, und die Felder "Neues Kennwort" und "Neues Kennwort erneut eingeben" sind deaktiviert.
4. Geben Sie in die Felder "Neues Kennwort" und "Neues Kennwort erneut eingeben" ein neues Kennwort ein, um das Benutzerkennwort zu ändern.

   Hinweis: Sind sichere Kennwörter aktiviert, muss das eingegebene Kennwort den definierten Regeln entsprechen. In der Informationszeile oben im Bildschirm werden die Kennwortanforderungen angezeigt. Ausführliche Informationen zu sicheren Kennwörtern finden Sie unter **Erweiterte Administration** *(auf Seite 282).*

5. Markieren Sie das Kontrollkästchen "Änderung des Kennworts bei der nächsten Anmeldung erzwingen", wenn der Benutzer gezwungen werden soll, das zugewiesene Kennwort bei der nächsten Anmeldung zu ändern.
6. Geben Sie in das Feld "E-Mail-Adresse" eine neue E-Mail-Adresse ein, um die vom Benutzer konfigurierte E-Mail-Adresse hinzuzufügen oder zu ändern. Sie wird zum Senden der Benutzerbenachrichtigungen verwendet.
7. Klicken Sie zum Speichern der Änderungen auf OK.

Benutzer löschen

Wenn Sie einen Benutzer löschen, wird dieser Benutzer aus CC-SG entfernt. Sie können dadurch Benutzerkonten löschen, die nicht mehr benötigt werden.

Dieser Vorgang löscht alle Instanzen des Benutzers. Dies gilt auch, wenn der Benutzer mehreren Benutzergruppen angehört. Informationen zum Entfernen von Benutzern aus einer Gruppe, ohne die Benutzer aus CC-SG zu löschen, finden Sie unter ***Benutzer aus einer Gruppe löschen*** (auf Seite 198).

So löschen Sie einen Benutzer:

1. Klicken Sie auf der Registerkarte "Benutzer" auf das Pluszeichen (+), um die Benutzergruppe einzublenden, die einen Benutzer enthält, den Sie löschen möchten. Wählen Sie dann den Benutzer aus. Das Benutzerprofil wird angezeigt.
2. Wählen Sie "Benutzer > Benutzermanager > Benutzer löschen".
3. Klicken Sie auf OK, um den Benutzer dauerhaft aus CC-SG zu löschen.

Benutzer einer Gruppe zuordnen

Verwenden Sie diesen Befehl, um einen vorhandenen Benutzer einer anderen Gruppe zuzuweisen. Benutzer, die auf diese Art und Weise zugeordnet werden, werden der neuen Gruppe hinzugefügt und sind weiterhin Mitglieder ihrer bereits bestehenden Gruppen. Sie können einen Benutzer mit diesem Befehl in Verbindung mit "Benutzer aus Gruppe löschen" verschieben.

So ordnen Sie einen Benutzer einer Gruppe zu:

1. Wählen Sie auf der Registerkarte "Benutzer" die Benutzergruppe aus, der Sie Benutzer zuordnen möchten.
2. Wählen Sie "Benutzer > Benutzergruppenmanager > Benutzer der Gruppe zuweisen".
3. Die ausgewählte Benutzergruppe wird im Feld "Benutzergruppenname" angezeigt.
4. Benutzer, die keiner Zielgruppe zugewiesen werden, werden in der Liste Benutzer nicht in Gruppe angezeigt.
   - Wählen Sie die Benutzer aus, die Sie von dieser Liste hinzufügen möchten, und klicken Sie dann auf >, um die Benutzer in die Liste "Benutzer in Gruppe" zu verschieben.
   - Klicken Sie auf die Schaltfläche >>, um alle Benutzer, die sich nicht in der Gruppe befinden, in die Liste "Benutzer in Gruppe" zu verschieben.
   - Wählen Sie die Benutzer aus, die Sie aus der Liste "Benutzer in Gruppe" entfernen möchten, und klicken Sie auf die Schaltfläche <, um sie zu entfernen.
   - Klicken Sie auf die Schaltfläche <<, um alle Benutzer aus der Liste "Benutzer in Gruppe" zu entfernen.
5. Wenn Sie alle Benutzer in die entsprechenden Spalten verschoben haben, klicken Sie auf OK. Die Benutzer in der Liste Benutzer in Gruppen werden zur ausgewählten Benutzergruppe hinzugefügt.

Benutzer aus einer Gruppe löschen

Wenn Sie einen Benutzer aus einer Gruppe löschen, wird der Benutzer nur aus der festgelegten Gruppe entfernt. Der Benutzer bleibt in allen anderen zugeordneten Gruppen. Durch das Löschen eines Benutzers aus einer Gruppe wird der Benutzer nicht aus CC-SG gelöscht.

Wenn ein Benutzer nur zu einer Gruppe gehört, können Sie den Benutzer nicht aus der Gruppe löschen. Sie können den Benutzer nur aus CC-SG löschen.

So löschen Sie einen Benutzer in einer Gruppe:

1. Klicken Sie auf der Registerkarte "Benutzer" auf das Pluszeichen (+), um die Benutzergruppe einzublenden, die den Benutzer enthält, den Sie aus der Gruppe löschen möchten. Wählen Sie dann den Benutzer aus. Das Benutzerprofil wird angezeigt.
2. Wählen Sie "Benutzer > Benutzermanager > Benutzer aus Gruppe löschen". Das Fenster "Benutzer löschen" **wird angezeigt.**
3. Klicken Sie zum Löschen des Benutzers aus der Gruppe auf OK.

Benutzer per CSV-Dateiimport hinzufügen

Sie können Benutzerinformationen zu CC-SG hinzufügen, indem Sie eine CSV-Datei, in der die Werte enthalten sind, importieren.

Wenn in einer Umgebung mehrere CC-SG-Einheiten vorhanden sind, können Sie durch das Exportieren von Benutzern von einer CC-SG-Einheit und Importieren auf eine andere CC-SG-Einheit schnell sicherstellen, dass alle lokal authentifizierten Benutzer auf beiden Mitgliedern präsent sind.

Sie benötigen die Berechtigungen "Benutzerverwaltung" und "CC-Setup und -Steuerung", um Benutzerinformationen importieren bzw. exportieren zu können.

Anforderungen an CSV-Dateien – Benutzer

Durch den Import können Sie Benutzergruppen, Benutzer und AD-Module hinzufügen sowie Richtlinien, Berechtigungen und Benutzergruppen zuweisen.

- Richtlinien müssen bereits in CC-SG erstellt worden sein. Durch den Import wird die Richtlinie einer Benutzergruppe zugewiesen. Über den Import können Sie keine neuen Richtlinien erstellen.
- Bei Benutzergruppennamen wird zwischen Groß- und Kleinschreibung unterschieden.
- Bei der Angabe von Benutzernamen spielt die Groß-/Kleinschreibung keine Rolle.
- Für jede definierte USERGROUP (Benutzergruppe) muss in der CSV-Datei jeweils ein Tag für USERGROUP-PERMISSIONS (Benutzergruppenberechtigungen) und USERGROUP-POLICY (Benutzergruppenrichtlinie) definiert werden, um die Benutzergruppe erstellen zu können.
- Exportieren Sie eine Datei aus CC-SG, um die Kommentare anzuzeigen. Diese enthalten alle Tags und Parameter, die zum Erstellen einer gültigen CSV-Datei erforderlich sind. Siehe ***Benutzer exportieren*** (auf Seite 205).
- Erfüllen Sie die zusätzlichen Anforderungen für alle CSV-Dateien. Siehe ***Häufige Anforderungen an CSV-Dateien*** (siehe "***Häufige Anforderungen für CSV-Dateien***" auf Seite 434).

So fügen Sie eine Benutzergruppe zur CSV-Datei hinzu:

Spaltennummer	Tag oder Wert	Details
1	`ADD (Hinzufügen)`	Die erste Spalte für alle Tags ist der Befehl `ADD` (Hinzufügen).
2	`USERGROUP (Benutzergruppe)`	Geben Sie das Tag wie beschrieben ein. Bei Tags wird die Groß- und Kleinschreibung nicht berücksichtigt.
3	Benutzergruppenname	Erforderliches Feld. Bei Benutzergruppennamen wird zwischen Groß- und Kleinschreibung unterschieden.
4	Beschreibung	Erforderliches Feld.
5	Max. Anzahl an KVM-Sitzungen pro Gerät einschränken	`TRUE` (Wahr) oder `FALSE` (Falsch) Der Standardwert ist `FALSE` (Falsch).

Spaltennummer	Tag oder Wert	Details
6	Maximal zulässige Anzahl an KVM-Sitzungen pro Benutzer	Geben Sie nur die Anzahl ein. Der Wert kann zwischen `1-8` liegen. Der Standardwert ist `2`.

So weisen Sie einer Benutzergruppe in der CSV-Datei Berechtigungen zu:

Geben Sie den Wert TRUE (Wahr) ein, um der Benutzergruppe eine Berechtigung zuzuweisen. Geben Sie den Wert FALSE (Falsch) ein, um der Benutzergruppe die Berechtigung nicht zuzuweisen.

Spaltennummer	Tag oder Wert	Details
1	`ADD (Hinzufügen)`	Die erste Spalte für alle Tags ist der Befehl `ADD` (Hinzufügen).
2	`USERGROUP-PERMISSIONS (Benutzergruppenberechtigungen)`	Geben Sie das Tag wie beschrieben ein. Bei Tags wird die Groß- und Kleinschreibung nicht berücksichtigt.
3	Benutzergruppenname	Erforderliches Feld. Bei Benutzergruppennamen wird zwischen Groß- und Kleinschreibung unterschieden.
4	CC Setup And Control	`TRUE` (Wahr) oder `FALSE` (Falsch)
5	Gerätekonfiguration – Aktualisierungsverwaltung	`TRUE` (Wahr) oder `FALSE` (Falsch)
6	Geräte-, Port- und Knotenverwaltung	`TRUE` (Wahr) oder `FALSE` (Falsch)
7	Benutzerverwaltung	`TRUE` (Wahr) oder `FALSE` (Falsch)
8	User Security Management	`TRUE` (Wahr) oder `FALSE` (Falsch)
9	Knoten IBA	`TRUE` (Wahr) oder `FALSE` (Falsch) Die Standardeinstellung ist `TRUE` (Wahr).
10	Knoten OOB	`TRUE` (Wahr) oder `FALSE` (Falsch) Die Standardeinstellung ist `TRUE` (Wahr).
11	Knoten Stromversorgung	`TRUE` (Wahr) oder `FALSE` (Falsch)

So weisen Sie einer Benutzergruppe in der CSV-Datei eine Richtlinie zu:

Spaltennummer	Tag oder Wert	Details
1	`ADD (Hinzufügen)`	Die erste Spalte für alle Tags ist der Befehl `ADD` (Hinzufügen).
2	`USERGROUP-POLICY (Benutzergruppenrichtlinie)`	Geben Sie das Tag wie beschrieben ein. Bei Tags wird die Groß- und Kleinschreibung nicht berücksichtigt.
3	Benutzergruppenname	Erforderliches Feld. Bei Benutzergruppennamen wird zwischen Groß- und Kleinschreibung unterschieden.
4	Richtlinienname	Erforderliches Feld.

So weisen Sie einer Benutzergruppe in der CSV-Datei ein AD-Modul zu:

Spaltennummer	Tag oder Wert	Details
1	`ADD (Hinzufügen)`	Die erste Spalte für alle Tags ist der Befehl `ADD` (Hinzufügen).
2	`USERGROUP-ADMODULE (Benutzergruppe – AD-Modul)`	Geben Sie das Tag wie beschrieben ein. Bei Tags wird die Groß- und Kleinschreibung nicht berücksichtigt.
3	Benutzergruppenname	Erforderliches Feld. Bei Benutzergruppennamen wird zwischen Groß- und Kleinschreibung unterschieden.
4	AD-Modulname	Erforderliches Feld.

So fügen Sie einen Benutzer zu CC-SG hinzu:

Spaltennummer	Tag oder Wert	Details
1	`ADD (Hinzufügen)`	Die erste Spalte für alle Tags ist der Befehl `ADD` (Hinzufügen).
2	`USER (Benutzer)`	Geben Sie das Tag wie beschrieben ein.

Spaltennummer	Tag oder Wert	Details
		Bei Tags wird die Groß- und Kleinschreibung nicht berücksichtigt.
3	Benutzergruppenname	Erforderliches Feld. Bei Benutzergruppennamen wird zwischen Groß- und Kleinschreibung unterschieden. Sie müssen den Benutzer zu einer Benutzergruppe hinzufügen. Mit dem Tag USERGROUP-MEMBER (Benutzergruppenmitglied) können Sie den Benutzer zu mehreren Benutzergruppen hinzufügen.
4	Benutzername	Erforderliches Feld.
5	Kennwort	Erforderliches Feld.
6	Vollständiger Name des Benutzers	Optional.
7	E-Mail-Adresse	Optional. Die E-Mail-Adresse wird für Systembenachrichtigungen verwendet.
8	Telefonnummer	Optional.
9	Anmeldung aktiviert	`TRUE` (Wahr) oder `FALSE` (Falsch) Die Standardeinstellung ist `TRUE` (Wahr). Aktivieren Sie die Anmeldung, damit sich der Benutzer bei CC-SG anmelden kann.
10	Remoteauthentifizierung	`TRUE` (Wahr) oder `FALSE` (Falsch)
11	Änderung des Kennworts periodisch erzwingen	`TRUE` (Wahr) oder `FALSE` (Falsch)
12	Gültigkeitsdauer	Wenn die Option "Änderung des Kennworts periodisch erzwingen" auf TRUE (Wahr) festgelegt ist, geben Sie die Anzahl an Tagen an, nach deren Ablauf das Kennwort geändert werden muss. Geben Sie nur die Anzahl ein. Der Wert kann zwischen `1` und `365` liegen.

So fügen Sie einen Benutzer zu einer Benutzergruppe hinzu:

Spaltennummer	Tag oder Wert	Details
1	`ADD (Hinzufügen)`	Die erste Spalte für alle Tags ist der Befehl `ADD` (Hinzufügen).
2	`USERGROUP-MEMBER (Benutzergruppenmitglied)`	Geben Sie das Tag wie beschrieben ein. Bei Tags wird die Groß- und Kleinschreibung nicht berücksichtigt.
3	Benutzergruppenname	Erforderliches Feld. Bei Benutzergruppennamen wird zwischen Groß- und Kleinschreibung unterschieden.
4	Benutzername	Erforderliches Feld.

Beispiel-CSV-Datei für Benutzer

ADD (Hinzufügen), USERGROUP (Benutzergruppe), Windows-Administratoren, MS-IT-Team

ADD (Hinzufügen), USERGROUP-PERMISSIONS (Benutzergruppenberechtigungen), Windows-Administratoren, FALSE (Falsch), TRUE (Wahr), TRUE (Wahr), TRUE (Wahr), TRUE (Wahr), TRUE (Wahr), TRUE (Wahr), TRUE (Wahr)

ADD (Hinzufügen), USERGROUP-POLICY (Benutzergruppenrichtlinie), Windows-Administratoren, Richtlinie mit unbeschränktem Zugriff

ADD (Hinzufügen), USERGROUP-ADMODULE (Benutzergruppe – AD-Modul), Windows-Administratoren, AD-USA-57-120

ADD (Hinzufügen), USERGROUP-MEMBER (Benutzergruppenmitglied), Windows-Administratoren, user1

ADD (Hinzufügen), USERGROUP-MEMBER (Benutzergruppenmitglied), Windows-Administratoren, user2

ADD (Hinzufügen), USER (Benutzer), Windows-Administratoren, user1, password, userfirstname userlastname, user1@company.com, 800-555-1212, TRUE (Wahr),,,

ADD (Hinzufügen), USER (Benutzer), Windows-Administratoren, user2, password, userfirstname userlastname, user2@raritan.com, 800-555-1212, TRUE (Wahr),,,

ADD (Hinzufügen), USERGROUP-MEMBER (Benutzergruppenmitglied), Systemadministratoren, user1

ADD (Hinzufügen), USERGROUP-MEMBER (Benutzergruppenmitglied), CC-Benutzer, user2

Benutzer importieren

Wenn Sie die CSV-Datei erstellt haben, überprüfen Sie sie auf Fehler und importieren Sie sie anschließend.

Doppelte Einträge werden übersprungen und somit nicht hinzugefügt.

1. Wählen Sie "Administration > Importieren > Benutzer importieren".
2. Klicken Sie auf "Durchsuchen" und wählen Sie die zu importierende CSV-Datei aus. Klicken Sie auf "Öffnen".
3. Klicken Sie auf Überprüfen. Die Dateiinhalte werden im Bereich "Analysebericht" angezeigt.

- Wenn die Datei ungültig ist, wird eine Fehlermeldung angezeigt. Klicken Sie auf "OK". Im Bereich "Probleme" auf der Seite wird eine Beschreibung der Dateiprobleme aufgeführt. Klicken Sie auf "In Datei speichern", um die Liste der Probleme zu speichern. Korrigieren Sie die CSV-Datei und versuchen Sie sie anschließend erneut zu validieren. Siehe ***Problembehebung bei CSV-Dateien*** (auf Seite 436).

4. Klicken Sie auf "Importieren".
5. Die Ergebnisse des Imports werden im Bereich "Aktionen" angezeigt. Erfolgreich importierte Elemente werden grün dargestellt. Nicht erfolgreich importierte Elemente werden rot dargestellt. Elemente, die aufgrund eines bereits vorhandenen oder bereits importierten Duplikats nicht erfolgreich importiert wurden, werden ebenso rot dargestellt.
6. Um weitere Details zu den Importergebnissen anzuzeigen, rufen Sie den Überwachungslistenbericht auf. Siehe ***Einträge in der Überwachungsliste für Importe*** (auf Seite 435).

Benutzer exportieren

In der Exportdatei sind alle Benutzer enthalten, die über ein in CC-SG erstelltes Benutzerkonto verfügen. Davon ausgenommen sind AD-authorisierte Benutzer, es sei denn, sie verfügen ebenso über ein in CC-SG erstelltes Benutzerkonto.

In der Exportdatei sind Benutzer sowie die Informationen des Benutzerprofils, Benutzergruppen, Benutzergruppenberechtigungen und -richtlinien sowie zugewiesene AD-Module enthalten.

Kennwörter werden als leere Felder exportiert.

So exportieren Sie Benutzer:

1. Wählen Sie "Administration > Exportieren > Benutzer exportieren".
2. Klicken Sie auf "In Datei exportieren".
3. Geben Sie einen Namen für die Datei ein, und wählen Sie den Speicherort aus.
4. Klicken Sie auf Speichern.

Ihr Benutzerprofil

Unter "Mein Profil" können Benutzer Kontoinformationen anzeigen, einige Details ändern und die Einstellungen zur Verwendung anpassen. Dies ist die einzige Möglichkeit für das CC-Superuser-Konto, den Kontonamen zu ändern.

So zeigen Sie Ihr Profil an:

Wählen Sie "Secure Gateway > Mein Profil". Der Bildschirm "Mein Profil" wird mit Informationen zu Ihrem Konto angezeigt.

Eigenes Kennwort ändern

1. Wählen Sie "Secure Gateway > Mein Profil".
2. Aktivieren Sie das Kontrollkästchen "Kennwort ändern (nur lokale Authentifizierung)".
3. Geben Sie das aktuelle Kennwort im Feld "Altes Kennwort" ein.
4. Geben Sie das neue Kennwort im Feld "Neues Kennwort" ein. Eine Meldung wird angezeigt, wenn sichere Kennwörter erforderlich sind.
5. Bestätigen Sie das neue Kennwort im Feld "Neues Kennwort" erneut eingeben.
6. Klicken Sie zum Speichern der Änderungen auf OK.

Eigenen Namen ändern

Sie können Ihren Benutzernamen nicht ändern. Sie können den Ihrem Benutzernamen zugewiesenen Vor- und Nachnamen ändern.

So ändern Sie Ihren Namen:

1. Wählen Sie "Secure Gateway > Mein Profil".
2. Geben Sie Ihren Vor- und Nachnamen in das Feld "Vollständiger Name" ein. Weitere Informationen zu den Regeln, die von CC-SG für die Länge von Namen verwendet werden, finden Sie unter ***Benennungskonventionen*** (siehe "***Benennungsregeln***" auf Seite 457).

Eigene Standardsucheinstellungen ändern

1. Wählen Sie "Secure Gateway > Mein Profil".
2. Wählen Sie im Bereich "Sucheinstellungen" eine bevorzugte Methode zur Suche nach Knoten, Benutzern und Geräten aus:
   - Nach Suchergebnissen filtern: Benutzer können Platzhalter verwenden und nur die Knoten, Benutzer oder Geräte anzeigen, die den Suchkriterien entsprechen.

- Übereinstimmungen suchen: Unterstützt keine Platzhalter, und die ähnlichste Entsprechung für Knoten, Benutzer oder Geräte wird beim Eingeben angezeigt. Die Liste ist auf die Elemente beschränkt, die nach Klicken auf Suchen den Suchkriterien entsprechen.

3. Klicken Sie zum Speichern der Änderungen auf OK.

Standardschriftgrad für CC-SG ändern

1. Wählen Sie "Secure Gateway > Mein Profil".
2. Klicken Sie auf das Dropdown-Menü "Schriftgrad", um den Schriftgrad anzupassen, den der Standard-CC-SG-Client verwendet.
3. Klicken Sie zum Speichern der Änderungen auf OK.

Eigene E-Mail-Adresse ändern

1. Wählen Sie "Secure Gateway > Mein Profil".
2. Geben Sie eine neue Adresse in das Feld E-Mail-Adresse ein, um die Adresse hinzuzufügen oder zu ändern, die CC-SG für Benachrichtigungen verwendet.
3. Klicken Sie zum Speichern der Änderungen auf OK.

Benutzernamen des CC-SG-Superusers ändern

Sie müssen sich bei CC-SG über das CC-SG-Superuser-Konto angemeldet haben, um den Benutzernamen des CC-Superusers zu ändern. Der Standardbenutzername des CC-Superusers ist *admin*.

1. Wählen Sie "Secure Gateway > Mein Profil".
2. Geben Sie einen neuen Namen in das Feld "Benutzername" ein.
3. Klicken Sie zum Speichern der Änderungen auf OK.

Benutzer abmelden

Sie können aktive Benutzer individuell oder nach Benutzergruppe von CC-SG abmelden.

So melden Sie einen Benutzer ab:

1. Klicken Sie auf der Registerkarte "Benutzer" auf das Pluszeichen (+), um die Benutzergruppe einzublenden, die den Benutzer enthält, den Sie bei CCSG abmelden möchten. Wählen Sie dann den Benutzer aus.
   - Halten Sie zum Auswählen mehrerer Benutzer die Umschalttaste gedrückt, während Sie auf weitere Benutzer klicken.

2. Wählen Sie "Benutzer > Benutzermanager > Benutzer abmelden". Der Bildschirm "Benutzer abmelden" wird mit den ausgewählten Benutzern angezeigt.
3. Klicken Sie auf OK, um die Benutzer bei CC-SG abzumelden.

So melden Sie alle Benutzer einer Benutzergruppe ab:

1. Wählen Sie auf der Registerkarte "Benutzer" die Benutzergruppe aus, die Sie bei CC-SG abmelden möchten.
   - Halten Sie zum Abmelden mehrerer Benutzergruppen die Umschalttaste gedrückt, während Sie auf weitere Benutzergruppen klicken.
2. Wählen Sie "Benutzer > Benutzergruppenmanager > Benutzer abmelden". Der Bildschirm "Benutzer abmelden" wird mit den aktiven Benutzern der ausgewählten Gruppen angezeigt.
3. Klicken Sie auf OK, um die Benutzer bei CC-SG abzumelden.

Massenkopieren von Benutzern

Sie können Massenkopieren für Benutzer verwenden, um die Benutzergruppenzugehörigkeiten eines Benutzers in einen anderen Benutzer oder in eine Benutzerliste zu kopieren. Wenn die Benutzer, die die Zugehörigkeiten erhalten, vorhandene Gruppenzugehörigkeiten haben, werden die vorhandenen Zugehörigkeiten entfernt.

So verwenden Sie Massenkopieren für Benutzer:

1. Klicken Sie auf der Registerkarte "Benutzer" auf das Pluszeichen (+), um die Benutzergruppe einzublenden, die den Benutzer enthält, dessen Richtlinien und Berechtigungen Sie kopieren möchten. Wählen Sie dann den Benutzer aus.
2. Wählen Sie "Benutzer > Benutzermanager > Massenkopieren". Im Feld "Benutzername" wird der Benutzer angezeigt, dessen Richtlinien und Berechtigungen Sie kopieren.
3. Wählen Sie in der Liste "Alle Benutzer" die Benutzer aus, die die Richtlinien und Berechtigungen des im Feld "Benutzername" angezeigten Benutzers übernehmen sollen.
   - Klicken Sie auf >, um einen Benutzernamen in die Liste "Ausgewählte Benutzer" zu verschieben.
   - Klicken Sie auf >>, um alle Benutzer in die Liste "Ausgewählte Benutzer" zu verschieben.
   - Wählen Sie den Benutzer in der Liste "Ausgewählte Benutzer" aus, und klicken Sie auf <, um den Benutzer zu entfernen.
   - Klicken Sie auf <<, um alle Benutzer aus der Liste "Benutzer in Gruppe" zu entfernen.

4. Klicken Sie zum Kopieren auf OK.

Kapitel 10 Richtlinien für die Zugriffssteuerung

Richtlinien sind Regeln, die definieren, auf welche Knoten und Geräte Benutzer zugreifen können, wann sie darauf zugreifen können und ob Berechtigungen für virtuelle Medien aktiviert sind, falls zutreffend. Richtlinien erstellen Sie am einfachsten durch Kategorisieren Ihrer Knoten und Geräte in Knoten- und Gerätegruppen. Anschließend erstellen Sie Richtlinien, die Zugriff auf die Knoten und Geräte in jeder Gruppe zulassen oder verweigern. Nachdem Sie eine Richtlinie erstellt haben, ordnen Sie die Richtlinie einer Benutzergruppe zu. Siehe ***Richtlinien Benutzergruppen zuordnen*** (auf Seite 215).

CC-SG enthält eine Richtlinie mit unbeschränktem Zugriff. Wenn Sie allen Benutzern jederzeit Zugriff auf alle Knoten und Geräte gewähren möchten, können Sie allen Benutzergruppen die Richtlinie mit unbeschränktem Zugriff zuordnen.

Wenn Sie den Setup-Assitenten abgeschlossen haben, wurden eventuell schon einige allgemeine Richtlinien erstellt. Siehe ***Konfigurieren von CC-SG mit dem Setup-Assistenten*** (auf Seite 39).

So steuern Sie den Zugriff mit Richtlinien:

- Erstellen Sie Knotengruppen, um die Knoten zu verwalten, für die Sie Zugriffsregeln erstellen möchten. Siehe ***Knotengruppen hinzufügen*** (auf Seite 180).
- Erstellen Sie Gerätegruppen, um die Geräte zu verwalten, für die Sie Zugriffsregeln erstellen möchten. Siehe ***Gerätegruppen hinzufügen*** (auf Seite 87).
- Erstellen Sie eine Richtlinie für eine Knoten- oder Gerätegruppe, die angibt, wann der Zugriff auf die Knoten- oder Gerätegruppe erfolgen darf. Siehe ***Richtlinien hinzufügen*** (auf Seite 211).
- Wenden Sie die Richtlinie auf eine Benutzergruppe an. Siehe ***Richtlinien Benutzergruppen zuordnen*** (auf Seite 215).

In diesem Kapitel

Richtlinien hinzufügen 211
Richtlinien bearbeiten 212
Richtlinien löschen.....214
Unterstützung für virtuelle Medien.....214
Richtlinien Benutzergruppen zuordnen 215

Richtlinien hinzufügen

Wenn Sie eine Richtlinie erstellen, die den Zugriff auf eine Knoten- oder Gerätegruppe verweigert (Ablehnen), müssen Sie auch eine Richtlinie erstellen, die den Zugriff auf die ausgewählten Knoten- oder Gerätegruppen zulässt (Steuerung). Benutzer erhalten nicht automatisch die Rechte Steuerung, wenn die Richtlinie zum Ablehnen nicht verwendet wird.

So fügen Sie eine Richtlinie hinzu:

1. Wählen Sie "Zuordnungen > Richtlinien". Das Fenster "Richtlinienmanager" wird angezeigt.
2. Klicken Sie auf "Hinzufügen". Geben Sie den Namen der Richtlinie in das Dialogfeld ein.
3. Geben Sie den Namen der neuen Richtlinie im Feld "Richtlinienname" ein. Weitere Informationen zu den Regeln, die von CC-SG für die Länge von Namen verwendet werden, finden Sie unter ***Benennungskonventionen*** (siehe "***Benennungsregeln***" auf Seite 457).
4. Klicken Sie auf OK. Die neue Richtlinie wird im Bildschirm "Richtlinienmanager" zur Liste "Richtlinienname" hinzugefügt.
5. Klicken Sie auf den Pfeil der Dropdown-Liste "Gerätegruppe", und wählen Sie die Gerätegruppe aus, für die diese Richtlinie den Zugriff steuern soll.
6. Klicken Sie auf den Pfeil der Dropdown-Liste "Knotengruppe", und wählen Sie die Knotengruppe aus, für die diese Richtlinie den Zugriff steuern soll.
7. Bezieht sich die Richtlinie nur auf eine Gruppenart, müssen Sie nur einen Wert für diese Art auswählen.
8. Klicken Sie auf den Pfeil der Dropdown-Liste "Tage", und wählen Sie aus, an welchen Wochentagen diese Richtlinie gelten soll: Alle Tage, Wochentag (nur Montag bis Freitag) und Wochenende (nur Samstag und Sonntag) oder Benutzerdefiniert (wählen Sie bestimmte Tage aus).
9. Wählen Sie "Benutzerdefiniert" aus, um die gewünschten Tage auszuwählen. Die Kontrollkästchen für die einzelnen Tage werden wählbar.
10. Markieren Sie die Kontrollkästchen für die Tage, an denen die Richtlinie gelten soll.
11. Geben Sie in das Feld "Startzeit" die Uhrzeit ein, die als Startzeit für diese Richtlinie gelten soll. Die Uhrzeit muss im 24-Stundenformat eingegeben werden.

12. Geben Sie in das Feld "Endzeit" die Uhrzeit ein, die als Endzeit für diese Richtlinie gelten soll. Die Uhrzeit muss im 24-Stundenformat eingegeben werden.
13. Wählen Sie im Feld "Geräte-/Knotenzugriffsberechtigung" die Option "Steuerung" aus, um diese Richtlinie so zu definieren, dass sie den Zugriff auf ausgewählte Knoten oder Gerätegruppen zu den angegebenen Uhrzeiten und Tagen zulässt. Wählen Sie "Ablehnen" aus, um diese Richtlinie so zu definieren, dass sie den Zugriff auf ausgewählte Knoten oder Gerätegruppen zu den angegebenen Uhrzeiten und Tagen verweigert.
14. Wenn Sie Steuerung im Feld "Geräte-/Knotenzugriffsberechtigung" ausgewählt haben, wird der Abschnitt "Berechtigung für virtuelle Medien" aktiv dargestellt. Wählen Sie im Feld "Berechtigung für virtuelle Medien" eine Option aus, um den Zugriff auf virtuelle Medien, die in den ausgewählten Knoten- oder Gerätegruppen verfügbar sind, zu den angegebenen Uhrzeiten und Tagen zuzulassen oder zu verweigern.
    - Lese-/Schreibzugriff ermöglicht sowohl Lese- als auch Schreibberechtigung auf virtuelle Medien.
    - Lesezugriff ermöglicht nur Leseberechtigung auf virtuelle Medien.
    - Ablehnen verweigert den Zugriff auf virtuelle Medien.
15. Klicken Sie auf Aktualisieren, um die neue Richtlinie zu CC-SG hinzuzufügen. Bestätigen Sie die Nachricht mit Ja.

Richtlinien bearbeiten

Beim Bearbeiten von Richtlinien wirken sich die Änderungen nicht auf Benutzer aus, die zu dem Zeitpunkt bei CC-SG angemeldet sind. Die Änderungen werden beim nächsten Anmeldevorgang aktiviert.

Um sicherzustellen, dass die Änderungen vorher übernommen werden, müssen Sie in den Wartungsmodus wechseln und die Richtlinien dann bearbeiten. Wenn Sie in den Wartungsmodus wechseln, werden alle angemeldeten Benutzer bei CC-SG abgemeldet, bis Sie den Wartungsmodus verlassen. Danach können sich die Benutzer erneut anmelden. Siehe ***Wartungsmodus*** (auf Seite 263).

So bearbeiten Sie eine Richtlinie:

1. Klicken Sie im Menü "Zuordnungen" auf "Richtlinien". Das Fenster "Richtlinienmanager" wird angezeigt.
2. Klicken Sie auf den Pfeil neben der Dropdown-Liste "Richtlinienname", und wählen Sie die Richtlinien, die Sie bearbeiten möchten, in der Liste aus.

3. Klicken Sie zum Bearbeiten des Namens der Richtlinie auf Bearbeiten. Das Fenster "Richtlinie bearbeiten" wird angezeigt. Geben Sie einen neuen Namen für die Richtlinie in das Feld ein, und klicken Sie auf OK, um den Namen der Richtlinie zu ändern. **Optional.**
4. Klicken Sie auf den Pfeil der Dropdown-Liste "Gerätegruppe", und wählen Sie die Gerätegruppe aus, für die diese Richtlinie den Zugriff steuern soll.
5. Klicken Sie auf den Pfeil der Dropdown-Liste "Knotengruppe", und wählen Sie die Knotengruppe aus, für die diese Richtlinie den Zugriff steuern soll.
6. Bezieht sich die Richtlinie nur auf eine Gruppenart, müssen Sie nur einen Wert für diese Art auswählen.
7. Klicken Sie auf den Pfeil der Dropdown-Liste "Tage", und wählen Sie aus, an welchen Wochentagen diese Richtlinie gelten soll: Alle Tage, Wochentag (nur Montag bis Freitag) und Wochenende (nur Samstag und Sonntag) oder Benutzerdefiniert (wählen Sie bestimmte Tage aus).
8. Wählen Sie "Benutzerdefiniert" aus, um die gewünschten Tage auszuwählen. Die Kontrollkästchen für die einzelnen Tage werden wählbar.
9. Markieren Sie die Kontrollkästchen für die Tage, an denen die Richtlinie gelten soll.
10. Geben Sie in das Feld "Startzeit" die Uhrzeit ein, die als Startzeit für diese Richtlinie gelten soll. Die Uhrzeit muss im 24-Stundenformat eingegeben werden.
11. Geben Sie in das Feld "Endzeit" die Uhrzeit ein, die als Endzeit für diese Richtlinie gelten soll. Die Uhrzeit muss im 24-Stundenformat eingegeben werden.
    - Führen Sie im Feld "Geräte-/Knotenzugriffsberechtigung" folgende Schritte durch:
    - Wählen Sie "Steuerung" aus, um diese Richtlinie so zu definieren, dass sie den Zugriff auf die ausgewählten Knoten- oder Gerätegruppen zu den angegebenen Uhrzeiten und Tagen zulässt.
    - Wählen Sie "Ablehnen" aus, um diese Richtlinie so zu definieren, dass sie den Zugriff auf ausgewählte Knoten oder Gerätegruppen zu den angegebenen Uhrzeiten und Tagen verweigert.

12. Wenn Sie Steuerung im Feld "Geräte-/Knotenzugriffsberechtigung" ausgewählt haben, wird der Abschnitt "Berechtigung für virtuelle Medien" aktiv dargestellt. Wählen Sie im Feld "Berechtigung für virtuelle Medien" eine Option aus, um den Zugriff auf virtuelle Medien, die in den ausgewählten Knoten- oder Gerätegruppen verfügbar sind, zu den angegebenen Uhrzeiten und Tagen zuzulassen oder zu verweigern.
    - Lese-/Schreibzugriff ermöglicht sowohl Lese- als auch Schreibberechtigung auf virtuelle Medien.
    - Lesezugriff ermöglicht nur Leseberechtigung auf virtuelle Medien.
    - Ablehnen verweigert den Zugriff auf virtuelle Medien.
13. Klicken Sie zum Speichern der Änderungen auf "Aktualisieren".
14. Klicken Sie in der Bestätigungsmeldung auf "Ja".

Richtlinien löschen

Sie können nicht mehr benötigte Richtlinien löschen.

So löschen Sie eine Richtlinie:

1. Wählen Sie "Zuordnungen > Richtlinien". Das Fenster "Richtlinienmanager" wird angezeigt.
2. Klicken Sie auf den Pfeil neben der Dropdown-Liste "Richtlinienname", und wählen Sie die Richtlinien, die gelöscht werden soll.
3. Klicken Sie auf "Löschen".
4. Klicken Sie in der Bestätigungsmeldung auf "Ja".

Unterstützung für virtuelle Medien

CC-SG bietet Remoteunterstützung von virtuellen Medien für Knoten, die an virtuelle Medien-fähige KX2-, KSX2- und KX2-101-Geräte angeschlossen sind. Ausführliche Anweisungen über den Zugriff auf virtuelle Medien mit Ihrem Gerät finden Sie im:

- **Benutzerhandbuch zu Dominion KX II**
- **Benutzerhandbuch zu Dominion KSX II**
- **Benutzerhandbuch zu KXII-101**

Weitere Informationen zum Erstellen von Richtlinien zum Zuordnen der Berechtigung für virtuelle Medien zu Benutzergruppen in CC-SG finden Sie unter ***Richtlinien hinzufügen*** (auf Seite 211).

Richtlinien Benutzergruppen zuordnen

Richtlinien müssen Benutzergruppen zugeordnet werden, bevor sie wirksam werden. Nachdem eine Richtlinie einer Benutzergruppe zugeordnet wurde, wird der Zugriff der Gruppenmitglieder durch diese Richtlinie bestimmt. Weitere Informationen zum Zuordnen von Richtlinien zu einer Benutzergruppe finden Sie unter ***Benutzer und Benutzergruppen*** (auf Seite 185).

Wenn ein Benutzer zu mehreren Gruppen gehört, wird die weniger strenge Richtlinie für die Gruppen, denen er zugeordnet ist, auf den Benutzer angewendet.

Beispiel:

Richtlinie 123: Erlaubt Zugriff auf die Server 1 2 3.

Richtlinie 456: Erlaubt Zugriff auf die Server 4 5 6.

Gruppe A: Gruppe A ist Richtlinie 123 zugewiesen.

Gruppe B: Gruppe B ist Richtlinie 456 zugewiesen.

Der Benutzer gehört sowohl zu Gruppe A als auch zu Gruppe B. Dadurch hat der Benutzer Zugriff auf die Server 1 2 3 4 5 6.

Anschließend wird die Richtlinie "Richtlinie Ablehnung 1" erstellt: Diese verweigert den Zugriff auf Server 1.

Die Richtlinie "Richtlinie Ablehnung 1" wird Gruppe A zugewiesen. Der Benutzer hat nun lediglich Zugriff auf die Server 2 3 4 5 6.

Wenn die Richtlinie "Richtlinie Ablehnung 1" von Gruppe A auf Gruppe B übertragen wird, hat der Benutzer Zugriff auf die Server 1 2 3 4 5 6.

Kapitel 11 Benutzerdefinierte Ansichten für Geräte und Knoten

Mit benutzerdefinierten Ansichten können Sie die Anzeige der Knoten und Geräte im linken Fensterbereich mit Kategorien, Knotengruppen und Gerätegruppen unterschiedlich festlegen.

In diesem Kapitel

Typen von benutzerdefinierten Ansichten 216
Verwenden von benutzerdefinierten Ansichten im Administrations-Client 217

Typen von benutzerdefinierten Ansichten

Es gibt drei Typen von benutzerdefinierten Ansichten: Ansicht nach Kategorie, Filter nach Knotengruppe und Filter nach Gerätegruppe.

Ansicht nach Kategorie

Bei einer benutzerdefinierten Ansicht des Typs "Ansicht nach Kategorie" werden in der Liste der Knoten oder Geräte alle Knoten und Geräte angezeigt, die durch die von Ihnen festgelegten Kategorien definiert sind. Knoten oder Geräte, die keiner Kategorie zugeordnet sind, werden ebenfalls angezeigt und sind als „nicht zugewiesen“ gekennzeichnet.

Filter nach Knotengruppe

Bei einer benutzerdefinierten Ansicht des Typs "Filter nach Knotengruppe" werden in der Liste der Knoten nur die von Ihnen festgelegten Knotengruppen angezeigt. Die Gliederung erfolgt auf erster Ebene nach Knotengruppenname. Ein Knoten kann mehrere Male in der Liste angezeigt werden, wenn der Knoten zu mehreren in der benutzerdefinierten Ansicht definierten Knotengruppen gehört. Knoten, die zu keiner der in der benutzerdefinierten Ansicht definierten Knotengruppen gehören, werden in der Liste nicht angezeigt.

Filter nach Gerätegruppe

Bei einer benutzerdefinierten Ansicht des Typs "Filter nach Gerätegruppe" werden in der Liste der Geräte nur die von Ihnen festgelegten Gerätegruppen angezeigt. Die Gliederung erfolgt auf erster Ebene nach Gerätegruppenname. Ein Gerät kann mehrere Male in der Liste angezeigt werden, wenn das Gerät zu mehreren in der benutzerdefinierten Ansicht definierten Gerätegruppen gehört. Geräte, die zu keiner der in der benutzerdefinierten Ansicht definierten Gerätegruppen gehören, werden in der Liste nicht angezeigt.

Verwenden von benutzerdefinierten Ansichten im Administrations-Client

Benutzerdefinierte Ansichten für Knoten

Benutzerdefinierte Ansicht für Knoten hinzufügen

So fügen Sie eine benutzerdefinierte Ansicht für Knoten hinzu:

1. Klicken Sie auf die Registerkarte "Knoten".
2. Wählen Sie "Knoten > Ansicht ändern > Benutzerdefinierte Ansicht erstellen". Das Fenster "Benutzerdefinierte Ansicht" wird angezeigt.
3. Klicken Sie im Fensterbereich "Benutzerdefinierte Ansicht" auf "Hinzufügen". Das Fenster "Benutzerdefinierte Ansicht hinzufügen" wird angezeigt.
4. Geben Sie in das Feld "Name der benutzerdefinierten Ansicht" einen Namen für die neue benutzerdefinierte Ansicht ein.
5. Führen Sie im Bereich "Typ" der benutzerdefinierten Ansicht folgende Schritte aus:
   - Aktivieren Sie die Option "Filter nach Knotengruppe", um eine benutzerdefinierte Ansicht zu erstellen, in der nur die von Ihnen festgelegten Knotengruppen angezeigt werden.
   - Aktivieren Sie die Option "Ansicht nach Kategorie", um eine benutzerdefinierte Ansicht zu erstellen, in der die Knoten nach den von Ihnen festgelegten Kategorien angezeigt werden.
6. Klicken Sie auf OK.
7. Führen Sie im Bereich "Details der benutzerdefinierten Ansicht" folgende Schritte aus:
   a. Wählen Sie in der Liste "Verfügbar" das Element aus, das in die benutzerdefinierte Ansicht aufgenommen werden soll. Klicken Sie anschließend auf "Hinzufügen", um das Element der Liste hinzuzufügen. Wiederholen Sie diesen Schritt für beliebig viele Elemente.

b. Ordnen Sie die Elemente in der Liste "Ausgewählt" in der Reihenfolge an, in der die einzelnen Gruppen auf der Registerkarte "Knoten" angezeigt werden sollen. Wählen Sie ein Element aus, und klicken Sie auf den Pfeil nach oben oder unten, um das Element in die gewünschte Reihenfolge zu bringen.

c. Wenn Sie ein Element aus der Liste löschen müssen, wählen Sie das Element aus, und klicken Sie auf "Entfernen".

8. Klicken Sie auf Speichern. In einer Meldung wird bestätigt, dass die benutzerdefinierte Ansicht hinzugefügt wurde.
9. Klicken Sie auf "Als aktuell festlegen", um die neue benutzerdefinierte Ansicht anzuwenden.

Benutzerdefinierte Ansicht für Knoten anwenden

So wenden Sie eine benutzerdefinierte Ansicht auf die Knotenliste an:

1. Wählen Sie "Knoten > Ansicht ändern > Benutzerdefinierte Ansicht". Das Fenster "Benutzerdefinierte Ansicht" wird angezeigt.
2. Klicken Sie auf den Pfeil neben der Dropdown-Liste "Name", und wählen Sie eine benutzerdefinierte Ansicht in der Liste aus.
3. Klicken Sie auf "Ansicht anwenden".

Oder

- Wählen Sie "Knoten > Ansicht ändern". Alle benutzerdefinierten Ansichten sind als Optionen im Popup-Menü verfügbar. Wählen Sie die benutzerdefinierte Ansicht aus, die angewendet werden soll.

Benutzerdefinierte Ansicht für Knoten ändern

1. Klicken Sie auf die Registerkarte "Knoten".
2. Wählen Sie "Knoten > Ansicht ändern > Benutzerdefinierte Ansicht erstellen". Das Fenster "Benutzerdefinierte Ansicht" wird angezeigt.
3. Klicken Sie auf den Pfeil neben der Dropdown-Liste "Name", und wählen Sie eine benutzerdefinierte Ansicht in der Liste aus. Im Fensterbereich "Details der benutzerdefinierten Ansicht" werden Details zu den enthaltenen Elementen und die Reihenfolge angezeigt.

So ändern Sie den Namen einer benutzerdefinierten Ansicht:

1. Klicken Sie im Fensterbereich "Benutzerdefinierte Ansicht" auf Bearbeiten. Das Fenster "Benutzerdefinierte Ansicht bearbeiten" wird angezeigt.

2. Geben Sie in das Feld "Neuen Namen für benutzerdefinierte Ansicht eingeben" einen Namen für die benutzerdefinierte Ansicht ein, und klicken Sie auf OK. Der Name der neuen Ansicht wird im Feld "Name" des Bildschirms "Benutzerdefinierte Ansicht" angezeigt.

So ändern Sie den Inhalt der benutzerdefinierten Ansicht:

1. Führen Sie im Bereich "Details der benutzerdefinierten Ansicht" folgende Schritte aus:
   a. Wählen Sie in der Liste "Verfügbar" das Element aus, das in die benutzerdefinierte Ansicht aufgenommen werden soll. Klicken Sie anschließend auf "Hinzufügen", um das Element der Liste hinzuzufügen. Wiederholen Sie diesen Schritt für beliebig viele Elemente.
   b. Ordnen Sie die Elemente in der Liste "Ausgewählt" in der Reihenfolge an, in der die einzelnen Gruppen auf der Registerkarte "Knoten" angezeigt werden sollen. Wählen Sie ein Element aus, und klicken Sie auf den Pfeil nach oben oder unten, um das Element in die gewünschte Reihenfolge zu bringen.
   c. Wenn Sie ein Element aus der Liste löschen müssen, wählen Sie das Element aus, und klicken Sie auf "Entfernen".
2. Klicken Sie auf Speichern. In einer Meldung wird bestätigt, dass die benutzerdefinierte Ansicht hinzugefügt wurde.
3. Klicken Sie auf "Als aktuell festlegen", um die neue benutzerdefinierte Ansicht anzuwenden.

Benutzerdefinierte Ansicht für Knoten löschen

So löschen Sie eine benutzerdefinierte Ansicht für Knoten:

1. Klicken Sie auf die Registerkarte "Knoten".
2. Wählen Sie "Knoten > Ansicht ändern > Benutzerdefinierte Ansicht erstellen". Das Fenster "Benutzerdefinierte Ansicht" wird angezeigt.
3. Klicken Sie auf den Pfeil neben der Dropdown-Liste "Name", und wählen Sie eine benutzerdefinierte Ansicht in der Liste aus. Im Fensterbereich "Details der benutzerdefinierten Ansicht" werden Details zu den enthaltenen Elementen und die Reihenfolge angezeigt.
4. Klicken Sie im Fensterbereich "Benutzerdefinierte Ansicht" auf "Löschen". Die Bestätigungsmeldung "Benutzerdefinierte Ansicht löschen" wird angezeigt.
5. Klicken Sie auf "Ja".

Benutzerdefinierte Ansicht als Standard für Knoten festlegen

So weisen Sie eine benutzerdefinierte Ansicht als Standard für Knoten hinzu:

1. Klicken Sie auf die Registerkarte "Knoten".
2. Wählen Sie "Knoten > Ansicht ändern > Benutzerdefinierte Ansicht erstellen". Das Fenster "Benutzerdefinierte Ansicht" wird angezeigt.
3. Klicken Sie auf den Pfeil neben der Dropdown-Liste "Name", und wählen Sie eine benutzerdefinierte Ansicht in der Liste aus.
4. Klicken Sie im Fensterbereich "Benutzerdefinierte Ansicht" auf "Als Standard festlegen". Bei der nächsten Anmeldung wird standardmäßig die ausgewählte benutzerdefinierte Ansicht verwendet.

Benutzerdefinierte Ansicht als Standard für Knoten und alle Benutzer festlegen

Wenn Sie über die Berechtigung **CC-Setup und -Steuerung** verfügen, können Sie eine benutzerdefinierte Ansicht als Standardansicht für alle Benutzer festlegen.

So legen Sie eine benutzerdefinierte Ansicht als Standard für Knoten und alle Benutzer fest:

1. Klicken Sie auf die Registerkarte "Knoten".
2. Wählen Sie "Knoten > Ansicht ändern > Benutzerdefinierte Ansicht erstellen".
3. Klicken Sie auf den Pfeil der Dropdown-Liste "Name", und wählen Sie in der Liste die benutzerdefinierte Ansicht aus, die Sie als systemweite Standardansicht festlegen möchten.
4. Markieren Sie das Kontrollkästchen "Systemansicht", und klicken Sie auf "Speichern".

Für alle Benutzer, die sich bei CC-SG anmelden, wird die Registerkarte "Knoten" anhand der ausgewählten benutzerdefinierten Ansicht sortiert. Die Benutzer können die benutzerdefinierte Ansicht ändern.

Benutzerdefinierte Ansichten für Geräte

Benutzerdefinierte Ansichten für Geräte hinzufügen

So fügen Sie eine benutzerdefinierte Ansicht für Geräte hinzu:

1. Klicken Sie auf die Registerkarte "Geräte".

2. Wählen Sie "Geräte > Ansicht ändern > Benutzerdefinierte Ansicht erstellen". Das Fenster "Benutzerdefinierte Ansicht" wird angezeigt.
3. Klicken Sie im Fensterbereich "Benutzerdefinierte Ansicht" auf "Hinzufügen". Das Fenster "Benutzerdefinierte Ansicht hinzufügen" wird angezeigt.
4. Geben Sie in das Feld "Name der benutzerdefinierten Ansicht" einen Namen für die neue benutzerdefinierte Ansicht ein.
5. Führen Sie im Bereich "Typ" der benutzerdefinierten Ansicht folgende Schritte aus:
   - Markieren Sie die Option "Filter nach Gerätegruppe", um eine benutzerdefinierte Ansicht zu erstellen, in der nur die von Ihnen festgelegten Gerätegruppen angezeigt werden.
   - Markieren Sie die Option "Ansicht nach Kategorie", um eine benutzerdefinierte Ansicht zu erstellen, in der die Geräte nach den von Ihnen festgelegten Kategorien angezeigt werden.
6. Klicken Sie auf OK.
7. Führen Sie im Bereich "Details der benutzerdefinierten Ansicht" folgende Schritte aus:
   a. Wählen Sie in der Liste "Verfügbar" das Element aus, das in die benutzerdefinierte Ansicht aufgenommen werden soll. Klicken Sie anschließend auf "Hinzufügen", um das Element der Liste hinzuzufügen. Wiederholen Sie diesen Schritt für beliebig viele Elemente.
   b. Ordnen Sie die Elemente in der Liste "Ausgewählt" in der Reihenfolge an, in der die einzelnen Gruppen auf der Registerkarte "Knoten" angezeigt werden sollen. Wählen Sie ein Element aus, und klicken Sie auf den Pfeil nach oben oder unten, um das Element in die gewünschte Reihenfolge zu bringen.
   c. Wenn Sie ein Element aus der Liste löschen müssen, wählen Sie das Element aus, und klicken Sie auf "Entfernen".
8. Klicken Sie auf Speichern. In einer Meldung wird bestätigt, dass die benutzerdefinierte Ansicht hinzugefügt wurde.
9. Klicken Sie auf "Als aktuell festlegen", um die neue benutzerdefinierte Ansicht anzuwenden.

Benutzerdefinierte Ansichten für Geräte anwenden

So wenden Sie eine benutzerdefinierte Ansicht auf die Geräteliste an:

1. Wählen Sie "Geräte > Ansicht ändern > Benutzerdefinierte Ansicht". Das Fenster "Benutzerdefinierte Ansicht" wird angezeigt.

2. Klicken Sie auf den Pfeil neben der Dropdown-Liste "Name", und wählen Sie eine benutzerdefinierte Ansicht in der Liste aus.
3. Klicken Sie auf "Als aktuell festlegen", um die benutzerdefinierte Ansicht anzuwenden.

Oder

Wählen Sie "Geräte > Ansicht ändern". Alle benutzerdefinierten Ansichten sind als Optionen im Popup-Menü verfügbar. Wählen Sie die benutzerdefinierte Ansicht aus, die angewendet werden soll.

Benutzerdefinierte Ansichten für Geräte ändern

1. Klicken Sie auf die Registerkarte "Geräte".
2. Wählen Sie "Geräte > Ansicht ändern > Benutzerdefinierte Ansicht erstellen". Das Fenster "Benutzerdefinierte Ansicht" wird angezeigt.
3. Klicken Sie auf den Pfeil neben der Dropdown-Liste "Name", und wählen Sie eine benutzerdefinierte Ansicht in der Liste aus. Im Fensterbereich "Details der benutzerdefinierten Ansicht" werden Details zu den enthaltenen Elementen und die Reihenfolge angezeigt.

So ändern Sie den Namen einer benutzerdefinierten Ansicht:

1. Klicken Sie im Fensterbereich "Benutzerdefinierte Ansicht" auf Bearbeiten. Das Fenster "Benutzerdefinierte Ansicht bearbeiten" wird angezeigt.
2. Geben Sie in das Feld "Neuen Namen für benutzerdefinierte Ansicht eingeben" einen Namen für die benutzerdefinierte Ansicht ein, und klicken Sie auf OK. Der Name der neuen Ansicht wird im Feld "Name" des Bildschirms "Benutzerdefinierte Ansicht" angezeigt.

So ändern Sie den Inhalt der benutzerdefinierten Ansicht:

1. Führen Sie im Bereich "Details der benutzerdefinierten Ansicht" folgende Schritte aus:
   a. Wählen Sie in der Liste "Verfügbar" das Element aus, das in die benutzerdefinierte Ansicht aufgenommen werden soll. Klicken Sie anschließend auf "Hinzufügen", um das Element der Liste hinzuzufügen. Wiederholen Sie diesen Schritt für beliebig viele Elemente.
   b. Ordnen Sie die Elemente in der Liste "Ausgewählt" in der Reihenfolge an, in der die einzelnen Gruppen auf der Registerkarte "Knoten" angezeigt werden sollen. Wählen Sie ein Element aus, und klicken Sie auf den Pfeil nach oben oder unten, um das Element in die gewünschte Reihenfolge zu bringen.

c. Wenn Sie ein Element aus der Liste löschen müssen, wählen Sie das Element aus, und klicken Sie auf "Entfernen".

2. Klicken Sie auf Speichern. In einer Meldung wird bestätigt, dass die benutzerdefinierte Ansicht hinzugefügt wurde.
3. Klicken Sie auf "Als aktuell festlegen", um die neue benutzerdefinierte Ansicht anzuwenden.

Benutzerdefinierte Ansichten für Geräte löschen

So löschen Sie eine benutzerdefinierte Ansicht für Geräte:

1. Klicken Sie auf die Registerkarte "Geräte".
2. Wählen Sie "Geräte > Ansicht ändern > Benutzerdefinierte Ansicht erstellen". Das Fenster "Benutzerdefinierte Ansicht" wird angezeigt.
3. Klicken Sie auf den Pfeil neben der Dropdown-Liste "Name", und wählen Sie eine benutzerdefinierte Ansicht in der Liste aus. Im Fensterbereich "Details der benutzerdefinierten Ansicht" werden Details zu den enthaltenen Elementen und die Reihenfolge angezeigt.
4. Klicken Sie im Fensterbereich "Benutzerdefinierte Ansicht" auf "Löschen". Die Bestätigungsmeldung "Benutzerdefinierte Ansicht löschen" wird angezeigt.
5. Klicken Sie auf "Ja".

Benutzerdefinierte Ansicht für Geräte als Standard zuordnen

So weisen Sie eine benutzerdefinierte Ansicht als Standard für Geräte hinzu:

1. Klicken Sie auf die Registerkarte "Geräte".
2. Wählen Sie "Geräte > Ansicht ändern > Benutzerdefinierte Ansicht erstellen". Das Fenster "Benutzerdefinierte Ansicht" wird angezeigt.
3. Klicken Sie auf den Pfeil neben der Dropdown-Liste "Name", und wählen Sie eine benutzerdefinierte Ansicht in der Liste aus.
4. Klicken Sie im Fensterbereich "Benutzerdefinierte Ansicht" auf "Als Standard festlegen". Bei der nächsten Anmeldung wird standardmäßig die ausgewählte benutzerdefinierte Ansicht verwendet.

Benutzerdefinierte Ansicht von Geräten als Standard für alle Benutzer zuordnen

Wenn Sie über die Berechtigung "Geräte-, Port- und Knotenverwaltung" verfügen, können Sie eine benutzerdefinierte Ansicht als Standardansicht für alle Benutzer zuordnen.

So legen Sie eine benutzerdefinierte Ansicht als Standard für Geräte und alle Benutzer fest

1. Klicken Sie auf die Registerkarte "Geräte".
2. Wählen Sie "Geräte > Ansicht ändern > Benutzerdefinierte Ansicht erstellen".
3. Klicken Sie auf den Pfeil der Dropdown-Liste "Name", und wählen Sie in der Liste die benutzerdefinierte Ansicht aus, die Sie als systemweite Standardansicht festlegen möchten.
4. Markieren Sie das Kontrollkästchen "Systemweit", und klicken Sie auf "Speichern".

Für alle Benutzer, die sich an CC-SG anmelden, wird die Registerkarte "Geräte" anhand der ausgewählten benutzerdefinierten Ansicht sortiert. Die Benutzer können die benutzerdefinierte Ansicht ändern.

Kapitel 12 Remoteauthentifizierung

In diesem Kapitel

Überblick über Authentifizierung und Autorisierung (AA) 225
Definierte Namen für LDAP und Active Directory 226
Module für die Authentifizierung und Autorisierung festlegen 227
Reihenfolge für externe AA-Server festlegen 228
Überblick über AD und CC-SG 228
AD-Module zu CC-SG hinzufügen 229
AD-Module bearbeiten 234
AD-Benutzergruppen importieren 235
Active Directory mit CC-SG synchronisieren 236
Umbenennen und Verschieben von AD-Gruppen 240
LDAP und CC-SG 240
LDAP-Module (Netscape) zu CC-SG hinzufügen 240
TACACS+ und CC-SG 245
TACACS+-Module hinzufügen 245
RADIUS und CC-SG 246
RADIUS-Module hinzufügen 246

Überblick über Authentifizierung und Autorisierung (AA)

CC-SG-Benutzer können lokal authentifiziert und in CC-SG autorisiert werden, oder die Authentifizierung kann mithilfe der folgenden unterstützten Verzeichnisserver remote durchgeführt werden:

- Microsoft Active Directory (AD)
- Lightweight Directory Access Protocol (LDAP) von Netscape
- TACACS+
- RADIUS

Jede Anzahl an Remoteservern kann für die externe Authentifizierung verwendet werden. Sie können beispielsweise drei Active Directory-Server, zwei iPlanet- (LDAP) Server und drei RADIUS-Server konfigurieren.

Nur Active Directory kann für die Remoteautorisierung von Benutzern verwendet werden.

LDAP-Implementierungen verwenden LDAP v3.

Authentifizierungsfluss

Ist die Remoteauthentifizierung aktiviert, werden bei der Authentifizierung und Autorisierung folgende Schritte durchgeführt:

1. Der Benutzer meldet sich mit seinem Benutzernamen und Kennwort bei CS-SG an.

2. CC-SG stellt eine Verbindung zum externen Server her und übermittelt den Benutzernamen und das Kennwort.
3. Der Benutzername und das Kennwort werden entweder akzeptiert oder zurückgewiesen und zurückgesendet. Bei einer zurückgewiesenen Authentifizierung schlägt die Anmeldung fehl.
4. Ist die Authentifizierung erfolgreich, wird die Autorisierung durchgeführt. CC-SG prüft, ob der eingegebene Benutzername einer Gruppe entspricht, die in CC-SG erstellt oder von Active Directory importiert wurde, und gewährt die Berechtigungen entsprechend der zugeordneten Richtlinie.

Ist die Remoteauthentifizierung deaktiviert, werden die Authentifizierung und Autorisierung lokal in CC-SG durchgeführt.

Benutzerkonten

Benutzerkonten müssen dem Authentifizierungsserver zur Remoteauthentifizierung hinzugefügt werden. Außer bei der Verwendung von Active Directory für die Authentifizierung und Autorisierung erfordern alle Authentifizierungsserver, dass Benutzer in CC-SG erstellt werden. Der Benutzername, der beim Authentifizierungsserver verwendet wird, muss mit dem bei CC-SG übereinstimmen; die Kennwörter dürfen jedoch voneinander abweichen. Das lokale CC-SG-Kennwort wird nur verwendet, wenn die Remoteauthentifizierung deaktiviert ist. Weitere Informationen zum Hinzufügen von Benutzern, für die Remoteauthentifizierung verwendet wird, finden Sie unter ***Benutzer und Benutzergruppen*** (auf Seite 185).

Hinweis: Bei Verwendung der Remoteauthentifizierung müssen sich die Benutzer an den Administrator wenden, wenn sie ihr Kennwort auf dem Remoteserver ändern möchten. Kennwörter können in CC-SG für Benutzer, bei denen die Remoteauthentifizierung verwendet wird, nicht geändert werden.

Definierte Namen für LDAP und Active Directory

Die Konfiguration von Benutzern auf LDAP- oder Active Directory-Servern, für die die Remoteauthentifizierung verwendet wird, erfordert die Eingabe von Benutzernamen und das Suchen im Format für definierte Namen. Das vollständige Format eines definierten Namens wird in RFC2253 (http://www.rfc-editor.org/rfc/rfc2253.txt) beschrieben.

Zur Konfiguration von CC-SG müssen Sie wissen, wie definierte Namen eingegeben werden sowie die Reihenfolge, in der jede Komponente des Namens aufgelistet werden soll.

Definierte Namen für Active Directory festlegen

Definierte Namen für Active Directory sollten dieser Struktur folgen. Sie müssen nicht beides, den allgemeinen Namen und die Organisationseinheit, festlegen.

- common name (cn), organizational unit (ou), domain component (dc)

Definierte Namen für LDAP festlegen

Definierte Namen für Netscape LDAP und eDirectory LDAP sollten dieser Struktur folgen:

- user id (uid), organizational unit (ou), organization (o)

Benutzernamen für Active Directory festlegen

Bei der Authentifizierung von CC-SG-Benutzern auf einem Active Directory-Server durch die Angabe von cn=administrator,cn=users,dc=xyz,dc=com in username erhalten die Benutzer Zugriff mithilfe dieser Angaben, wenn ein CC-SG einer importierten AD-Gruppe zugewiesen ist. Beachten Sie, dass Sie mehrere allgemeine Namen, Organisationseinheiten und Domänenkomponenten festlegen können.

Basis-DNs festlegen

Sie können auch einen definierten Namen eingeben, um festzulegen, wo die Suche für Benutzer beginnt. Geben Sie einen definierten Namen in das Feld "Basis-DN" ein, um einen Active Directory-Container festzulegen, in dem die Benutzer gefunden werden können. Die Eingabe von "ou=DCAdmins,ou=IT,dc=xyz,dc=com" führt beispielsweise zu einer Suche unter allen Benutzern in den Organisationseinheiten "DCAdmins" und "IT" und der Domäne "xyz.com".

Module für die Authentifizierung und Autorisierung festlegen

Nachdem Sie alle externen Server in CC-SG als Module hinzugefügt haben, legen Sie fest, ob CC-SG jeden dieser Server für die Authentifizierung, Autorisierung oder beides verwenden soll.

So legen Sie Module für die Authentifizierung und Autorisierung fest:

1. Wählen Sie "Administration > Sicherheit".
2. Klicken Sie auf die Registerkarte "Authentifizierung". Alle konfigurierten externen Autorisierungs- und Authentifizierungsserver werden in einer Tabelle angezeigt.
3. Führen Sie für jeden aufgelisteten Server folgende Schritte durch:

a. Markieren Sie das Kontrollkästchen "Authentifizierung", wenn CC-SG die Benutzer mit dem Server authentifizieren soll.

b. Markieren Sie das Kontrollkästchen "Autorisierung", wenn CC-SG die Benutzer mit dem Server autorisieren soll. Nur AD-Server können zur Autorisierung verwendet werden.

4. Klicken Sie zum Speichern der Änderungen auf "Aktualisieren".

Reihenfolge für externe AA-Server festlegen

CC-SG fragt die konfigurierten externen Autorisierungs- und Authentifizierungsserver in der festgelegten Reihenfolge ab. Wenn die erste aktivierte Option nicht verfügbar ist, probiert CC-SG die zweite Option aus, dann die dritte usw., bis der Vorgang erfolgreich ist.

So legen Sie die Reihenfolge fest, in der CC-SG externe Authentifizierungs- und Autorisierungsserver verwendet:

1. Wählen Sie "Administration > Sicherheit".
2. Klicken Sie auf die Registerkarte "Authentifizierung". Alle konfigurierten externen Autorisierungs- und Authentifizierungsserver werden in einer Tabelle angezeigt.
3. Wählen Sie in der Liste einen Server aus, und klicken Sie auf die Pfeile nach oben und nach unten, um die Reihenfolge der Verwendung festzulegen.
4. Klicken Sie zum Speichern der Änderungen auf "Aktualisieren".

Überblick über AD und CC-SG

CC-SG unterstützt die Authentifizierung und Autorisierung von Benutzern, die von einem AD-Domänencontroller importiert wurden, ohne dass die Benutzer lokal in CC-SG definiert werden müssen. Benutzer können somit ausschließlich auf dem AD-Server verwaltet werden. Sobald Ihr AD-Server als Modul in CC-SG konfiguriert wurde, kann CC-SG alle Domänenkontroller nach einer bestimmten Domäne durchsuchen. Sie können Ihre AD-Module mit Ihren AD-Servern in CC-SG synchronisieren, um sicherzustellen, dass CC-SG über die aktuellsten Autorisierungsinformationen hinsichtlich Ihrer AD-Benutzergruppen verfügt.

Fügen Sie keine doppelten AD-Module hinzu. Wenn Ihre Benutzer bei einem Anmeldeversuch die Nachricht "Sie sind kein Mitglied einer Benutzergruppe" erhalten, haben Sie möglicherweise doppelte AD-Module konfiguriert. Überprüfen Sie die konfigurierten Module, um festzustellen, ob sie überlappende Domänenbereiche beschreiben.

AD-Module zu CC-SG hinzufügen

Wichtig: Erstellen Sie entsprechende AD-Benutzergruppen, und ordnen Sie AD-Benutzer zu, bevor Sie diesen Vorgang starten. Vergewissern Sie sich außerdem, dass Sie das CC-SG DNS- und Domänensuffix im Konfigurationsmanager konfiguriert haben. Siehe *CC-SG-Netzwerk konfigurieren* (auf Seite 288).

So fügen Sie ein AD-Modul zu CC-SG hinzu:

1. Wählen Sie "Administration > Sicherheit".
2. Klicken Sie auf die Registerkarte "Authentifizierung".
3. Klicken Sie auf "Hinzufügen", um das Fenster "Modul hinzufügen" zu öffnen.
4. Klicken Sie auf das Dropdown-Menü "Modultyp", und wählen Sie AD in der Liste aus.
5. Geben Sie den Namen des AD-Servers in das Feld "Modulname" ein.
   - Die Höchstanzahl an Zeichen ist 31.
   - Alle druckbaren Zeichen können verwendet werden.
   - Der Modulname ist optional und wird nur angegeben, um dieses AD-Servermodul von anderen zu unterscheiden, die Sie in CC-SG konfigurieren. Der Name wird nicht mit dem tatsächlichen AD-Servernamen verknüpft.
6. Klicken Sie auf "Weiter". Die Registerkarte "Allgemein" wird angezeigt.

Allgemeine AD-Einstellungen

Auf der Registerkarte "Allgemein" müssen Sie Informationen hinzufügen, damit CC-SG den AD-Server abfragen kann.

Fügen Sie keine doppelten AD-Module hinzu. Wenn Ihre Benutzer bei einem Anmeldeversuch die Nachricht "Sie sind kein Mitglied einer Benutzergruppe" erhalten, haben Sie möglicherweise doppelte AD-Module konfiguriert. Überprüfen Sie die konfigurierten Module, um festzustellen, ob sie überlappende Domänenbereiche beschreiben.

1. Geben Sie die AD-Domäne zum Abfragen in das Feld "Domäne" ein. Ist die AD-Domäne beispielsweise in der Domäne xyz.com installiert, geben Sie xyz.com in das Feld "Domäne" ein. CC-SG und der AD-Server, den Sie abfragen möchten, müssen entweder in derselben Domäne oder in verschiedenen Domänen konfiguriert sein, die sich vertrauen.

   Hinweis: CC-SG fragt alle bekannten Domänencontroller nach der angegebenen Domäne ab.

2. Geben Sie die IP-Adressen der primären und sekundären DNS-Server in die Felder "IP-Adresse des primären DNS-Servers" und "IP-Adresse des sekundären DNS-Servers" ein, oder markieren Sie das Kontrollkästchen "CC-SG-Standard-DNS verwenden", um das DNS zu verwenden, das im Bereich "Konfigurationsmanager" von CC-SG konfiguriert ist. Siehe ***Erweiterte Administration*** (auf Seite 282).
3. Aktivieren Sie das Kontrollkästchen "Anonyme Bindung", wenn Sie ohne Festlegung eines Benutzernamens und Kennworts eine Verbindung mit dem AD-Server herstellen möchten. Wenn Sie diese Option verwenden, sollten Sie sicherstellen, dass der AD-Server anonyme Abfragen zulässt.

   Hinweis: Standardmäßig lässt Windows 2003 KEINE anonymen Abfragen zu. Windows 2000 Server lassen bestimmte anonyme Funktionen zu, wenn die Abfrageergebnisse auf den Berechtigungen für jedes Objekt beruhen.

4. Wenn Sie keine anonyme Bindung verwenden, geben Sie den Benutzernamen des Benutzerkontos, den Sie für die Abfrage des AD-Servers verwenden möchten, in das Feld "Benutzername" ein. Das erforderliche Format ist von der AD-Version und -Konfiguration abhängig. Verwenden Sie eines der folgenden Formate.

   Ein Benutzer namens Benutzername und mit dem Anmeldenamen Benutzern in der Domäne raritan.com könnte folgendermaßen eingegeben werden:

   - cn=Benutzername,cn=users,dc=Raritan,dc=com
   - Benutzername@raritan.com
   - Raritan/Benutzername

   Hinweis: Der angegebene Benutzer muss über die Berechtigung verfügen, Suchabfragen in der AD-Domäne durchführen zu können. Der Benutzer kann beispielsweise einer Gruppe im Acitve Directory angehören, für die Group scope (Gruppenumfang) auf Global und Group type (Gruppentyp) auf Security (Sicherheit) gesetzt ist.

5. Geben Sie in die Felder "Kennwort" und "Kennwort bestätigen" das Kennwort für das Benutzerkonto ein, das Sie für die Abfrage des AD-Servers verwenden möchten. Der Name darf aus maximal 32 Zeichen bestehen.
6. Klicken Sie auf Verbindung testen, um die Verbindung zum Active Directory-Server mit den angegebenen Parametern zu testen. Sie sollten eine Bestätigung über eine erfolgreiche Verbindung erhalten. Wird die Bestätigungsmeldung nicht angezeigt, prüfen Sie die Einstellungen sorgfältig auf Fehler, und versuchen Sie es erneut.
7. Klicken Sie auf "Weiter". Die Registerkarte "Erweitert" wird angezeigt.

Erweiterte AD-Einstellungen

So konfigurieren Sie die erweiterten AD-Einstellungen:

1. Klicken Sie auf die Registerkarte "Erweitert".
2. Geben Sie die Portnummer ein, die der AD-Server überwacht. Der Standardport lautet 389. Wenn Sie sichere Verbindungen für LDAP verwenden, müssen Sie diesen Port ggf. ändern. Der Standardport für sichere LDAP-Verbindungen lautet 636.
3. Aktivieren Sie das Kontrollkästchen "Sichere Verbindung für LDAP", wenn Sie einen sicheren Kanal für die Verbindung verwenden möchten. Ist das Feld markiert, verwendet CC-SG zur Verbindung mit AD LDAP über SSL. Diese Option wird ggf. nicht von Ihrer AD-Konfiguration unterstützt.
4. Legen Sie einen Basis-DN (Verzeichnisebene/Eintrag) fest, unter dem die Authentifizierungssuchabfrage ausgeführt wird. CC-SG kann eine rekursive Suche vom Basis-DN nach unten durchführen.

Beispiel	Beschreibung
dc=raritan,dc=com	Die Abfrage für den Benutzereintrag wird für die gesamte Verzeichnisstruktur durchgeführt.
cn=Administrators,cn=Users,dc=raritan,dc=com	Die Abfrage für den Benutzereintrag wird nur im Unterverzeichnis „Administrators" (Eintrag) durchgeführt.

5. Geben Sie die Attribute eines Benutzers in das Feld "Filter" ein, damit die Suchabfrage auf die Einträge beschränkt wird, die diese Kriterien erfüllen. Der Filter ist standardmäßig objectclass=user, d. h., dass nur Einträge vom Typ user durchsucht werden.
6. Geben Sie die Art und Weise für die Durchführung der Abfrage für den Benutzereintrag an.
   - Markieren Sie das Kontrollkästchen "Bindung verwenden", wenn der Benutzer, der sich über das Applet anmeldet, über die Berechtigungen verfügt, Abfragen an den AD-Server zu senden. Ist das Muster des Benutzernamens unter "Bindungsmuster für Benutzernamen" angegeben, wird das Muster mit dem Benutzernamen vereint, der im Applet angegeben ist, und der vereinte Benutzername wird für die Verbindung zum AD-Server verwendet.

Beispiel: Ist "cn={0},cn=Users,dc=raritan,dc=com" und "TestUser" im Applet angegeben, verwendet CC-SG "cn=TestUser,cn-Users,dc=raritan,dc=com" für die Verbindung zum AD-Server.

- Aktivieren Sie das Kontrollkästchen "Bindung nach Suche verwenden", um mit dem Benutzernamen und dem Kennwort, die auf der Registerkarte "Allgemein" festgelegt wurden, eine Verbindung mit dem Active Directory-Server herzustellen. Der Eintrag wird in dem angegebenen Basis-DN gesucht. Treffer treten auf, wenn die bestimmten Filterkriterien übereinstimmen und das Attribut "BerndKontoname" dem Benutzernamen entspricht, der im Applet angegeben wurde. Dann wird die zweite Verbindung mit dem Benutzernamen und Kennwort versucht, die im Applet angegeben sind. Durch diese zweite Verbindung wird sichergestellt, dass der Benutzer das richtige Kennwort angegeben hat.

7. Klicken Sie auf "Weiter". Die Registerkarte "Gruppen" wird angezeigt.

AD-Gruppeneinstellungen

Auf der Registerkarte "Gruppen" können Sie den Speicherort angeben, von dem Sie AD-Benutzergruppen importieren möchten.

Wichtig: Sie müssen Gruppeneinstellungen angeben, bevor Sie Gruppen von AD importieren können.

1. Klicken Sie auf die Registerkarte "Gruppen".
2. Legen Sie einen Basis-DN (Verzeichnisebene/Eintrag) fest, unter dem die Gruppen, die den zu authentifizierenden Benutzer enthalten, gesucht werden.

Beispiel	Beschreibung
dc=raritan,dc=com	Die Abfrage für den Benutzer in der Gruppe wird für die gesamte Verzeichnisstruktur durchgeführt.
cn=Administrators,cn=Users,dc=raritan,dc=com	Die Abfrage für den Benutzer in der Gruppe wird nur im Unterverzeichnis "Administrators" (Eintrag) durchgeführt.

3. Geben Sie die Attribute eines Benutzers in das Feld "Filter" ein, damit die Suchabfrage für den Benutzer in der Gruppe auf die Einträge beschränkt wird, die diese Kriterien erfüllen.

Wenn Sie beispielsweise cn=Groups,dc=raritan,dc=com als den Basis-DN und (objectclass=group) als Filter angeben, werden alle Einträge zurückgegeben, die sich im Eintrag Groups befinden und den Typ group aufweisen.

4. Klicken Sie auf "Weiter". Die Registerkarte "Trusts" (Vertrauen) wird angezeigt.

AD-Vertrauenseinstellungen

Auf der Registerkarte "Vertrauensstellungen" können Sie Vertrauensbeziehungen zwischen dieser neuen AD-Domäne und vorhandenen Domänen einrichten. Eine Vertrauensbeziehung bietet authentifizierten Benutzern verschiedener Domänen den Zugriff auf Ressourcen. Vertrauensbeziehungen können eingehend, ausgehend, bidirektional oder deaktiviert sein. Sie sollten Vertrauensbeziehungen einrichten, wenn AD-Module, die verschiedene Gesamtstrukturen in AD darstellen, auf die Informationen anderer Gesamtstrukturen zugreifen sollen. Die von Ihnen in CC-SG konfigurierten Vertrauensstellungen sollten mit den in Active Directory konfigurierten Vertrauensstellungen übereinstimmen.

1. Klicken Sie auf die Registerkarte "Trusts" (Vertrauen). Wenn Sie mehrere AD-Domänen konfiguriert haben, werden alle anderen Domänen auf der Registerkarte "Trusts" (Vertrauen) aufgeführt.
2. Klicken Sie für jede Domäne in der Spalte "Trust Partner" (Vertrauenspartner) auf das Dropdown-Menü "Trust Direction" (Vertrauensrichtung), und wählen Sie die Richtung für das Vertrauen zwischen den Domänen aus. Vertrauensrichtungen werden in allen AD-Modulen aktualisiert, wenn Sie Änderungen an einem AD-Modul vornehmen.
   - Incoming (Eingehend): Informationen, die von anderen Domänen eingehen, sind vertrauenswürdig.
   - Outgoing (Ausgehend): Informationen, die an die ausgewählten Domänen gesendet werden, sind vertrauenswürdig.
   - Bidirectional (Bidirektional): Informationen aus beiden Richtungen jeder Domäne sind vertrauenswürdig.
   - Disabled (Deaktiviert): Unter den Domänen findet kein Informationsaustausch statt.
3. Klicken Sie auf Übernehmen, um die Änderungen zu speichern. Klicken Sie dann auf OK, um das AD-Modul zu speichern und das Fenster zu schließen.

   Das neue AD-Modul wird im Fenster "Sicherheitsmanager" unter "Externe AA-Server" angezeigt.
4. Markieren Sie das Kontrollkästchen "Authentifizierung", wenn CC-SG die Benutzer mit dem AD-Modul authentifizieren soll. Markieren Sie das Kontrollkästchen "Autorisierung", wenn CC-SG die Benutzer mit dem AD-Modul autorisieren soll.

5. Klicken Sie zum Speichern der Änderungen auf "Aktualisieren".

AD-Module bearbeiten

Nachdem Sie AD-Module konfiguriert haben, können Sie sie jederzeit bearbeiten.

So bearbeiten Sie ein AD-Modul:

1. Wählen Sie "Administration > Sicherheit".
2. Klicken Sie auf die Registerkarte "Authentifizierung". Alle konfigurierten externen Autorisierungs- und Authentifizierungsserver werden in einer Tabelle angezeigt.
3. Wählen Sie das AD-Modul aus, das Sie bearbeiten möchten, und klicken Sie auf "Bearbeiten".
4. Klicken Sie auf jede Registerkarte des Fensters "Modul bearbeiten", um die konfigurierten Einstellungen anzuzeigen. Nehmen Sie bei Bedarf Änderungen vor. Siehe ***Allgemeine AD-Einstellungen*** (auf Seite 229), ***Erweiterte AD-Einstellungen*** (auf Seite 231), ***AD-Gruppeneinstellungen*** (auf Seite 232) und ***AD-Vertrauenseinstellungen*** (auf Seite 233).
5. Wenn Sie die Verbindungsinformationen ändern, klicken Sie auf "Verbindung testen", um die Verbindung zum AD-Server mit den festgelegten Parametern zu testen. Sie sollten eine Bestätigung über eine erfolgreiche Verbindung erhalten. Wird die Bestätigungsmeldung nicht angezeigt, prüfen Sie die Einstellungen sorgfältig auf Fehler, und versuchen Sie es erneut.
6. Klicken Sie zum Speichern der Änderungen auf OK.
7. Sie müssen die von Ihnen geänderten AD-Benutzergruppen synchronisieren. Sie können auch alle AD-Module synchronisieren, um alle Gruppen und Benutzer in allen Modulen zu synchronisieren. Siehe ***Alle Benutzergruppen mit Active Directory synchronisieren*** (auf Seite 237) und ***Alle AD-Module synchronisieren*** (auf Seite 238).

AD-Benutzergruppen importieren

Sie müssen Gruppeneinstellungen im AD-Modul angeben, bevor Sie Gruppen vom AD-Server importieren können. Siehe ***AD-Gruppeneinstellungen*** (auf Seite 232).

Nach dem Ändern von importierten Gruppen oder Benutzern müssen Sie die geänderten AD-Benutzergruppen synchronisieren, damit die importierten Gruppen den entsprechenden Gruppen in Active Directory zugeordnet werden. Außerdem müssen Sie alle AD-Module synchronisieren, um alle Gruppen und Benutzer in allen Modulen zu synchronisieren. Siehe ***Alle Benutzergruppen mit Active Directory synchronisieren*** (auf Seite 237) und ***Alle AD-Module synchronisieren*** (auf Seite 238).

Sie können verschachtelte Gruppen aus Active Directory importieren.

Hinweis: Vergewissern Sie sich, dass Sie das CC-SG DNS und Domänensuffix im Konfigurationsmanager konfiguriert haben, bevor Sie AD-Benutzergruppen importieren. Siehe **Erweiterte Administration** *(auf Seite 282).*

So importieren Sie eine AD-Benutzergruppe:

1. Wählen Sie "Administration > Sicherheit".
2. Klicken Sie auf die Registerkarte "Authentifizierung". Alle konfigurierten Autorisierungs- und Authentifizierungsserver werden in einer Tabelle angezeigt.
3. Wählen Sie den AD-Server aus, dessen AD-Benutzergruppe Sie importieren möchten.
4. Klicken Sie auf "AD-Benutzergruppen importieren", um eine Liste der Benutzergruppenwerte abzurufen, die auf dem AD-Server gespeichert sind. Befinden sich noch nicht alle Benutzergruppen in CC-SG, können Sie diese hier importieren und ihnen Zugriffsrichtlinien zuordnen.
5. Wählen Sie die Gruppen aus, die Sie nach CC-SG importieren möchten.
   - Die Namen von importierten Benutzergruppen dürfen bis zu 64 Zeichen enthalten.
   - Geben Sie zur Suche nach Benutzergruppen einen Suchbegriff in das Feld "Suche für Gruppen" ein, und klicken Sie auf "Los".
   - Klicken Sie auf eine Spaltenüberschrift, um die Liste der Benutzergruppen nach den Daten in der Spalte zu sortieren.
   - Klicken Sie auf "Alles auswählen", um alle Benutzergruppen zum Importieren auszuwählen.

- Klicken Sie auf "Gesamte Auswahl aufheben", um die Auswahl aller Benutzergruppen aufzuheben.

6. Wählen Sie in der Spalte "Richtlinien" eine CC-SG-Zugriffsrichtlinie in der Liste aus, um die Richtlinie der ausgewählten Gruppe zuzuordnen.
7. Klicken Sie auf "Importieren", um die ausgewählten Benutzergruppen zu importieren.

Tipp: Klicken Sie zum Überprüfen, dass die Gruppe ordnungsgemäß importiert wurde, und zum Anzeigen der Rechte dieser gerade importierten Gruppe auf die Registerkarte "Benutzer". Wählen Sie dann die importierte Gruppe aus, um das Fenster "Benutzergruppenprofil" anzuzeigen. Prüfen Sie die Daten auf den Registerkarten "Berechtigungen" und "Geräte-/Knotenrichtlinien". Klicken Sie auf die Registerkarte "Active Directory Associations" (Active Directory-Zuordnungen), um die Daten für das AD-Modul anzuzeigen, das mit der Benutzergruppe verknüpft ist.

Active Directory mit CC-SG synchronisieren

Die in CC-SG gespeicherten Daten können mithilfe mehrerer Methoden mit den Informationen auf Ihrem AD-Server synchronisiert werden.

- Tägliche Synchronisierung aller Module: Sie können die geplante Synchronisierung aktivieren, damit CC-SG alle AD-Module täglich zu der ausgewählten Uhrzeit synchronisieren kann. Siehe ***Alle AD-Module synchronisieren*** (auf Seite 238). Diese Synchronisierung ist nur erforderlich, wenn Sie Active Directory für die Autorisierung verwenden.
- Geplante Synchronisierung mit dem Aufgabenmanager: Siehe ***Aufgaben planen*** (auf Seite 332).
- Manuelle Synchronisierung: Bei dieser Methode können Sie zwei Typen von Synchronisierungen durchführen:
  1. **Alle Active Directory-Module:** Bei dieser Option wird der gleiche Vorgang wie bei der täglichen Synchronisierung aller Module durchgeführt. Sie können diese Synchronisierung jedoch jederzeit manuell durchführen. Diese Synchronisierung ist nur erforderlich, wenn Sie Active Directory für die Autorisierung verwenden. Siehe ***Alle AD-Module synchronisieren*** (auf Seite 238).

2. **Alle Benutzergruppen:** Verwenden Sie diese Option, wenn Sie eine Benutzergruppe geändert haben. Die Synchronisierung aller Benutzergruppen ermöglicht Ihnen, importierte und lokale Benutzergruppen den Benutzergruppen zuzuordnen, die als Teil eines AD-Moduls identifiziert wurden. Bei der Synchronisierung von Benutzergruppen werden die Zugriffsinformationen in CC-SG nicht aktualisiert. Zur Aktualisierung der Zugriffsinformationen müssen Sie alle AD-Module synchronisieren. Warten Sie hierzu entweder auf die Ausführung der täglichen Synchronisierung, oder führen Sie die Synchronisierung aller Module manuell aus. Siehe ***Alle Benutzergruppen mit Active Directory synchronisieren*** (auf Seite 237).

Alle Benutzergruppen mit Active Directory synchronisieren

Sie müssen alle Benutzergruppen synchronisieren, wenn Sie eine Benutzergruppe geändert haben, z. B. wenn Sie eine Benutzergruppe von einem AD-Modul in ein anderes verschoben haben. Sie können auch die AD-Zuordnung einer Benutzergruppe manuell ändern. Dies führen Sie auf der Registerkarte "Active Directory-Zuordnungen" des Benutzergruppenprofils durch.

Wenn Sie die Benutzer oder Domänencontroller geändert haben, sollten Sie alle AD-Module synchronisieren. Siehe ***Alle AD-Module synchronisieren*** (auf Seite 238).

Beim Synchronisieren von AD-Benutzergruppen ruft CC-SG die Gruppen für das ausgewählte AD-Modul ab, vergleicht die Namen mit den Benutzergruppen in CC-SG und ermittelt die Übereinstimmungen. Die Ergebnisse werden in CC-SG angezeigt, und Sie können auswählen, welche Gruppen in Active Directory Sie CC-SG zuweisen möchten. Hierbei werden die Benutzerzugriffsinformationen in CC-SG nicht aktualisiert. Bei der Synchronisierung von AD-Benutzergruppen werden nur die Gruppennamen aus Active Directory zu CC-SG zugeordnet.

So synchronisieren Sie alle Benutzergruppen mit Active Directory:

1. Wählen Sie "Administration > Sicherheit".
2. Klicken Sie auf die Registerkarte "Authentifizierung". Alle konfigurierten Autorisierungs- und Authentifizierungsserver werden in einer Tabelle angezeigt.
3. Wählen Sie den AD-Server aus, dessen Benutzergruppen Sie mit den Benutzergruppen in CC-SG synchronisieren möchten.
4. Wählen Sie in der Liste "Manuelle Synchronisierung" die Option "Alle Benutzergruppen" aus, und klicken Sie dann auf "Jetzt synchronisieren".

5. Eine Liste aller im AD-Modul gefundenen Benutzergruppen, deren Namen mit Benutzergruppen in CC-SG übereinstimmen, wird angezeigt. Wählen Sie die Benutzergruppen aus, die Sie synchronisieren möchten, und klicken Sie dann auf OK.

   Eine Bestätigung wird angezeigt, sobald alle importieren Benutzergruppen des ausgewählten Moduls erfolgreich synchronisiert wurden.

Alle AD-Module synchronisieren

Sie sollten alle AD-Module immer dann synchronisieren, wenn Sie einen Benutzer in Active Directory ändern oder löschen, Benutzerberechtigungen in AD ändern oder einen Domänencontroller ändern.

Wenn Sie alle AD-Module synchronisieren, ruft CC-SG die Benutzergruppen für alle konfigurierten AD-Module ab, vergleicht die Namen mit den Benutzergruppen, die in CC-SG importiert oder dem AD-Modul in CC-SG zugewiesen wurden, und aktualisiert den lokalen CC-SG-Cache. Der lokale CC-SG-Cache enthält alle Domänencontroller für jede Domäne, alle Benutzergruppen, die Modulen in CC-SG zugewiesen sind, sowie die Benutzerdaten für alle bekannten AD-Benutzer. Wurden Benutzergruppen aus den AD-Modulen gelöscht, entfernt CC-SG alle Zuordnungen zu der gelöschten Gruppe aus dem lokalen Cache. Dadurch wird sichergestellt, dass CC-SG über die aktuellen AD-Benutzergruppendaten verfügt.

So synchronisieren Sie alle AD-Module:

1. Wählen Sie "Administration > Sicherheit".
2. Klicken Sie auf die Registerkarte "Authentifizierung". Alle konfigurierten Autorisierungs- und Authentifizierungsserver werden in einer Tabelle angezeigt.
3. Wählen Sie in der Liste "Manuelle Synchronisierung" die Option "Alle Active Directory-Module" aus, und klicken Sie dann auf "Jetzt synchronisieren". Nachdem alle AD-Module erfolgreich synchronisiert wurden, wird eine Bestätigungsmeldung angezeigt.

Wenn Sie das Kennwort eines Benutzers in MSFT Windows Server 2003 AD ändern, stehen sowohl das alte als auch das neue Kennwort für ca. 30 Minuten zur Verfügung. Während dieses Zeitraums kann sich der Benutzer mit einem dieser Kennwörter bei CC-SG anmelden. Dies liegt daran, dass AD das alte Kennwort für ca. 30 Minuten im Cache-Speicher ablegt, bevor das neue Kennwort vollständig aktualisiert wurde.

Tägliche Synchronisierung aller AD-Module aktivieren oder deaktivieren

Um die Synchronisierung häufiger durchzuführen, planen Sie eine Aufgabe zum Synchronisieren aller AD-Module. Siehe ***Aufgaben planen*** (auf Seite 332).

So aktivieren Sie die tägliche Synchronisierung aller AD-Module:

1. Wählen Sie "Administration > Sicherheit".
2. Klicken Sie auf die Registerkarte "Authentifizierung". Alle konfigurierten Autorisierungs- und Authentifizierungsserver werden in einer Tabelle angezeigt.
3. Markieren Sie das Kontrollkästchen Tägliche Synchronisierung aller Module".
4. Klicken Sie im Feld "Synchronisierungszeitpunkt" auf die Pfeile nach oben oder unten, um die Uhrzeit auszuwählen, zu der CC-SG die tägliche Synchronisierung der AD-Module ausführen soll.
5. Klicken Sie zum Speichern der Änderungen auf "Aktualisieren".

So deaktivieren Sie die tägliche Synchronisierung aller AD-Module:

1. Wählen Sie "Administration > Sicherheit".
2. Klicken Sie auf die Registerkarte "Authentifizierung". Alle konfigurierten Autorisierungs- und Authentifizierungsserver werden in einer Tabelle angezeigt.
3. Heben Sie die Markierung des Kontrollkästchens "Tägliche Synchronisierung aller Module" auf.
4. Klicken Sie zum Speichern der Änderungen auf "Aktualisieren".

Täglichen AD-Synchronisierungszeitpunkt ändern

Wenn die tägliche Synchronisierung aktiviert ist, können Sie den Zeitpunkt festlegen, zu dem die automatische Synchronisierung durchgeführt wird. Die tägliche Synchronisierung wird standardmäßig um 23:30 Uhr durchgeführt.

So ändern Sie den täglichen AD-Synchronisierungszeitpunkt:

1. Wählen Sie "Administration > Sicherheit".
2. Wählen Sie die Registerkarte "Authentifizierung". Stellen Sie sicher, dass das Kontrollkästchen "Tägliche Synchronisierung aller Module" markiert ist.

3. Klicken Sie unten im Feld "Synchronisierungszeitpunkt" auf die Pfeile nach oben oder unten, um die Uhrzeit auszuwählen, zu der CC-SG die tägliche Synchronisierung der AD-Module ausführen soll.
4. Klicken Sie zum Speichern der Änderungen auf "Aktualisieren".

Umbenennen und Verschieben von AD-Gruppen

Umbenennen einer Gruppe in AD:

Wenn eine in CC-SG importierte AD-Gruppe ihren Namen in AD ändert, gibt CC-SG bei Feststellung der Namensänderung eine Warnmeldung in der Überwachungsliste aus. Dies kann entweder im Rahmen der Synchronisierung erfolgen oder wenn sich ein betroffener AD-Benutzer zum ersten Mal danach anmeldet.

```
"Benutzergruppe <Gruppenname> wurde im AD-Modul
<Modulname> in <Gruppe neuer Name> umbenannt."
```

Löschen oder Verschieben einer Gruppe in AD:

Wenn eine in CC-SG importierte AD-Gruppe aus der Suchdatenbank der Gruppe gelöscht oder verschoben wurde, gibt CC-SG eine Warnmeldung in der Überwachungsliste aus. Die AD-Verknüpfung für die Gruppe wird entfernt.

```
"Benutzergruppe <Gruppenname> kann im AD-Modul
<Modulname> nicht gefunden werden."
```

So verschieben Sie eine Gruppe in AD innerhalb der Suchdatenbank:

Wenn eine AD-Gruppe innerhalb der Suchdatenbank verschoben wird, wird keine Warnmeldung ausgegeben, und die Gruppe funktioniert wie gewohnt.

LDAP und CC-SG

Nach dem Starten von CC-SG und der Eingabe eines Benutzernamens und Kennworts wird eine Abfrage entweder über CC-SG oder direkt an den LDAP-Server weitergeleitet. Stimmen der Benutzername und das Kennwort mit denjenigen im LDAP-Verzeichnis überein, wird der Benutzer authentifiziert. Der Benutzer wird dann für die lokalen Benutzergruppen auf dem LDAP-Server autorisiert.

LDAP-Module (Netscape) zu CC-SG hinzufügen

So fügen Sie ein LDAP-Modul (Netscape) zu CC-SG hinzu:

1. Wählen Sie "Administration > Sicherheit".

2. Klicken Sie auf die Registerkarte "Authentifizierung".
3. Klicken Sie auf "Hinzufügen", um das Fenster "Modul hinzufügen" zu öffnen.
4. Klicken Sie auf das Dropdown-Menü "Modultyp", und wählen Sie LDAP in der Liste aus.
5. Geben Sie den Namen des LDAP-Servers in das Feld "Modulname" ein.
6. Klicken Sie auf "Weiter". Die Registerkarte "Allgemein" wird angezeigt.

Allgemeine LDAP-Einstellungen

1. Klicken Sie auf die Registerkarte "Allgemein".
2. Geben Sie die IP-Adresse oder den Hostnamen des LDAP-Servers im Feld IP-Adresse/Hostname ein. Die Regeln zur Vergabe von Hostnamen werden unter ***Terminologie/Abkürzungen*** (auf Seite 2) beschrieben.
3. Geben Sie **den Portwert im Feld "Port" ein. Der Standardport lautet 389.**
4. Markieren Sie "LDAP over SSL" (LDAP über SSL), wenn Sie einen sicheren LDAP-Server verwenden.
5. Markieren Sie die Option "Anonyme Bindung", wenn Ihr LDAP-Server anonyme Abfragen zulässt. Sie müssen bei anonymen Verbindungen keinen Benutzernamen und kein Kennwort eingeben.

   Hinweis: Standardmäßig lässt Windows 2003 KEINE anonymen Abfragen zu. Windows 2000 Server lassen bestimmte anonyme Funktionen zu, wenn die Abfrageergebnisse auf den Berechtigungen für jedes Objekt beruhen.

6. Wenn Sie keine anonyme Verbindung verwenden, geben Sie einen Benutzernamen in das Feld Benutzername ein. Geben Sie einen DN (Distinguished Name) ein, um die Berechtigungen festzulegen, die beim Abfragen des LDAP-Servers verwendet werden. Geben Sie für den DN den allgemeinen Namen, die Organisationseinheit und Domäne ein.

   Geben Sie beispielsweise uid=admin,ou=Administrators,ou=TopologyManagement,o=Netscape Root ein. Trennen Sie die Werte durch Komma, verwenden Sie vor oder nach dem Komma jedoch keine Leerstellen. Die Werte können Leerstellen enthalten (z. B. Command Center).
7. Geben Sie das Kennwort in die Felder Kennwort und Kennwort bestätigen ein.

8. Geben Sie einen DN (Distinguished Name) im Feld Basis-DN ein, um anzugeben, wo die Suche nach Benutzern anfangen soll. Mit dem Wert ou=Administrators,ou=TopologyManagement,o=NetscapeRoot werden beispielsweise alle Organisationseinheiten der Domäne durchsucht.
9. Sie können die Suche auf bestimmte Objekttypen beschränken, indem Sie einen Wert im Feld Filter eingeben. Der Wert (objectclass=person) schränkt die Suche beispielsweise auf Personenobjekte ein.
10. Klicken Sie auf Verbindung testen, um den LDAP-Server mit den vorhandenen Parametern zu testen. Sie sollten eine Bestätigung über eine erfolgreiche Verbindung erhalten. Ist dies nicht der Fall, prüfen Sie die Einstellungen sorgfältig auf Fehler, und versuchen Sie es erneut.
11. Klicken Sie auf "Weiter", um die Registerkarte "Erweitert" anzuzeigen und die erweiterten Konfigurationsoptionen für den LDAP-Server einzustellen.

Erweiterte LDAP-Einstellungen

1. Klicken Sie auf die Registerkarte "Erweitert".
2. Wählen Sie "Base 64", wenn Sie das Kennwort mit Verschlüsselung zum LDAP-Server senden möchten. Wählen Sie "Unformatierter Text", wenn Sie das Kennwort als unformatierten Text zum LDAP-Server senden möchten.
3. Standarddigest: Wählen Sie die Standardverschlüsselung für Benutzerkennwörter aus.
4. Geben Sie die Parameter für die Benutzer- und Gruppenmitgliedschaftsattribute in die Felder "Benutzerattribute" und "Gruppenmitgliedschaftsattribute" ein. Diese Werte sollten Sie aus Ihrem LDAP-Verzeichnisschema abrufen.
5. Geben Sie das Bindungsmuster im Feld Benutzernamenmuster binden ein.
   - Aktivieren Sie Bindung verwenden, wenn CC-SG den Benutzernamen und das Kennwort, die bei der Anmeldung eingegeben wurden, zur Authentifizierung an den LDAP-Server senden soll. Ist Bindung verwenden nicht aktiviert, sucht CC-SG auf dem LDAP-Server nach dem Benutzernamen. Wird der Name gefunden, ruft CC-SG das LDAP-Objekt ab und vergleicht das zugeordnete Kennwort lokal mit dem eingegebenen Kennwort.

- Auf einigen LDAP-Servern kann das Kennwort nicht als Teil des LDAP-Objekts abgerufen werden. Aktivieren Sie das Kontrollkästchen "Bindung nach Suche verwenden", damit CC-SG das Kennwort wieder an das LDAP-Objekt bindet und es zur Authentifizierung an den Server zurücksendet.

6. Klicken Sie zum Speichern der Änderungen auf OK. Das neue LDAP-Modul wird im Fenster Sicherheitsmanager unter Externe AA-Server angezeigt.
7. Markieren Sie das Kontrollkästchen "Authentifizierung", wenn CC-SG die Benutzer mit dem LDAP-Modul authentifizieren soll.
8. Klicken Sie zum Speichern der Änderungen auf "Aktualisieren".

Konfigurationseinstellungen für Sun One LDAP (iPlanet)

Beispiel bei Verwendung eines Sun One LDAP-Server zur Remoteauthentifizierung:

Parametername	SUN One LDAP-Parameter
IP-Adresse/Hostname	<IP-Adresse des DNS-Servers>
Benutzername	CN=<Gültige Benutzer-ID>
Kennwort	<Kennwort>
Basis-DN	O=<Organisation>
Filter	(objectclass=person)
Kennwörter (Fenster Erweitert)	Unformatierter Text
Standarddigest für Kennwort (Erweitert):	SHA
Bindung verwenden	Deaktiviert
Bindung nach Suche verwenden	Aktiviert

Konfigurationseinstellungen für OpenLDAP (eDirectory)

Verwenden Sie bei einem OpenLDAP-Server für die Remoteauthentifizierung das folgende Beispiel:

Parametername	Open LDAP-Parameter
IP-Adresse/Hostname	<IP-Adresse des DNS-Servers>
Benutzername	CN=<Gültige Benutzer-ID>, O=<Organisation>
Kennwort	<Kennwort>
Benutzerbasis	O=accounts, O=<Organisation>
Benutzerfilter	(objectclass=person)

Parametername	Open LDAP-Parameter
Kennwörter (Fenster Erweitert)	Base64
Standarddigest für Kennwort (Erweitert):	Crypt
Bindung verwenden	Deaktiviert
Bindung nach Suche verwenden	Aktiviert

IBM LDAP-Konfigurationseinstellungen

Verwenden Sie bei einem IBM LDAP-Server für die Remoteauthentifizierung das folgende Beispiel:

Parametername	IBM LDAP-Parameter
IP-Adresse/Hostname	<IP-Adresse des DNS-Servers>
Benutzername	CN=<Gültige Benutzer-ID>
Kennwort	<Kennwort>
Benutzerbasis	Beispiel: cn=users,DC=raritan,DC=com,DC=us
Benutzerfilter	(objectclass=person)
Kennwörter (Fenster Erweitert)	Base64
Standarddigest für Kennwort (Erweitert):	Keine
Benutzerattribut	uid
Gruppenmitgliedschaftsattribut	Leer lassen.
Bindungsmuster für Benutzernamen	Beispiel: cn={0},cn=users,DC=raritan,DC=com,DC=us
Bindung verwenden	Deaktiviert
Bindung nach Suche verwenden	Aktiviert

TACACS+ und CC-SG

CC-SG-Benutzer, für die ein TACACS+-Server und Remoteauthentifizierung verwendet wird, müssen auf dem TACACS+-Server und in CC-SG erstellt werden. Der Benutzername, der für den TACACS+-Server verwendet wird, muss mit dem für CC-SG übereinstimmen; die Kennwörter dürfen jedoch voneinander abweichen. Siehe ***Benutzer und Benutzergruppen*** (auf Seite 185).

TACACS+-Module hinzufügen

So fügen Sie ein TACACS+-Modul hinzu:

1. Wählen Sie "Administration > Sicherheit".
2. Klicken Sie auf die Registerkarte "Authentifizierung".
3. Klicken Sie auf "Hinzufügen", um das Fenster "Modul hinzufügen" zu öffnen.
4. Wählen Sie "Modultyp" > "TACACS+".
5. Geben Sie den Namen des TACACS+-Servers in das Feld Modulname ein.
6. Klicken Sie auf "Weiter". Die Registerkarte "Allgemein" wird angezeigt.

Allgemeine TACACS+-Einstellungen

1. Geben Sie die IP-Adresse oder den Hostnamen des TACACS+-Servers im Feld "IP-Adresse/Hostname" ein. Die Regeln zur Vergabe von Hostnamen werden unter ***Terminologie/Abkürzungen*** (auf Seite 2) beschrieben.
2. Geben Sie die Portnummer in das Feld "Portnummer" ein, die der TACACS+-Server überwacht. Der Standardport lautet 49.
3. Geben Sie den Authentifizierungsport im Feld "Authentifizierungsport" ein.
4. Geben Sie den gemeinsamen Schlüssel in die Felder "Gemeinsamer Schlüssel" und "Bestätigung des gemeinsamen Schlüssels" ein. Der Name darf aus maximal 128 Zeichen bestehen.
5. Klicken Sie zum Speichern der Änderungen auf OK. Das neue TACACS+-Modul wird im Fenster "Sicherheitsmanager" unter "Externe AA-Server" angezeigt.
6. Markieren Sie das Kontrollkästchen "Authentifizierung", wenn CC-SG die Benutzer mit dem TACACS+-Modul authentifizieren soll.
7. Klicken Sie zum Speichern der Änderungen auf "Aktualisieren".

RADIUS und CC-SG

CC-SG-Benutzer, für die ein RADIUS-Server und Remoteauthentifizierung verwendet wird, müssen auf dem RADIUS-Server und in CC-SG erstellt werden. Der Benutzername, der für den RADIUS-Server verwendet wird, muss mit dem für CC-SG übereinstimmen. Die Kennwörter dürfen jedoch voneinander abweichen. Siehe ***Benutzer und Benutzergruppen*** (auf Seite 185).

RADIUS-Module hinzufügen

So fügen Sie ein RADIUS-Modul hinzu:

1. Wählen Sie "Administration > Sicherheit".
2. Klicken Sie auf die Registerkarte "Authentifizierung".
3. Klicken Sie auf "Hinzufügen", um das Fenster "Modul hinzufügen" zu öffnen.
4. Klicken Sie auf das Dropdown-Menü "Modultyp", und wählen Sie RADIUS in der Liste aus.
5. Geben Sie den Namen des RADIUS-Servers in das Feld "Modulname" ein.
6. Klicken Sie auf "Weiter". Die Registerkarte "Allgemein" wird angezeigt.

Allgemeine RADIUS-Einstellungen

1. Klicken Sie auf die Registerkarte "Allgemein".
2. Geben Sie die IP-Adresse oder den Hostnamen des RADIUS-Servers im Feld "IP-Adresse/Hostname" ein. Die Regeln zur Vergabe von Hostnamen werden unter ***Terminologie/Abkürzungen*** (auf Seite 2) beschrieben.
3. Geben Sie die Portnummer im Feld "Portnummer" ein. Der Standardport lautet 1812.
4. Geben Sie den Authentifizierungsport im Feld "Authentifizierungsport" ein.
5. Geben Sie den gemeinsamen Schlüssel in die Felder "Gemeinsamer Schlüssel" und "Bestätigung des gemeinsamen Schlüssels" ein.
6. Klicken Sie zum Speichern der Änderungen auf OK.
7. Das neue RADIUS-Modul wird im Fenster "Sicherheitsmanager" unter "Externe AA-Server" angezeigt. Markieren Sie das Kontrollkästchen "Authentifizierung", wenn CC-SG die Benutzer mit dem RADIUS-Modul authentifizieren soll.
8. Klicken Sie zum Speichern der Änderungen auf "Aktualisieren".

Zwei-Faktoren-Authentifizierung mit RADIUS

Mithilfe eines RSA RADIUS-Servers, der die Zwei-Faktoren-Authentifizierung in Verbindung mit einem RSA-Authentifizierungsmanager verwendet, kann CC-SG die Zwei-Faktoren-Authentifizierung mit dynamischen Token nutzen.

In einer solchen Umgebung melden sich die Benutzer bei CC-SG an, indem sie zunächst ihren Benutzernamen in das Feld "Benutzername", dann ihr festgelegtes Kennwort und dann den Wert für den dynamischen Token in das Feld "Kennwort" eingeben.

CC-SG wird wie bei der standardmäßigen RADIUS-Remoteauthentifizierung (wie oben beschrieben) konfiguriert. Siehe ***Zwei-Faktoren-Authentifizierung* (auf Seite 444).**

Kapitel 13 Berichte

In diesem Kapitel

Berichte verwenden 248
Überwachungslistenbericht 251
Fehlerprotokollbericht 252
Zugriffsbericht 252
Verfügbarkeitsbericht 253
Bericht „Aktive Benutzer“ 254
Bericht "Gesperrte Benutzer" 254
Bericht "Alle Benutzerdaten" 254
Bericht "Benutzergruppendaten" 255
Geräteanlagenbericht 256
Bericht "Gerätegruppendaten" 256
Portabfragebericht 256
Knotenanlagebericht 258
Bericht „Aktive Knoten“ 259
Knotenerstellungsbericht 259
Bericht "Knotengruppendaten" 260
AD-Benutzergruppenbericht 260
Geplante Berichte 261
Bericht "Gerätefirmware aktualisieren" 262

Berichte verwenden

Die Benutzerrichtlinie ist der Standardfilter für alle Berichte. Beispielsweise werden die Knoten oder Geräte, auf die der Benutzer keinen Zugriff hat, nicht in den Berichten angezeigt.

Berichtsdaten sortieren

- Klicken Sie auf eine Spaltenüberschrift, um die Berichtsdaten nach den Werten in der Spalte zu sortieren. Die Daten werden in aufsteigender Reihenfolge alphabetisch, numerisch oder chronologisch angezeigt.
- Klicken Sie erneut auf die Spaltenüberschrift, um die Daten in absteigender Reihenfolge zu sortieren.

Spaltenbreite in Berichten vergrößern/verkleinern

Die ausgewählten Spaltenbreiten werden bei der nächsten Anmeldung und Ausführung von Berichten als Standardberichtsansicht verwendet.

1. Positionieren Sie Ihren Mauszeiger auf der Spaltentrennung in der obersten Zeile, bis der Mauszeiger als Pfeil mit zwei Spitzen angezeigt wird.

2. Klicken Sie und ziehen Sie den Pfeil nach links oder rechts, um die Spaltenbreite anzupassen.

Berichtsdetails anzeigen

- Doppelklicken Sie auf eine Zeile, um die Berichtsdetails anzuzeigen.
- Ist die Zeile hervorgehoben, drücken Sie die Eingabetaste, um Details anzuzeigen.

Es werden nicht nur die Einzelheiten, die in einem Berichtsfenster angezeigt werden, sondern alle Einzelheiten des ausgewählten Berichts in einem Dialogfeld angezeigt. Beispielsweise wird im Bildschirm "Zugriffsbericht" für Knoten weder der Schnittstellentyp noch die Meldung angezeigt. Diese Informationen werden jedoch im Dialogfeld "Knotenzugriffsdetails" angezeigt.

In mehrseitigen Berichten navigieren

- Klicken Sie auf die Pfeile unten im Bericht, um in mehrseitigen Berichten zu navigieren.

Berichte drucken

In CC-SG gibt es zwei Druckoptionen. Sie können eine Berichtsseite so drucken, wie sie auf dem Bildschirm angezeigt wird (Screenshot drucken), oder Sie können einen vollständigen Bericht mit allen Details für jedes Element drucken.

Hinweis: Die Druckoptionen können für alle CC-SG-Seiten verwendet werden.

So drucken Sie einen Screenshot eines Berichts:

1. Erstellen Sie den Bericht, den Sie drucken möchten.
2. Wählen Sie "Secure Gateway > Fenster drucken".

So drucken Sie alle Berichtsdetails:

1. Erstellen Sie den Bericht, den Sie drucken möchten. Stellen Sie sicher, dass im Feld "Anzuzeigende Einträge" die Option "Alle" ausgewählt ist.
2. Wählen Sie "Secure Gateway > Drucken".

Berichte in Dateien speichern

Sie können einen Bericht in einer CSV-Datei speichern, die in Excel geöffnet werden kann. Beim Speichern eines Berichts in einer Datei werden alle Berichtsdetails gespeichert; nicht nur die Details, die Sie im Berichtsfenster anzeigen können. Beispielsweise werden im Bildschirm "Zugriffsbericht" für Knoten die Spalten "Typ" und "Meldung" nicht angezeigt. Diese Informationen sind verfügbar, nachdem Sie den Zugriffsbericht gespeichert und in Excel geöffnet haben.

1. Erstellen Sie den Bericht, den Sie in einer Datei speichern möchten.
2. Klicken Sie auf "In Datei speichern".
3. Geben Sie einen Namen für die Datei ein, und wählen Sie den Speicherort aus.
4. Klicken Sie auf Speichern.

Berichtsdaten aus CC-SG leeren

Sie können die Daten, die im Überwachungslistenbericht und Fehlerprotokollbericht enthalten sind, leeren. Beim Leeren dieser Berichte werden alle Daten gelöscht, die den verwendeten Suchkriterien entsprechen. Wenn Sie z. B. alle Überwachungslisteneinträge vom 26. März 2008 bis zum 27. März 2008 suchen, werden nur diese Datensätze geleert. Einträge vor dem 26. März oder nach dem 27. März bleiben in der Überwachungsliste.

Geleerte Daten werden permanent aus CC-SG entfernt.

So leeren Sie Berichtsdaten aus CC-SG:

1. Erstellen Sie den Bericht, dessen Daten Sie aus CC-SG löschen möchten.
2. Klicken Sie auf "Leeren".
3. Klicken Sie zum Bestätigen auf "Ja".

Berichtsfilter ausblenden oder einblenden

In einigen Berichten sind oben im Berichtsfenster Filterkriterien enthalten. Sie können den Filterbereich ausblenden, wodurch der Berichtsbereich erweitert wird.

So blenden Sie die Berichtsfilter aus oder ein:

- Klicken Sie oben im Fenster auf die Filtersymbolleiste, um den Filterbereich auszublenden.
- Klicken Sie erneut auf die Filtersymbolleiste, um den Filterbereich einzublenden.

Überwachungslistenbericht

CC-SG verwaltet eine Überwachungsliste für Ereignisse im System: In der Überwachungsliste werden Ereignisse wie Hinzufügen, Bearbeiten oder Löschen von Geräten oder Ports und andere Änderungen am System aufgezeichnet.

Hinweis: Wenn ein Benutzer eine Verbindung zu einem mit einem Lesezeichen versehenen Port herstellt, wird dies in der Überwachungsliste vermerkt. Es wird jedoch erst ein Eintrag für die Abmeldung vorgenommen, wenn die zum Herstellen der Verbindung genutzte Browserinstanz geschlossen wird.

So erstellen Sie den Überwachungslistenbericht:

1. Wählen Sie "Berichte > Überwachungsliste".
2. Legen Sie den Datumsbereich für den Bericht in den Feldern "Startdatum" und "Startzeit" sowie "Enddatum" und "Endzeit" fest. Klicken Sie auf jede Komponente des Standarddatums (Monat, Tag, Jahr, Stunde, Minute), um sie auszuwählen, und legen Sie den gewünschten Wert fest, indem Sie auf die Pfeile nach oben und nach unten klicken.
3. Sie können die Daten im Bericht einschränken, indem Sie weitere Parameter in die Felder "Meldungstyp", "Meldung", "Benutzername" und "Benutzer-IP-Adresse" eingeben. In diese Felder, ausgenommen dem Feld "Meldungstyp" können Platzhalter eingegeben werden.
   - Wählen Sie einen Typ im Feld "Meldungstyp" aus, um den Bericht auf einen Meldungstyp zu beschränken.
   - Wenn Sie den Bericht auf Meldungstexte beschränken möchten, die mit einer Aktivität verknüpft sind, geben Sie den Text in das Feld "Meldung" ein.
   - Wenn Sie den Bericht auf bestimmte Benutzeraktivitäten beschränken möchten, geben Sie den Benutzernamen in das Feld "Benutzername" ein.
   - Wenn Sie den Bericht auf bestimmte IP-Adressen-Aktivitäten beschränken möchten, geben Sie die IP-Adresse des Benutzers in das Feld "Benutzer-IP-Adresse" ein.
4. Wählen Sie im Feld "Anzuzeigende Einträge" die Anzahl an Einträgen aus, die im Berichtsfenster angezeigt werden sollen.
5. Klicken Sie zum Erstellen des Berichts auf "Übernehmen".
   - Klicken Sie auf "Leeren", um die Datensätze im Bericht zu leeren. Siehe ***Berichtsdaten aus CC-SG leeren*** (auf Seite 250).

Fehlerprotokollbericht

CC-SG speichert Fehlermeldungen in verschiedenen Fehlerprotokolldateien, die aufgerufen und zum Beheben von Problemen verwendet werden können. Das Fehlerprotokoll enthält einen Teil der Überwachungslisteneinträge, die einer Fehlerbedingung zugewiesen sind.

So erstellen Sie den Fehlerprotokollbericht:

1. Wählen Sie "Berichte > Fehlerprotokoll".
2. Legen Sie den Datumsbereich für den Bericht in den Feldern "Startdatum" und "Startzeit" sowie "Enddatum" und "Endzeit" fest. Klicken Sie auf jede Komponente des Standarddatums (Monat, Tag, Jahr, Stunde, Minute), um sie auszuwählen, und legen Sie den gewünschten Wert fest, indem Sie auf die Pfeile nach oben und nach unten klicken.
3. Sie können die Daten im Bericht einschränken, indem Sie weitere Parameter in die Felder "Meldung", "Benutzername" und "Benutzer-IP-Adresse eingeben". In diese Felder können Platzhalter eingegeben werden.
   - Wenn Sie den Bericht auf Meldungstexte beschränken möchten, die mit einer Aktivität verknüpft sind, geben Sie den Text in das Feld "Meldung" ein.
   - Wenn Sie den Bericht auf bestimmte Benutzeraktivitäten beschränken möchten, geben Sie den Benutzernamen in das Feld "Benutzername" ein.
   - Wenn Sie den Bericht auf bestimmte IP-Adressen-Aktivitäten beschränken möchten, geben Sie die IP-Adresse des Benutzers in das Feld "Benutzer-IP-Adresse" ein.
4. Wählen Sie im Feld "Anzuzeigende Einträge" die Anzahl an Einträgen aus, die im Berichtsfenster angezeigt werden sollen.
5. Klicken Sie zum Erstellen des Berichts auf "Übernehmen".
   - Klicken Sie auf "Leeren", um das Fehlerprotokoll zu löschen. Siehe ***Berichtsdaten aus CC-SG leeren*** (auf Seite 250).

Zugriffsbericht

Erstellen Sie den Zugriffsbericht, um folgende Informationen anzuzeigen: alle Geräte und Knoten, auf die zugegriffen wurde, den Zeitpunkt des Zugriffs und den Benutzer, der zugegriffen hat.

So erstellen Sie den Zugriffsbericht:

1. Wählen Sie "Berichte > Zugriffsbericht".

2. Wählen Sie "Geräte" oder "Knoten".
3. Legen Sie den Datums- und Zeitbereich für den Bericht in den Feldern "Startdatum" und "Startzeit" sowie "Enddatum" und "Endzeit" fest. Klicken Sie auf jede Komponente des Standarddatums (Monat, Tag, Jahr, Stunde, Minute), um sie auszuwählen, und legen Sie den gewünschten Wert fest, indem Sie auf die Pfeile nach oben und nach unten klicken.
4. Sie können die Daten im Bericht einschränken, indem Sie weitere Parameter in die Felder "Gerätename", "Knotenname", "Benutzername" und "Benutzer-IP-Adresse" eingeben. In diese Felder können Platzhalter eingegeben werden.
   - Wenn Sie den Bericht auf Meldungstexte beschränken möchten, die mit einer Aktivität verknüpft sind, geben Sie den Text in das Feld "Meldung" ein.
   - Wenn Sie den Bericht auf ein bestimmtes Gerät beschränken möchten, geben Sie den Gerätenamen in das Feld "Gerätename" ein.
   - Wenn Sie den Bericht auf einen bestimmten Knoten beschränken möchten, geben Sie den Portnamen in das Feld "Knotenname(n)" ein.
   - Wenn Sie den Bericht auf bestimmte Benutzeraktivitäten beschränken möchten, geben Sie den Benutzernamen in das Feld "Benutzername(n)" ein.
   - Wenn Sie den Bericht auf bestimmte IP-Adressen-Aktivitäten beschränken möchten, geben Sie die IP-Adresse des Benutzers in das Feld "IP-Adresse(n)" ein.
5. Wählen Sie im Feld "Anzuzeigende Einträge" die Anzahl an Einträgen aus, die im Berichtsfenster angezeigt werden sollen.
6. Klicken Sie zum Erstellen des Berichts auf "Übernehmen".

Verfügbarkeitsbericht

Der Verfügbarkeitsbericht zeigt den Status aller Verbindungen zu Geräten und Knoten an. Dieser Bericht vermittelt einen vollständigen Überblick über die Verfügbarkeit aller Geräte oder Knoten in Ihrem von CC-SG verwalteten Netzwerk.

So erstellen Sie den Verfügbarkeitsbericht:

1. Wählen Sie "Berichte > Verfügbarkeitsbericht".
2. Wählen Sie "Knoten" oder "Geräte".
3. Klicken Sie auf Übernehmen.

Bericht „Aktive Benutzer“

Der Bericht „Aktive Benutzer“ enthält alle aktuellen Benutzer und Benutzersitzungen. Sie können aktive Benutzer im Bericht auswählen und bei CC-SG abmelden.

So erstellen Sie den Bericht „Aktive Benutzer“:

- Wählen Sie "Berichte > Benutzer > Aktive Benutzer".

So melden Sie einen Benutzer während einer aktiven Sitzung in CC-SG ab:

1. Wählen Sie im Bericht "Aktive Benutzer" den Benutzernamen aus, den Sie abmelden möchten.
2. Klicken Sie auf "Abmelden".

Bericht "Gesperrte Benutzer"

Der Bericht "Gesperrte Benutzer" zeigt die Benutzer an, die zurzeit in CC-SG gesperrt sind, da zu viele fehlerhafte Anmeldeversuche aufgetreten sind. Sie können die Sperre für Benutzer im Bericht aufheben. Siehe ***Sperreinstellungen*** (auf Seite 320).

So erstellen Sie den Bericht "Gesperrte Benutzer":

- Wählen Sie "Berichte > Benutzer > Gesperrte Benutzer".

So heben Sie die Sperre für einen Benutzer, der für CC-SG gesperrt war, wieder auf:

- Wählen Sie den Benutzer aus, dessen Sperre Sie aufheben möchten, und klicken Sie auf "Benutzersperre aufheben".

Bericht "Alle Benutzerdaten"

Der Benutzerdatenbericht enthält bestimmte Daten über alle Benutzer in der CC-SG-Datenbank.

So erstellen Sie den Bericht "Alle Benutzerdaten":

- Wählen Sie "Berichte > Benutzer > Alle Benutzerdaten".
  - Im Feld "Benutzername" werden die Benutzernamen aller CC-SG-Benutzer angezeigt.

- Das Feld "Aktiviert" enthält den Wert "wahr", wenn der Benutzer sich bei CC-SG anmelden darf, bzw. "falsch", wenn der Benutzer sich nicht bei CC-SG anmelden darf. Dies hängt davon ab, ob die Option "Anmeldung aktiviert" im Benutzerprofil markiert ist. Siehe ***Benutzer hinzufügen*** (auf Seite 194).
- Im Feld "Gültigkeitsdauer des Kennworts" wird die Anzahl von Tagen angezeigt, die der Benutzer dasselbe Kennwort verwenden kann, bevor es geändert werden muss. Siehe ***Benutzer hinzufügen*** (auf Seite 194).
- Im Feld "Gruppen" werden die Benutzergruppen angezeigt, denen der Benutzer angehört.
- Im Feld "Berechtigungen" werden die CC-SG-Berechtigungen angezeigt, die dem Benutzer zugewiesen wurden. Siehe ***Benutzergruppenberechtigungen*** (auf Seite 421).
- Im Feld "E-Mail "wird die E-Mail-Adresse des Benutzers angezeigt, die im Benutzerprofil angegeben wurde.
- Im Feld "Benutzertyp" wird abhängig von der Zugriffsmethode des Benutzers "Lokal" oder "Remote" angezeigt.

Bericht "Benutzergruppendaten"

Der Bericht "Benutzergruppendaten" enthält Informationen über die Benutzer und Gruppen, denen sie zugewiesen sind.

So erstellen Sie den Bericht "Benutzergruppendaten":

1. Wählen Sie "Berichte > Benutzer > Benutzergruppendaten".
2. Doppelklicken Sie auf die Benutzergruppe, um die zugeordneten Richtlinien anzuzeigen.

Geräteanlagenbericht

Der Geräteanlagenbericht enthält Daten zu Geräten, die zurzeit von CC-SG verwaltet werden.

So erstellen Sie den Geräteanlagenbericht:

- Wählen Sie "Berichte > Knoten > Geräteanlagenbericht". Der Bericht wird für alle Geräte erzeugt.

So filtern Sie die Berichtsdaten nach dem Gerätetyp:

- Wählen Sie einen Gerätetyp aus, und klicken Sie dann auf "Übernehmen". Der Bericht wird erneut mit dem ausgewählten Filter generiert.
  - Bei Geräten, deren Version nicht der Kompatibilitätsmatrix entspricht, wird der Text im Feld "Gerätename" rot angezeigt.

Bericht "Gerätegruppendaten"

Der Bericht "Gerätegruppendaten" zeigt Gerätegruppeninformationen.

So erstellen Sie den Bericht "Gerätegruppendaten":

1. Wählen Sie "Berichte > Geräte > Gerätegruppendaten".
2. Doppelklicken Sie auf eine Zeile, um die Liste der Geräte in der Gruppe anzuzeigen.

Portabfragebericht

Im Portabfragebericht werden alle Ports nach Portstatus aufgelistet.

So erstellen Sie den Portabfragebericht:

1. Wählen Sie "Berichte > Ports > Port abfragen".
2. Wählen Sie im Bereich "Portstatus/Verfügbarkeit" den Portstatus aus, den der Bericht enthalten soll. Durch das Markieren mehrerer Kontrollkästchen werden Ports mit allen ausgewählten Statuszuständen eingeschlossen. Sie müssen mindestens eine Verfügbarkeitsoption auswählen, wenn eine Statusoption festgelegt ist.

Statustyp	Portstatus	Definition
	Alle	Alle Ports.
Status:		

Statustyp	Portstatus	Definition
	Verfügbar	
	Nicht verfügbar	Die Verbindung zum Port ist nicht möglich, da das Gerät ausgeschaltet und nicht verfügbar ist.
Verfügbarkeit:		
	Leerlauf	Der Port ist konfiguriert, und eine Verbindung zum Port ist möglich.
	Verbunden	
	Beschäftigt	Ein Benutzer ist mit diesem Port verbunden.
	Eingeschaltet	
	Ausgeschaltet	
Nicht konfiguriert:		
	Neu	Dem Port wurde ein neuer Zielserver angefügt, doch der Port wurde noch nicht konfiguriert.
	Nicht verwendet	An den Port ist kein Zielserver angeschlossen, und der Port wurde nicht konfiguriert.

3. Markieren Sie "Verwaiste Ports", um verwaiste Ports einzuschließen. Ein verwaister Port kann entstehen, wenn ein CIM- oder Zielserver im Paragon-System entfernt oder (manuell oder unbeabsichtigt) abgeschaltet wird. Siehe das **Benutzerhandbuch für Paragon II-Geräte von Raritan**. **Optional.**
4. Markieren Sie "Angehaltene Ports" oder "Gesperrte Ports", um angehaltene oder gesperrte Ports einzuschließen. Angehaltene Ports entstehen, wenn die CC-SG-Verwaltung eines Geräts angehalten wurde. Gesperrte Ports entstehen, wenn ein Gerät aktualisiert wird. **Optional.**
5. Wählen Sie die Anzahl an Datenzeilen aus, die im Berichtsfenster im Feld "Anzuzeigende Einträge" angezeigt werden sollen.

   Hinweis: Diese Einstellung gilt nicht, wenn der Bericht als Aufgabe erstellt wird.

6. Klicken Sie zum Erstellen des Berichts auf "Übernehmen".

Knotenanlagebericht

Der Knotenanlagebericht zeigt den Knotennamen, Schnittstellennamen und -typ, Gerätenamen und -typ und die Knotengruppe für alle Knoten an, die in CC-SG verwaltet werden. Sie können Filter für den Bericht verwenden, damit nur Daten für Knoten angezeigt werden, die bestimmten Werten für Knotengruppe, Schnittstellentyp, Gerätetyp oder Gerät entsprechen.

So erstellen Sie den Knotenanlagebericht:

1. Wählen Sie "Berichte > Knoten > Knotenanlagebericht".
2. Wählen Sie die Filterkriterien aus, die Sie auf den Bericht anwenden möchten. Die folgenden Kriterien sind verfügbar: Alle Knoten, Knotengruppe, Gerätegruppe und Geräte.
   - Wenn Sie "Knotengruppe", "Schnittstellentyp" oder "Gerätegruppe" wählen, müssen Sie einen Parameter aus dem entsprechenden Menü auswählen.
   - Wenn Sie "Geräte" auswählen, wählen Sie in der Liste "Verfügbar" die Geräte aus, deren Knotenanlagen im Bericht enthalten sein sollen. Klicken Sie dann auf "Hinzufügen", um sie in die Liste "Ausgewählt" zu verschieben.
3. Klicken Sie zum Erstellen des Berichts auf "Übernehmen". Der Knotenanlagebericht wird erstellt.

So erhalten Sie Lesezeichen-URLs für Knoten:

1. Generieren Sie den Knotenanlagenbericht, und doppelklicken Sie auf einen Knoten, um das Dialogfeld "Details" anzuzeigen.
2. Klicken Sie auf "In Datei speichern". Alle Berichtsinformationen werden in einer .csv-Datei gespeichert.
3. Die Spalte "URL" enthält direkte Links zu jedem Knoten. Sie können mit diesen Informationen eine Webseite mit Links zu jedem Knoten erstellen, anstatt jeden Knoten mit einem Lesezeichen zu versehen. Siehe ***Lesezeichen für Schnittstelle*** (auf Seite 161).

Bericht „Aktive Knoten“

Der Bericht "Aktive Knoten" enthält den Namen und Typ jeder aktiven Schnittstelle, den Verbindungsmodus, das zugehörige Gerät, einen Zeitstempel, den aktuellen Benutzer und die Benutzer-IP-Adresse für jeden Knoten mit einer aktiven Verbindung. Sie können die Liste der aktiven Knoten und getrennten Knoten in diesem Bericht anzeigen.

So erstellen Sie den Bericht "Aktive Knoten":

- Wählen Sie "Berichte > Knoten > Aktive Knoten". Der Bericht "Aktive Knoten" wird erstellt, falls aktive Knoten vorhanden sind.

So trennen Sie einen Knoten von einer aktiven Sitzung:

- Wählen Sie im Bericht "Aktive Knoten" den Knoten aus, den Sie trennen möchten, und klicken Sie dann auf "Trennen".

Knotenerstellungsbericht

Der Knotenerstellungsbericht führt alle Knotenerstellungs-Versuche auf, die in einem bestimmten Zeitfenster erfolgreich durchgeführt wurden oder fehlgeschlagen sind. Sie können festlegen, ob Sie alle derartigen Versuche oder nur solche Versuche anzeigen möchten, bei denen potenziell doppelte Knoten erstellt wurden.

So erstellen Sie den Knotenerstellungsbericht:

1. Wählen Sie "Berichte > Knoten > Knotenerstellung".
2. Wählen Sie "Alle Knoten" oder "Potentielle Duplikate" aus. "Potentielle Duplikate" beschränkt den Bericht auf die Knoten, die als potentielle Duplikate gekennzeichnet wurden.
3. Wenn Sie "Alle Knoten" ausgewählt haben, legen Sie den Datumsbereich für den Bericht in den Feldern "Startdatum" und "Startzeit" sowie "Enddatum" und "Endzeit" fest. Klicken Sie auf jede Komponente des Standarddatums (Monat, Tag, Jahr, Stunde, Minute), um sie auszuwählen, und legen Sie den gewünschten Wert fest, indem Sie auf die Pfeile nach oben und nach unten klicken.
4. Klicken Sie auf Übernehmen. Der Knotenerstellungsbericht wird erstellt.
   - Im Ergebnisfeld wird Erfolg, Fehlgeschlagen oder Potenzielle Duplikate angezeigt, um den Status nach dem Knotenerstellungs-Versuch zu beschreiben.

Bericht "Knotengruppendaten"

Im Knotengruppendaten-Bericht werden die Knoten, die zu jeder Gruppe gehören, die Benutzergruppen, die Zugriff auf die Knotengruppen haben, und ggf. die Regeln, die die Knotengruppe definieren, angezeigt. Die Liste der Knoten befindet sich in den Berichtsdetails, die Sie anzeigen können, indem Sie auf der Berichtsseite auf eine Zeile doppelklicken, oder der Bericht als CSV-Datei speichern. Siehe ***Berichte in Dateien speichern*** (auf Seite 250).

Im Knotenanlagebericht werden die Gruppen angezeigt, denen die einzelnen Knoten angehören. Siehe ***Knotenanlagebericht*** (auf Seite 258).

So erstellen Sie den Bericht "Knotengruppendaten":

1. Wählen Sie "Berichte > Benutzer > Knotengruppendaten".
2. Doppelklicken Sie auf eine Zeile, um die Liste der Knoten in der Gruppe anzuzeigen.

AD-Benutzergruppenbericht

Im AD-Benutzergruppenbericht werden alle Benutzer in Gruppen angezeigt, die von AD-Servern, die zur Authentifizierung und Autorisierung konfiguriert wurden, in CC-SG importiert wurden. Der Bericht enthält keine Benutzer, die lokal über CC-SG zu den AD-Benutzergruppen hinzugefügt wurden.

So erstellen Sie den AD-Benutzergruppenbericht:

1. Wählen Sie "Berichte > Active Directory > AD-Benutzergruppenbericht".
2. In der Liste AD-Server werden alle AD-Server aufgeführt, die in CC-SG zur Authentifizierung und Autorisierung konfiguriert wurden. Markieren Sie das Kontrollkästchen jedes AD-Servers, den CC-SG im Bericht berücksichtigen soll.
3. Im Bereich AD-Benutzergruppen enthält die Liste Verfügbar alle Benutzergruppen, die über AD-Server, die in der Liste AD-Server markiert wurden, in CC-SG importiert wurden. Wählen Sie die Benutzergruppen aus, die im Bericht enthalten sein sollen, und klicken Sie auf "Hinzufügen", um die Benutzergruppen in die Liste "Ausgewählt" zu verschieben.
4. Klicken Sie zum Erstellen des Berichts auf "Übernehmen".

Geplante Berichte

Geplante Berichte sind Berichte, die im Aufgabenmanager geplant wurden. Sie finden die Berichte "Gerätefirmware aktualisieren" und "Gerät neu starten" im Fenster "Geplante Berichte". Geplante Berichte können nur im HTML-Format angezeigt werden. Weitere Informationen finden Sie unter ***Aufgabenmanager*** (auf Seite 330).

So greifen Sie auf einen geplanten Bericht zu:

1. Wählen Sie "Berichte > Geplante Berichte".
2. Wählen Sie einen Berichtstyp aus.
3. Wählen Sie einen Berichtseigentümer aus.
4. Geben Sie einen Berichtsnamen ein, um nach dem Namen zu filtern. Sie können den vollständigen Namen oder einen Teil des Namens eingeben. Bei den Übereinstimmungen wird die Groß- und Kleinschreibung nicht berücksichtigt. Platzhalter sind nicht zulässig.
5. Legen Sie den Datumsbereich für den Bericht in den Feldern "Startdatum" und "Startzeit" sowie "Enddatum" und "Endzeit" fest. Klicken Sie auf jede Komponente des Standarddatums (Monat, Tag, Jahr, Stunde, Minute), um sie auszuwählen, und legen Sie den gewünschten Wert fest, indem Sie auf die Pfeile nach oben und nach unten klicken.
6. Klicken Sie auf Übernehmen. Die Liste der geplanten Berichte wird generiert.

So zeigen Sie einen geplanten Bericht an:

1. Wählen Sie den Bericht in der Liste aus.
2. Klicken Sie auf "Bericht anzeigen".

Hinweis: Die manuell erstellten Überwachungslistenberichte, Fehlerprotokollberichte und Zugriffsberichte enthalten alle Einträge im Bericht, während der aufgrund einer geplanten Aufgabe erstellte Bericht maximal 10.000 Zeilen enthält.

So löschen Sie einen geplanten Bericht:

1. Wählen Sie die Berichte aus, die gelöscht werden sollen. Klicken Sie bei gedrückter Strg- oder gedrückter Umschalttaste, um mehrere Berichte auszuwählen.
2. Klicken Sie auf "Berichte löschen".
3. Klicken Sie zum Bestätigen auf "Ja".

Bericht "Gerätefirmware aktualisieren"

Sie finden den Bericht "Gerätefirmware aktualisieren" in der Liste "Geplante Berichte". Dieser Bericht wird erstellt, wenn die Aufgabe Gerätefirmware aktualisieren ausgeführt wird. Zeigen Sie den Bericht an, um Statusinformationen über die Aufgabe in Echtzeit zu erhalten. Nachdem die Aufgabe abschlossen wurde, sind die Berichtsinformationen statisch.

Weitere Informationen zum Anzeigen des Berichts finden Sie unter ***Geplante Berichte*** (auf Seite 261).

Kapitel 14 Systemwartung

In diesem Kapitel

Wartungsmodus 263
Wartungsmodus starten 264
Wartungsmodus beenden 264
CC-SG sichern 265
Sicherungsdateien speichern und löschen.....267
CC-SG wiederherstellen.....268
CC-SG zurücksetzen.....270
CC-SG neu starten.....272
CC-SG aktualisieren.....273
Aktualisieren eines Clusters 276
CC-SG-Datenbank migrieren 277
CC-SG herunterfahren (CC-SG Shutdown) 279
CC-SG nach dem Herunterfahren neu starten.....279
CC-SG herunterfahren (Powering Down CC-SG) 280
CC-SG-Sitzung beenden.....280

Wartungsmodus

Der Wartungsmodus schränkt den Zugriff auf CC-SG ein, damit Administratoren Aufgaben ohne Unterbrechung durchführen können. Zu den Aufgaben, die am besten im Wartungsmodus durchgeführt werden, zählen Änderungen des Leerlaufzeitgebers oder Sicherung von CC-SG. Dadurch wird sichergestellt, dass systemweite Einstellungen wie der Leerlaufzeitgeber für alle Benutzer geändert werden.

Aktuelle Benutzer mit Ausnahme des Administrators, der den Wartungsmodus startet, werden benachrichtigt und nach Ablauf der konfigurierbaren Zeitspanne abgemeldet. Im Wartungsmodus können sich andere Administratoren bei CC-SG anmelden, Benutzer, die keine Administratoren sind, können sich nicht anmelden. Jedes Mal, wenn CC-SG den Wartungsmodus startet oder beendet, werden SNMP-Traps erzeugt.

Hinweis 1: Der Wartungsmodus steht nur in Standalone-CC-SG-Einheiten zur Verfügung, die sich nicht in einer Clusterkonfiguration befinden.

Hinweis 2: CC-SG kann nur im Wartungsmodus aktualisiert werden.

Geplante Aufgaben und der Wartungsmodus

Geplante Aufgaben können nicht durchgeführt werden, wenn sich CC-SG im Wartungsmodus befindet. Weitere Informationen finden Sie unter ***Aufgabenmanager*** (auf Seite 330). Beendet CC-SG den Wartungsmodus, werden geplante Aufgaben so schnell wie möglich ausgeführt.

Wartungsmodus starten

1. Wählen Sie "Systemwartung > Wartungsmodus > Wartungsmodus starten".
2. Kennwort: Geben Sie Ihr Kennwort ein. Nur Benutzer mit der Berechtigung CC-Setup- und -Steuerung können den Wartungsmodus starten.
3. Broadcastnachricht: Geben Sie die Nachricht für Benutzer ein, die bei CC-SG abgemeldet werden.
4. Wartungsmodus starten nach (Min.): Geben Sie die Dauer in Minuten von 0 bis 720 ein, die verstreichen sollen, bis CC-SG den Wartungsmodus startet. Durch die Eingabe von 0 Minuten wird der Wartungsmodus sofort gestartet.

   Wenn Sie mehr als 10 Minuten angeben, wird den Benutzern die Broadcastnachricht sofort angezeigt und 10 Minuten und 5 Minuten vor dem Ereignis wiederholt.
5. Klicken Sie auf OK.
6. Klicken Sie im Bestätigungsfeld auf OK.

Wartungsmodus beenden

1. Wählen Sie "Systemwartung > Wartungsmodus > Wartungsmodus beenden".
2. Klicken Sie auf OK, um den Wartungsmodus zu beenden.
3. Eine Nachricht wird angezeigt, wenn CC-SG den Wartungsmodus beendet hat. Benutzer können jetzt wieder normal auf CC-SG zugreifen.

CC-SG sichern

Vor der Sicherung von CC-SG sollten Sie in den Wartungsmodus wechseln. Durch das Starten des Wartungsmodus wird sichergestellt, dass die Datenbank während der Sicherung nicht geändert wird.

Sie können in CC-SG bis zu 50 Sicherungsdateien speichern. Wenn Sie diese Anzahl erreicht haben, können Sie so lange keine neuen Sicherungen erstellen, bis Sie einige der alten Sicherungsdateien von CC-SG gelöscht haben. Siehe ***Sicherungsdateien speichern und löschen*** (auf Seite 267).

So sichern Sie CC-SG:

1. Wählen Sie "Systemwartung > Sicherung".
2. Geben Sie einen Namen für diese Sicherung im Feld "Sicherungsname" ein.
3. Geben Sie eine Beschreibung für die Sicherung in das Feld "Beschreibung" ein. **Optional.**
4. Wählen Sie einen Sicherungstyp aus: Vollständig oder Standard. Siehe ***Worin besteht der Unterschied zwischen einer vollständigen und einer Standardsicherung?*** (auf Seite 267)
5. Um eine Kopie dieser Sicherungsdatei auf einem externen Server zu speichern, markieren Sie das Kontrollkästchen "Sicherung an Remotestandort". **Optional.**
   a. Wählen Sie ein Protokoll, das für die Verbindung zum Remoteserver verwendet wird (entweder FTP oder SFTP).
   b. Geben Sie die IP-Adresse oder den Hostnamen des Servers im Feld "IP-Adresse/Hostname" ein.
   c. Wenn Sie den Standardport nicht für das ausgewählte Protokoll (FTP: 21, SFTP: 22) verwenden, geben Sie den verwendeten Kommunikationsport im Feld "Portnummer" an.
   d. Geben Sie einen Benutzernamen für den Remoteserver in das Feld "Benutzername" ein.
   e. Geben Sie ein Kennwort für den Remoteserver in das Feld "Kennwort" ein.
   f. Geben Sie im Feld "Directory (Relative Path)" (Verzeichnis (Relativer Pfad)) den Speicherort für die Sicherungsdatei auf dem FTP-Server an.

- Lassen Sie das Feld leer, wenn Sie die Sicherungsdatei in das Standard-Basisverzeichnis auf dem FTP-Server speichern möchten.
- Wählen Sie einen relativen Pfad im Standard-Basisverzeichnis aus, um die Sicherungsdatei auf einer Ebene unterhalb dieses Verzeichnisses auf dem FTP-Server zu speichern. Wenn Sie die Sicherungsdatei beispielsweise in einem Ordner mit der Bezeichnung "Sicherungen" im Standard-Basisverzeichnis speichern möchten, geben Sie in das Feld "Directory (Relative Path)" (Verzeichnis (Relativer Pfad)) `Sicherungen` ein.

g. Geben Sie im Feld "Dateiname (leer lassen, um Standardkonvention für Dateinamen zu verwenden)" einen Dateinamen für die Sicherung auf dem Remoteserver ein oder lassen Sie das Feld leer, um den Standardnamen zu verwenden. Der Standardname beinhaltet "backup" (Sicherung) zusammen mit Datum und Uhrzeit.

h. Klicken Sie auf "Als Standard speichern", wenn Sie die aktuellen Einstellungen des Remoteservers als Standardwerte speichern möchten. Eine Bestätigungsmeldung wird angezeigt. Klicken Sie auf OK. **Optional.**

6. Klicken Sie auf OK.

   Nach Abschluss der Sicherung wird eine Meldung angezeigt. Die Sicherungsdatei wird im CC-SG-Dateisystem gespeichert. Ist das Kontrollkästchen "Sicherung an Remotestandort" markiert, wird sie auch auf einem Remoteserver gespeichert. Diese Sicherung kann später wiederhergestellt werden. Siehe ***CC-SG wiederherstellen*** (auf Seite 268).

Wichtig: Die Konfiguration der Netzwerkumgebung ist in der CC-SG-Sicherungsdatei enthalten. Merken Sie sich aus diesem Grund die diesbezügliche Einstellung zum Zeitpunkt der Datensicherung, oder notieren Sie sich die Einstellung. Dies ist sinnvoll, um festzustellen, ob sich die Sicherungsdatei für die wiederherzustellende CC-SG-Einheit eignet.

Worin besteht der Unterschied zwischen einer vollständigen und einer Standardsicherung?

Standardsicherung:

Eine Standardsicherung umfasst alle Daten in allen Feldern auf allen CC-SG-Seiten mit Ausnahme von Daten auf den folgenden Seiten:

- Registerkarte "Administration > Konfigurationsmanager > Netzwerk"
- "Administration > Clusterkonfiguration"

CC-SG-Sicherungsdateien, die auf CC-SG gespeichert sind, werden ebenfalls nicht gesichert. Sie können eine Liste der auf CC-SG gespeicherten Sicherungsdateien auf der Seite "Systemwartung > Wiederherstellen" anzeigen.

Des Weiteren werden bei der Standardsicherung auch sonstige temporäre Daten in Feldern, z. B. Datumsbereiche auf Berichtsseiten, nicht gesichert.

Vollständige Sicherung:

Eine vollständige Sicherung umfasst alle Elemente der Standardsicherung sowie die Sicherung der Firmwaredateien von CC-SG und Geräten, von Anwendungsdateien und Protokollen. Zu den Anwendungsdateien zählen RRC, MPC, RC und VNC.

Sicherungsdateien speichern und löschen

Verwenden Sie den Bildschirm "CommandCenter wiederherstellen", um Sicherungen in CC-SG zu speichern und in CC-SG gespeicherte Sicherungen zu löschen. Durch das Speichern von Sicherungen können Sie eine Kopie der Sicherungsdatei auf einem anderen PC verwahren. Sie können ein Archiv der Sicherungsdateien erstellen. Sicherungsdateien, die an einem anderen Ort gespeichert sind, können an andere CC-SG-Einheiten gesendet und dann wiederhergestellt werden, um eine Konfiguration von einer CC-SG-Einheit zu einer anderen zu kopieren.

Durch das Löschen von unbenötigten Sicherungen haben Sie mehr Platz auf dem CC-SG.

Sicherungsdateien speichern

1. Wählen Sie "Systemwartung > CommandCenter wiederherstellen".
2. Wählen Sie in der Tabelle "Verfügbare Sicherungen" die Sicherung aus, die Sie auf Ihrem PC speichern möchten.
3. Klicken Sie auf "In Datei speichern". Ein Speicherdialog wird angezeigt.

4. Geben Sie einen Namen für die Datei ein, und wählen Sie den Speicherort aus.
5. Klicken Sie auf "Speichern", um die Sicherungsdatei an den angegebenen Speicherort zu kopieren.

Sicherungsdateien löschen

1. Wählen Sie in der Tabelle "Verfügbare Sicherungen" die Sicherung zum Löschen aus.
2. Klicken Sie auf "Löschen". Ein Bestätigungsfeld wird angezeigt.
3. Klicken Sie auf OK, um die Sicherung aus dem CC-SG-System zu löschen.

CC-SG wiederherstellen

Sie können CC-SG über eine Sicherungsdatei wiederherstellen.

Wichtig: Die Konfiguration der Netzwerkumgebung ist in der CC-SG-Sicherungsdatei enthalten. Merken Sie sich aus diesem Grund die diesbezügliche Einstellung zum Zeitpunkt der Datensicherung, oder notieren Sie sich die Einstellung. Dies ist sinnvoll, um festzustellen, ob sich die Sicherungsdatei für die wiederherzustellende CC-SG-Einheit eignet.

So stellen Sie CC-SG wieder her:

1. Wählen Sie "Systemwartung > Wiederherstellen". Die Seite "CommandCenter wiederherstellen" wird mit einer Liste der Sicherungsdateien angezeigt, die CC-SG zur Verfügung stehen. Die Liste enthält die Sicherungsart, das Sicherungsdatum, die Beschreibung, welche CC-SG-Version verwendet wurde, sowie die Größe der Sicherungsdatei.
2. Wenn Sie eine Sicherung wiederherstellen möchten, die nicht auf dem CC-SG-System gespeichert wurde, müssen Sie die Sicherungsdatei zunächst an CC-SG senden. **Optional.**
   a. Klicken Sie auf "Upload".
   b. Suchen Sie nach der Sicherungsdatei, und wählen Sie sie im Dialogfenster aus. Sie können die Datei überall im Netzwerk des Clients abrufen.
   c. Klicken Sie auf "Öffnen", um diese Datei an CC-SG zu senden. Nach Abschluss wird die Sicherungsdatei in der Tabelle "Verfügbare Sicherungen" angezeigt.
3. Wählen Sie die Sicherungsdatei, die Sie wiederherstellen möchten, in der Tabelle "Verfügbare Sicherungen" aus.

4. Wählen Sie ggf. die Art der Wiederherstellung für diese Sicherung aus:
   - Standard: Nur wichtige Daten werden auf CC-SG wiederhergestellt. Diese Sicherung umfasst CC-SG-Konfigurationsinformationen, Geräte- und Knotenkonfigurationen und Benutzerkonfigurationen. Siehe ***Worin besteht der Unterschied zwischen einer vollständigen und einer Standardsicherung?*** (auf Seite 267)
   - Vollständig: Stellt alle Daten, Protokolle, Firmware- und Anwendungsdateien sowie Lizenzdateien wieder her, die sich in der Sicherungsdatei befinden. Siehe ***Worin besteht der Unterschied zwischen einer vollständigen und einer Standardsicherung?*** (auf Seite 267) Dies setzt voraus, dass für die Datei eine vollständige Sicherung durchgeführt wurde. In der Spalte "Typ" der Tabelle "Verfügbare Sicherungen" sehen Sie, welche vollständigen Sicherungen verfügbar sind.
   - Benutzerdefiniert: Sie können angeben, welche Komponenten der Sicherung auf CC-SG wiederhergestellt werden sollen, indem Sie sie im Bereich "Wiederherstellungsoptionen" unten markieren. Markieren Sie jede der folgenden Optionen, um sie in der Wiederherstellung einzuschließen.
     - Daten wiederherstellen: CC-SG-Konfiguration, Geräte- und Knotenkonfiguration sowie Benutzerdaten. Durch diese Auswahl wird der Standardsicherungsteil einer vollständigen Sicherungsdatei wiederhergestellt. Siehe ***Worin besteht der Unterschied zwischen einer vollständigen und einer Standardsicherung?*** (auf Seite 267)
     - Protokolle wiederherstellen: Fehlerprotokolle und Ereignisberichte, die unter CC-SG gespeichert sind.
     - CommandCenter-Firmware wiederherstellen: Gespeicherte Firmwaredateien, die zur Aktualisierung des CC-SG-Servers verwendet werden.
     - Firmwarebinärdateien wiederherstellen: Gespeicherte Firmwaredateien, die zur Aktualisierung von CC-SG verwalteten Raritan-Geräten verwendet werden.
     - Anwendungen wiederherstellen: Gespeicherte Anwendungen, die von CC-SG verwendet werden, um Benutzer mit Knoten zu verbinden.
     - Restore Licenses (Lizenzen wiederherstellen): Gespeicherte Lizenzdateien, die den Zugriff auf CC-SG-Funktionen und -Knoten erlauben. Siehe ***Verfügbare Lizenzen*** (auf Seite 11).
5. Geben Sie in das Feld "Wiederherstellen nach (Min)" die Minuten von 0 bis 60 ein, die verstreichen sollen, bevor CC-SG die Wiederherstellung durchführt. Dadurch erhalten die Benutzer die Möglichkeit, ihre Arbeiten abzuschließen und sich abzumelden.

Wenn Sie mehr als 10 Minuten angeben, wird den Benutzern die Broadcastnachricht sofort angezeigt und 10 Minuten und 5 Minuten vor dem Ereignis wiederholt.

6. Geben Sie in das Feld "Broadcastnachricht" eine Nachricht ein, die andere CC-SG-Benutzer darüber informiert, dass eine Wiederherstellung durchgeführt wird.
7. Klicken Sie auf "Wiederherstellen". CC-SG lässt die angegebene Zeit verstreichen, bevor die Konfiguration über die ausgewählte Sicherung wiederhergestellt wird. Während der Wiederherstellung werden alle anderen Benutzer abgemeldet.

   Wenn die Sicherungsdatei beschädigt ist, wird eine Nachricht angezeigt und das Ereignis in der Überwachungsliste protokolliert. Beschädigte Sicherungsdateien können nicht zum Wiederherstellen von CC-SG verwendet werden.

CC-SG zurücksetzen

Sie können CC-SG zurücksetzen, um die Datenbank zu leeren oder die werkseitigen Standardwerte anderer Komponenten wiederherzustellen. Vor der Verwendung von Optionen zum Zurücksetzen sollten Sie eine Sicherung durchführen und die Sicherungsdatei an einem anderen Ort speichern.

Es wird empfohlen, die ausgewählten Standardoptionen zu verwenden.

Hinweis: CC-SG-Sicherungsdateien, die auf der CC-SG-Einheit gespeichert sind, werden durch das Zurücksetzen von CC-SG nicht gelöscht. Sie müssen jede Datei manuell löschen, um sie von CC-SG zu entfernen. Siehe **Sicherungsdateien speichern und löschen** *(auf Seite 267).*

Option	Beschreibung
Gesamte Datenbank	Diese Option entfernt die vorhandene CC-SG-Datenbank und erstellt eine neue Version mit den werkseitigen Standardwerten. Netzwerkeinstellungen, SNMP-Agenten, Firmware und Diagnosekonsole-Einstellungen sind nicht Teil der CC-SG-Datenbank. Die SNMP-Konfiguration und -Traps werden zurückgesetzt. Der SNMP-Agent wird nicht zurückgesetzt. Die IP-ACL-Einstellungen werden mit einer vollständigen Datenbankzurücksetzung zurückgesetzt, unabhängig davon, ob Sie die Option "IP-ACL-Tabellen" auswählen oder nicht. Die Konfiguration der Netzwerkumgebung wird beim Zurücksetzen gelöscht, d. h. die CC-SG-Einheit "weiß" nicht mehr, ob es ein Mitglied der Netzwerkumgebung war oder nicht. Wenn die Datenbank entfernt wird, werden alle Geräte, Knoten

Option	Beschreibung
	und Benutzer entfernt. Außerdem sind alle Authentifizierungs- und Autorisierungsserver entfernt. Ihr CC-Superuser-Konto wird auf die Standardwerte zurückgesetzt. Nach Abschluss des Zurücksetzens müssen Sie sich mit dem Standardbenutzernamen und dem Standardkennwort (admin/raritan) anmelden.
Persönliche Einstellungen speichern	Diese Option kann nur ausgewählt werden, wenn Sie "Full CC-SG Database Reset" auswählen. Mit dieser Option werden die zuvor konfigurierten Optionen beim Wiederherstellen der CC-SG-Datenbank gespeichert ▪ Sichere Kennwörter erzwingen ▪ Direkte und Proxy-Verbindungen zu Out-of-Band-Knoten ▪ Einstellung für Leerlaufzeitgeber
Netzwerkeinstellungen	Diese Option setzt die Netzwerkeinstellungen auf die werkseitigen Standardwerte zurück. ▪ Hostname: CommandCenter ▪ Domänenname: localdomain ▪ Modus: IP-Ausfallsicherung ▪ Konfiguration: Statisch ▪ IP-Address (IP-Adresse): 192.168.0.192 ▪ Netzmaske: 255.255.255.0 ▪ Gateway: keiner ▪ Primärer DNS-Server: keiner ▪ Sekundärer DNS-Server: keiner ▪ Adaptergeschwindigkeit: Automatisch
SNMP-Konfiguration	Diese Option setzt die SNMP-Einstellungen auf die werkseitigen Standardwerte zurück. ▪ Port: 161 ▪ Community mit Lesezugriff: public ▪ Community mit Lese/Schreibzugriff: private ▪ Systemkontakt, -name, -standort: keiner ▪ SNMP-Trap-Konfiguration ▪ SNMP-Trap-Ziele
Standard-Firmware	Diese Option setzt alle Geräte-Firmeware-Dateien auf die werkseitigen Standardwerte zurück. Diese Option ändert die CC-SG-Datenbank nicht.
Nach dem Zurücksetzen Firmware in Datenbank laden	Diese Option lädt die Firmware-Dateien für die aktuelle CC-SG-Version in die CC-SG-Datenbank.

Option	Beschreibung
Diagnosekonsole	Diese Option stellt die Einstellungen für die Diagnosekonsolen mit den werkseitigen Standardwerten wieder her.
IP-ACL-Tabellen	Diese Option entfernt alle Einträge aus der IP-ACL-Tabelle. Die IP-ACL-Einstellungen werden mit einer vollständigen Datenbankzurücksetzung zurückgesetzt, unabhängig davon, ob Sie die Option "IP-ACL-Tabellen" auswählen oder nicht.
Lizenzen	Diese Option entfernt alle Lizenzdateien aus CC-SG.

So setzen Sie CC-SG zurück:

1. Legen Sie vor dem Zurücksetzen eine Sicherung von CC-SG an, und speichern Sie die Sicherungsdatei an einem Remotestandort. Siehe ***CC-SG sichern*** (auf Seite 265).
2. Wählen Sie "Systemwartung > Zurücksetzen".
3. Wählen Sie die Rücksetzungsoptionen.
4. Geben Sie Ihr CC-SG-Kennwort ein.
5. Broadcastnachricht: Geben Sie die Nachricht für Benutzer ein, die bei CC-SG abgemeldet werden.
6. Geben Sie die Dauer in Minuten von 0 bis 720 ein, die verstreichen sollen, bis CC-SG den Zurücksetzungsvorgang durchführt.

   Wenn Sie mehr als 10 Minuten angeben, wird den Benutzern die Broadcastnachricht sofort angezeigt und 10 Minuten und 5 Minuten vor dem Ereignis wiederholt.
7. Klicken Sie auf OK. Eine Meldung wird angezeigt, um das Zurücksetzen zu bestätigen.

Während des Zurücksetzens darf CC-SG NICHT ausgeschaltet, aus- und wiedereingeschaltet oder unterbrochen werden. Andernfalls kann es beim CC-SG zu Datenverlust kommen.

CC-SG neu starten

Mit dem Befehl Neu starten wird die CC-SG-Software erneut gestartet. Durch den CC-SG-Neustart werden alle aktiven Benutzer bei CC-SG abgemeldet.

Durch den Neustart wird CC-SG nicht aus- und eingeschaltet. Wenn Sie CC-SG neu hochfahren möchten, müssen Sie auf die Diagnostic Console zugreifen oder den Betriebsschalter an der CC-SG-Einheit verwenden.

1. Wählen Sie "Systemwartung > Neu starten".

2. Geben Sie Ihr Kennwort im Feld "Kennwort" ein.
3. Broadcastnachricht: Verwenden Sie die Standardmeldung, oder bearbeiten Sie sie. Die Meldung wird den Benutzern angezeigt, die bei CC-SG abgemeldet werden.
4. Neustart nach (Min.): Geben Sie die Dauer in Minuten von 0 bis 720 ein, die verstreichen sollen, bis CC-SG neu startet.

   Wenn Sie mehr als 10 Minuten angeben, wird den Benutzern die Broadcastnachricht sofort angezeigt und 10 Minuten und 5 Minuten vor dem Ereignis wiederholt.
5. Klicken Sie auf OK, um CC-SG neu zu starten.

CC-SG aktualisieren

Sie können die Firmware von CC-SG aktualisieren, wenn eine neuere Version veröffentlicht wird. Sie finden die Firmware-Dateien auf der Raritan-Website im Support-Bereich. Um CC-SG von Version 3.x auf Version 4.1 zu aktualisieren, müssen Sie sie zuerst auf Version 4.0 aktualisieren. Um CC-SG von Version 4.x auf eine höhere Version als Version 5.0 zu aktualisieren, müssen Sie zuerst auf Version 5.0 aktualisieren.

CC-SG Version 4.0 oder höher ist mit dieser G1-Hardware nicht kompatibel. Eine CC-SG G1-Einheit darf nicht auf Version 4.0 oder höher aktualisiert werden.

Laden Sie die Firmware-Datei auf Ihren Client-PC herunter, bevor Sie mit der Aktualisierung beginnen.

Nur Benutzer mit der Berechtigung "CC-Setup- und -Steuerung" können CC-SG aktualisieren.

Erstellen Sie vor der Aktualisierung eine Sicherungskopie von CC-SG, und senden Sie die Sicherungsdateien zur Aufbewahrung an mehrere PCs. Siehe ***Sicherungskopie von CC-SG erstellen*** (siehe "***CC-SG sichern***" auf Seite 265) und ***Sicherungsdatei speichern*** (siehe "***Sicherungsdateien speichern***" auf Seite 267).

Wenn Sie mit einem CC-SG-Cluster arbeiten, müssen Sie das Cluster vor dem Aktualisieren entfernen. Aktualisieren Sie jeden CC-SG-Koten einzeln, und erstellen Sie das Cluster neu.

Wichtig: Wenn Sie sowohl CC-SG als auch ein Gerät oder eine Gerätegruppe aktualisieren müssen, aktualisieren Sie zuerst CC-SG und dann die Geräte.

CC-SG wird während des Aktualisierungsvorgangs neu gestartet. Während der Aktualisierung dürfen Sie Folgendes NICHT: den Vorgang anhalten, die Einheit manuell neu starten, die Einheit ausschalten oder die Einheit aus- und einschalten.

So aktualisieren Sie CC-SG:

1. Laden Sie die Datei mit der Firmware auf Ihren Client PC herunter.
2. Melden Sie sich mit einem Konto beim CC-SG-Administrations-Client an, das über die Berechtigung "CC-Setup und -Steuerung" verfügt.
3. Starten Sie den Wartungsmodus. Siehe ***Wartungsmodus starten*** (auf Seite 264).
4. Sobald sich CC-SG im Wartungsmodus befindet, wählen Sie "Systemwartung > Aktualisieren".
5. Klicken Sie auf "Durchsuchen". Wechseln Sie zur CC-SG-Firmwaredatei (.zip), wählen Sie diese aus, und klicken Sie auf "Öffnen".
6. Klicken Sie auf OK, um die Firmwaredatei an CC-SG zu senden.

   Nachdem die Firmwaredatei an CC-SG gesandt wurde, wird eine Erfolgsmeldung angezeigt. In dieser Meldung wird Ihnen mitgeteilt, dass CC-SG mit dem Aktualisierungsvorgang begonnen hat. Dazu werden alle Benutzer bei CC-SG abgemeldet.
7. Sie müssen mit der erneuten Anmeldung bei CC-SG warten, bis die Aktualisierung abgeschlossen ist. Sie können die Aktualisierung in der Diagnosekonsole überwachen.
   a. Greifen Sie über das Konto "admin" auf die Diagnosekonsole zu. Siehe ***Auf die Administratorkonsole zugreifen*** (auf Seite 361).
   b. Wählen Sie "Admin > System Logfile Viewer". Wählen Sie "sg/upgrade.log" und dann "Ansicht", um das Aktualisierungsprotokoll anzuzeigen.
   c. Warten Sie, bis der Aktualisierungsvorgang ausgeführt wird. Der Aktualisierungsvorgang ist beendet, wenn die Nachricht "Upgrade completed" (Aktualisierung beendet) im Aktualisierungsprotokoll zu finden ist. Sie können jedoch auf den SNMP-Trap ccImageUpgradeResults mit der Meldung "Erfolg" warten.
   d. Der Server muss neu gestartet werden. Der Neustart beginnt, wenn die Meldung "Linux reboot" (Linux-Neustart) im Aktualisierungsprotokoll zu finden ist. Der Server wird heruntergefahren und neu gestartet.

   Hinweis: Für Aktualisierungen von CC-SG 3.x auf 4.0x wird das System zweimal neu gestartet. Dies ist normal.

   e. Nach ungefähr zwei Minuten nach dem Neustart können Sie mithilfe des Kontos "admin" wieder auf die Diagnosekonsole zugreifen und den Fortschritt der Aktualisierung überwachen. **Optional.**
8. Klicken Sie auf OK, um CC-SG zu beenden.

9. Löschen Sie den Browser-Cache, und schließen Sie das Browserfenster. Siehe ***Browser-Cache löschen*** (auf Seite 275).
10. Löschen Sie den Java-Cache. Siehe ***Java-Cache löschen*** (auf Seite 275).
11. Starten Sie ein neues Browserfenster.
12. Melden Sie sich mit einem Konto beim CC-SG-Administrations-Client an, das über die Berechtigung "CC-Setup und -Steuerung" verfügt.
13. Wählen Sie "Hilfe > Info zu Raritan Secure Gateway". Überprüfen Sie die Versionsnummer, um zu bestätigen, dass die Aktualisierung erfolgreich war.
    - Wurde die Version nicht aktualisiert, wiederholen Sie die Schritte oben.
    - War die Aktualisierung erfolgreich, fahren Sie mit dem nächsten Schritt fort.
14. Beenden Sie den Wartungsmodus. Siehe ***Wartungsmodus beenden*** (auf Seite 264).
15. Legen Sie eine Sicherungskopie von CC-SG an. Siehe ***CC-SG sichern*** (auf Seite 265).

Browser-Cache löschen

Die Anweisungen können je nach Browserversion etwas variieren.

So löschen Sie den Browser-Cache in Internet Explorer:

1. Wählen Sie "Extras > Internetoptionen".
2. Klicken Sie auf der Registerkarte "Allgemein" auf "Dateien löschen", und klicken Sie dann zur Bestätigung auf OK.

In FireFox 2.0 und 3.0:

1. Wählen Sie "Extras > Private Daten löschen".
2. Stellen Sie sicher, dass "Cache" ausgewählt ist, und klicken Sie auf "Private Daten jetzt löschen".

Java-Cache löschen

Die Anweisungen können je nach Java-Version und Betriebssystem etwas variieren.

Unter Windows XP mit Java 1.6:

1. Wählen Sie "Systemsteuerung > Java".
2. Klicken Sie auf der Registerkarte "Allgemein" auf "Einstellungen".
3. Klicken Sie im Dialogfeld auf "Dateien löschen".

4. Stellen Sie sicher, dass das Kontrollkästchen "Anwendungen und Applets" ausgewählt ist, und klicken Sie auf "OK".

Aktualisieren eines Clusters

Befolgen Sie die nachfolgenden empfohlenen Aktualisierungsanweisungen zum Aktualisieren eines CC-SG-Clusters. Ein Cluster kann nur physische CC-SG-Einheiten enthalten.

Eine CC-SG-Clusterlizenz ist eine besondere Art der Lizenzdatei, die von den beiden CC-SG-Einheiten im Cluster gemeinsam genutzt werden. Weitere Informationen finden Sie unter ***Clusterlizenzen*** (auf Seite 310).

Wenn die Aktualisierung des primären Knotens während dieses Vorgangs fehlschlägt, lesen Sie den Abschnitt ***Fehlgeschlagene Aktualisierung des primären Knotens*** (auf Seite 277).

So aktualisieren Sie einen Cluster:

1. Zwingen Sie den Sicherungsknoten, die Funktion des primären Knotens zu übernehmen. Wählen Sie dazu "Administration > Clusterkonfiguration". Klicken Sie auf der Registerkarte "Konfiguration" auf "Primären Knoten und Sicherungsknoten wechseln". Weitere Informationen finden Sie unter ***Zwischen primärem und sekundärem Knotenstatus wechseln*** (auf Seite 307).
   - Der Sicherungsknoten wird zum primären Knoten. Der frühere primäre Knoten wechselt in den Status "Warten".
2. Fahren Sie die CC-SG-Anwendung auf dem neuen primären Knoten herunter. Wählen Sie dazu "Systemwartung > Herunterfahren".
   - Wenn Sie die CC-SG-Anwendung herunterfahren, ist die Einheit immer noch eingeschaltet und es kann immer noch über die Diagnosekonsole darauf zugegriffen werden. Weitere Informationen finden Sie im Abschnitt ***CC-SG herunterfahren*** (siehe "***CC-SG herunterfahren (CC-SG Shutdown)***" auf Seite 279).
3. Starten Sie den früheren primären Knoten neu, der sich im Status "Warten" befand. Weitere Informationen zum Neustart finden Sie im Abschnitt ***CC-SG mit der Diagnosekonsole neu starten*** (auf Seite 375).
   - Die neu gestartete CC-SG-Einheit wechselt wieder in den Status "Hauptknoten". Der heruntergefahrene Sicherungsknoten wird als "Fehlgeschlagen" erkannt.
4. Löschen Sie den Cluster durch Auswahl von "Administration > Clusterkonfiguration". Klicken Sie auf "Delete Cluster" (Cluster löschen).

5. Wechseln Sie in den Wartungsmodus, und aktualisieren Sie den primären Knoten. Siehe ***Wartungsmodus starten*** (auf Seite 264) und ***CC-SG aktualisieren*** (auf Seite 273).
6. Wenn der primäre Knoten erfolgreich aktualisiert wurde, stellen Sie den Sicherungsknoten auf die Werkseinstellungen zurück. Greifen Sie dazu auf die Diagnosekonsole zu, und wählen Sie "Operation (Vorgang) > Admin (Administration) > Factory Reset (Auf Werkseinstellung zurücksetzen) > Full CC-SG Database Reset (CC-SG-Datenbank vollständig zurücksetzen)". Siehe ***Werksseitig eingestellte Konfiguration von CC-SG wiederherstellen*** (auf Seite 379).
   - Schlägt die Aktualisierung des primären Knotens fehl, lesen Sie den Abschnitt ***Fehlgeschlagene Aktualisierung des primären Knotens*** (auf Seite 277).
7. Aktualisieren Sie den Sicherungsknoten, den Sie zurückgesetzt haben. Siehe ***CC-SG aktualisieren*** (auf Seite 273).
8. Erstellen Sie den Cluster neu. Siehe ***Cluster erstellen*** (auf Seite 305). Die Daten des primären Knotens werden mit dem Sicherungsknoten synchronisiert.

Fehlgeschlagene Aktualisierung des primären Knotens

Führen Sie die Clusteraktualisierung anhand der folgenden Schritte aus, wenn die Aktualisierung bei den Anweisungen unter "***Aktualisieren eines Clusters*** (auf Seite 276)" fehlschlägt.

1. Wenn die Aktualisierung des primären Knotens fehlschlägt, fahren Sie die CC-SG-Anwendung durch Auswahl von "Systemwartung > Herunterfahren" herunter. Wenn Sie die CC-SG-Anwendung herunterfahren, ist die Einheit immer noch eingeschaltet und es kann immer noch über die Diagnosekonsole darauf zugegriffen werden. Weitere Informationen finden Sie im Abschnitt ***CC-SG herunterfahren*** (siehe "***CC-SG herunterfahren (CC-SG Shutdown)***" auf Seite 279).
2. Starten Sie den Sicherungsknoten neu. Weitere Informationen zum Neustart finden Sie im Abschnitt ***CC-SG mit der Diagnosekonsole neu starten*** (auf Seite 375).
3. Der Sicherungsknoten wechselt in den Status "Hauptknoten".
4. Wenden Sie sich an den technischen Support von Raritan, um festzustellen, weshalb die Aktualisierung fehlgeschlagen ist.

CC-SG-Datenbank migrieren

Führen Sie das nachfolgende empfohlene Migrationsverfahren aus, um eine physische CC-SG-Einheit durch eine neue zu ersetzen oder von einer physischen CC-SG-Einheit zu einer virtuellen CC-SG-Einheit zu migrieren.

Migrationsvoraussetzungen

- Beide CC-SG-Einheiten müssen dieselbe Firmwareversion (Version 5.1 oder höher) aufweisen.
- Sie müssen gültige Lizenzen für die CC-SG-Einheit haben, zu der Sie Ihre Datenbank migrieren, bevor die migrierte CC-SG-Einheit komplett funktionsfähig ist.

CC-SG-Datenbank migrieren

So migrieren Sie eine CC-SG-Datenbank:

1. Unterbrechen Sie die Verwaltung aller Gerät. Optional: Sie können eine Aufgabe zum Unterbrechen aller Geräte planen, wenn Sie die CC-SG-Firmwareversion 5.1 oder höher verwenden. Siehe ***Aufgaben planen*** (auf Seite 332).
2. Führen Sie eine vollständige Sicherung der CC-SG-Einheit durch, von der Sie migrieren. Achten Sie darauf, dass Sie "Vollständig" als Sicherungstyp auswählen, und speichern Sie die Sicherungsdatei an einem Remotestandort. Siehe ***CC-SG sichern*** (auf Seite 265).
3. Wählen Sie auf der CC-SG-Einheit, von der Sie migrieren, "Systemwartung > Herunterfahren", um die CC-SG-Anwendung herunterzufahren.
4. Laden Sie die Datei der vollständigen Sicherung auf der CC-SG-Einheit hoch, zu der Sie migrieren, und führen Sie eine vollständige Wiederherstellung durch. Achten Sie darauf, dass Sie "Vollständig" als Wiederherstellungstyp auswählen. Siehe ***CC-SG wiederherstellen*** (auf Seite 268).

   Hinweis: Die CC-SG-Einheit, zu der Sie migrieren, muss eigene gültige Lizenzen besitzen, um vollständig betriebsbereit zu sein. Für die vollständige Wiederherstellung ist keine gültige Lizenz erforderlich.

5. Setzen Sie die Verwaltung aller Geräte fort. Sie können eine Aufgabe zum Fortsetzen der Wartung aller Geräte planen, wenn Sie die CC-SG-Firmwareversion 5.1 oder höher verwenden. Siehe ***Aufgaben planen*** (auf Seite 332).
6. Führen Sie einen Bericht zur Geräteverfügbarkeit aus, um den Status des verwalteten Geräts zu prüfen. Siehe ***Verfügbarkeitsbericht*** (auf Seite 253).

7. Wenn die neue CC-SG-Einheit erfolgreich ausgeführt wird, setzen Sie die Datenbank auf der CC-SG-Einheit, von der Sie migriert haben, zurück, um Konflikte zu vermeiden, wenn beide versehentlich online geschaltet werden. Zum Zurücksetzen der Datenbank greifen Sie auf die Diagnosekonsole zu, und wählen Sie "Operation (Vorgang) > Admin (Administration) > Factory Reset (Auf Werkseinstellung zurücksetzen) > Full CC-SG Database Reset (CC-SG-Datenbank vollständig zurücksetzen)". Siehe ***Werksseitig eingestellte Konfiguration von CC-SG wiederherstellen*** (auf Seite 379).

CC-SG herunterfahren (CC-SG Shutdown)

Wenn Sie CC-SG herunterfahren, wird die CC-SG-Software heruntergefahren, die CC-SG-Einheit wird jedoch nicht ausgeschaltet.

Nachdem CC-SG heruntergefahren wurde, sind alle Benutzer abgemeldet. Benutzer können sich erst wieder anmelden, nachdem Sie CC-SG entweder über die Diagnostic Console oder durch Aus- und Einschalten der CC-SG-Stromversorgung neu gestartet haben.

So fahren Sie CC-SG herunter:

1. Wählen Sie "Systemwartung > Herunterfahren".
2. Geben Sie Ihr Kennwort im Feld "Kennwort" ein.
3. Übernehmen Sie die Standardnachricht, oder geben Sie im Feld "Broadcastnachricht" für alle derzeit mit Sitzungen verbundenen Benutzer eine Meldung ein. Teilen Sie den Benutzern beispielsweise mit, wie viel Zeit ihnen zum Abschließen ihrer Aufgaben bleibt, und weisen Sie sie darauf hin, wann CC-SG wieder einsatzbereit sein wird. Beim Herunterfahren von CC-SG werden alle Benutzerverbindungen getrennt.
4. Geben Sie in das Feld "Herunterfahren nach (Min)" die Minuten von 0 bis 720 ein, die verstreichen sollen, bevor CC-SG heruntergefahren wird.

   Wenn Sie mehr als 10 Minuten angeben, wird den Benutzern die Broadcastnachricht sofort angezeigt und 10 Minuten und 5 Minuten vor dem Ereignis wiederholt.
5. Klicken Sie auf OK, um CC-SG herunterzufahren.

CC-SG nach dem Herunterfahren neu starten

Nach dem Herunterfahren von CC-SG gibt es zwei Möglichkeiten, die Einheit neu zu starten:

- Über die Diagnostic Console: Siehe ***CC-SG mit der Diagnosekonsole neu starten*** (auf Seite 375).
- Schalten Sie die CC-SG-Einheit aus und dann wieder ein.

CC-SG herunterfahren (Powering Down CC-SG)

Wenn die Stromversorgung zu CC-SG unterbrochen wird, während das Gerät eingeschaltet ist und ausgeführt wird, merkt sich CC-SG den letzten Stromversorgungsstatus. Sobald die Stromversorgung wiederhergestellt ist, fährt CC-SG automatisch neu hoch. Wenn jedoch die Stromversorgung zu CC-SG unterbrochen wird, wenn das Gerät ausgeschaltet ist, bleibt CC-SG auch dann ausgeschaltet, wenn die Stromversorgung wiederhergestellt wurde.

Wichtig: Drücken Sie nicht die POWER-Taste, um CC-SG zwangsweise herunterzufahren. Wir empfehlen, CC-SG mithilfe des Diagnosekonsolen-Befehls "CC-SG System Power OFF" (CC-SG-System ausschalten). Siehe *CC-SG-System über die Diagnosekonsole ausschalten* (auf Seite 377).

So fahren Sie CC-SG herunter:

1. Entfernen Sie die Blende, und drücken Sie die POWER-Taste.
2. Warten Sie etwa eine Minute, während CC-SG ordnungsgemäß heruntergefahren wird.

   Hinweis: Benutzer, die über die Diagnostic Console in CC-SG angemeldet sind, erhalten eine kurze Broadcastnachricht, wenn die CC-SG-Einheit ausgeschaltet wird. Benutzer, die über einen Webbrowser oder SSH in CC-SG angemeldet sind, erhalten keine Nachricht, wenn die CC-SG-Einheit ausgeschaltet wird.

3. Warten Sie, bis der Vorgang des Herunterfahrens vollständig abgeschlossen ist, bevor Sie den Netzstecker ziehen. Nur so kann CC-SG vor der Unterbrechung der Stromversorgung alle Transaktionen beenden, die Datenbanken schließen und die Festplattenlaufwerke in einen sicheren Zustand versetzen.

CC-SG-Sitzung beenden

Eine CC-SG-Sitzung kann auf zwei Arten beendet werden.

- Melden Sie sich ab, um Ihre Sitzung zu beenden, wobei das Client-Fenster geöffnet bleibt. Siehe ***CC-SG verlassen*** (auf Seite 280).
- Mit der Option "Beenden" beenden Sie Ihre Sitzung und schließen das Client-Fenster. Siehe ***CC-SG beenden*** (auf Seite 281).

CC-SG verlassen

1. Wählen Sie "Secure Gateway > Abmelden". Das Fenster "Abmelden" wird angezeigt.

2. Klicken Sie auf "Ja", um CC-SG zu verlassen. Nach dem Abmelden wird das CC-SG-Anmeldefenster angezeigt.

CC-SG beenden

1. Wählen Sie "Secure Gateway > Beenden".
2. Klicken Sie auf "Ja", um CC-SG zu beenden.

Kapitel 15 Erweiterte Administration

In diesem Kapitel

Tipp des Tages konfigurieren 282
Anwendungen für den Zugriff auf Knoten konfigurieren....283
Standardanwendungen konfigurieren 286
Gerätefirmware verwalten 287
CC-SG-Netzwerk konfigurieren....288
Protokollaktivitäten konfigurieren 295
CC-SG-Serverzeit und -datum konfigurieren 296
Verbindungsmodi: Direkt und Proxy....297
Geräteeinstellungen 299
Benutzerdefinierte JRE-Einstellungen konfigurieren....301
SNMP konfigurieren 303
CC-SG-Cluster konfigurieren....304
Netzwerkumgebung konfigurieren....311
Sicherheitsmanager....316
Benachrichtigungsmanager....329
Aufgabenmanager 330
SSH-Zugriff auf CC-SG 339
Serieller Administrationsport....349
Web Services-API 350
CC-NOC 352

Tipp des Tages konfigurieren

Mit dem Tipp des Tages können Sie allen Benutzern beim Anmelden eine Nachricht einblenden. Sie müssen über die Berechtigung "CC-Setup und -Steuerung" verfügen, um den Tipp des Tages zu konfigurieren.

So konfigurieren Sie den Tipp des Tages:

1. Wählen Sie "Administration > Tipp des Tages einrichten".
2. Markieren Sie das Kontrollkästchen "Tipp des Tages für alle Benutzer anzeigen", wenn die Nachricht allen Benutzern nach dem Anmelden angezeigt werden soll. **Optional.**
3. Markieren Sie das Kontrollkästchen "Inhalt des Tipp des Tages", wenn Sie eine Nachricht in CC-SG eingeben möchten, oder markieren Sie das Kontrollkästchen "Datei für Tipp des Tages", wenn Sie eine vorhandene Datei mit der Nachricht laden möchten.
   - Bei Markierung von Inhalt des Tipp des Tages:
   a. Geben Sie eine Nachricht in das Dialogfeld ein.
   b. Klicken Sie auf das Dropdown-Menü "Schriftartname", und wählen Sie die Schriftart für die Meldung aus.

c. Klicken Sie auf das Dropdown-Menü "Schriftgrad", und wählen Sie den Schriftgrad für die Meldung aus.

- Bei Markierung von Datei für Tipp des Tages:

a. Klicken Sie auf "Durchsuchen", um die Datei zu suchen.

b. Wählen Sie die Datei im Dialogfenster aus, und klicken Sie auf "Öffnen".

c. Klicken Sie auf "Vorschau", um den Inhalt der Datei anzuzeigen.

4. Klicken Sie zum Speichern der Änderungen auf OK.

Anwendungen für den Zugriff auf Knoten konfigurieren

Anwendungen für den Zugriff auf Knoten

CC-SG bietet mehrere Anwendungen, mit denen Sie auf Knoten zugreifen können. Mit dem Anwendungsmanager können Sie Anwendungen anzeigen, neue Anwendungen hinzufügen, Anwendungen löschen und die Standardanwendung für jeden Gerätetyp einstellen.

So zeigen Sie in CC-SG verfügbare Anwendungen an:

1. Wählen Sie "Administration > Anwendungen".
2. Klicken Sie auf das Dropdown-Menü Anwendungsname, um die Liste der in CC-SG verfügbaren Anwendungen anzuzeigen.

Anwendungsversionen prüfen und aktualisieren

Prüfen und aktualisieren Sie die CC-SG-Anwendungen, einschließlich Raritan Console (RC) und Raritan Remote Client (RRC).

So überprüfen Sie eine Anwendungsversion:

1. Wählen Sie "Administration > Anwendungen".
2. Wählen Sie in der Liste einen Anwendungsnamen aus. Beachten Sie die Zahl im Feld Version. Für einige Anwendungen wird nicht automatisch eine Versionszahl angezeigt.

So aktualisieren Sie eine Anwendung:

Handelt es sich nicht um die aktuelle Anwendungsversion, müssen Sie die Anwendung aktualisieren. Sie können die Aktualisierungsdatei für die Anwendung auf der Website von Raritan herunterladen. Eine vollständige Liste der unterstützten Anwendungsversionen finden Sie in der Kompatibilitätsmatrix auf der Support-Website von Raritan.

Am besten starten Sie den Wartungsmodus, bevor Sie Anwendungen aktualisieren. Siehe ***Wartungsmodus starten*** (auf Seite 264).

1. Speichern Sie die Datei mit der Anwendung auf Ihrem Client-PC.

2. Klicken Sie auf die Dropdown-Liste Anwendungsname, und wählen Sie die zu aktualisierende Anwendung in der Liste aus. Wenn Sie die Anwendung nicht sehen, müssen Sie die Anwendung zuerst hinzufügen. Siehe ***Anwendungen hinzufügen*** (auf Seite 284).
3. Klicken Sie auf "Durchsuchen", und wählen Sie die Datei zur Anwendungsaktualisierung im angezeigten Dialogfeld aus. Klicken Sie auf "Öffnen".
4. Der Anwendungsname wird im Anwendungsmanager im Feld "Neue Anwendungsdatei" angezeigt.
5. Klicken Sie auf "Upload". Eine Statusanzeige informiert über den Ladevorgang der neuen Anwendung. Nach dem Laden wird in einem neuen Fenster angezeigt, dass die Anwendung der CC-SG-Datenbank hinzugefügt wurde und nun verwendet werden kann.
6. Wenn das Feld "Version" nicht automatisch aktualisiert wird, geben Sie die neue Versionszahl in das Feld "Version" ein. Das Feld "Version" wird bei einigen Anwendungen automatisch aktualisiert.
7. Klicken Sie auf "Aktualisieren".

Hinweis: Benutzer, die während der Aktualisierung angemeldet sind, müssen sich von CC-SG abmelden und dann wieder anmelden, um sicherzustellen, dass die neue Version der Anwendung gestartet wird. Siehe auch **Ältere Version der Anwendung öffnet sich nach Aktualisierung** *(auf Seite 284).*

Ältere Version der Anwendung öffnet sich nach Aktualisierung

Wenn Sie eine Verbindung herstellen möchten und die neuesten Versionen von Anwendungen verwendet werden sollten, die falschen, alten Versionen jedoch geöffnet werden, löschen Sie den Java-Cache. Dies kann vorkommen, wenn der Cache seit einer Aktualisierung von CC-SG nicht geleert wurde.

Siehe ***Java-Cache löschen*** (auf Seite 275).

Anwendungen hinzufügen

Wenn Sie CC-SG eine Anwendung hinzufügen, müssen Sie festlegen, mit welchen Gerätetypen die Anwendung verwendet wird. Bietet ein Gerät KVM- und seriellen Zugriff, wird es für beide Methoden aufgeführt.

So fügen Sie eine Anwendung hinzu:

1. Wählen Sie "Administration > Anwendungen".
2. Klicken Sie auf "Hinzufügen". Das Fenster "Anwendungen hinzufügen" wird geöffnet.

3. Geben Sie den Namen der Anwendung im Feld "Anwendungsname" ein.
4. Wählen Sie in der Liste "Verfügbar" die Raritan-Geräte für die Anwendung aus, und klicken Sie auf "Hinzufügen", um sie der Liste "Ausgewählt" hinzuzufügen.
   - Sie können Geräte entfernen, damit sie nicht mehr mit der Anwendung verwendet werden können. Wählen Sie dazu das Gerät in der Liste "Ausgewählt" aus, und klicken Sie auf "Entfernen".
5. Klicken Sie auf OK. Ein Dialogbildschirm "Öffnen" wird angezeigt.
6. Navigieren Sie zur Anwendungsdatei (normalerweise eine JAR- oder CAB-Datei), wählen Sie die Datei aus, und klicken Sie dann auf "Öffnen".
7. Die ausgewählte Anwendung wird in CC-SG geladen.

Anwendungen löschen

So löschen Sie eine Anwendung:

1. Wählen Sie "Administration > Anwendungen".
2. Wählen Sie im Dropdown-Menü "Anwendungsname" eine Anwendung aus.
3. Klicken Sie auf "Löschen". Ein Bestätigungsfeld wird angezeigt.
4. Klicken Sie auf "Ja", um die Anwendung zu löschen.

Voraussetzungen für die Verwendung des AKC

So verwenden Sie den AKC:

- Stellen Sie sicher, dass die Cookies von der IP-Adresse des Geräts, auf das zugegriffen wird, nicht blockiert werden.
- Die Benutzer von Windows Vista-, Windows 7- und Windows 2008-Servern müssen sicherstellen, dass die IP-Adresse des Geräts, auf das zugegriffen wird, in der Zone "Vertrauenswürdige Sites" hinzugefügt wurde und dass der "Geschützte Modus" nicht aktiv ist, wenn auf das Gerät zugegriffen wird.

Enable AKC Download Server Certificate Validation (AKC-Download-Serverzertifikat-Validierung aktivieren)

Falls durch den Geräteadministrator (oder CC-SG-Administrator) die Option "Enable AKC Download Server Certificate Validation" (AKC-Download-Serverzertifikat-Validierung aktivieren) aktiviert wurde:

- Administratoren müssen ein gültiges Zertifikat auf das Gerät hochladen oder ein selbstsigniertes Zertifikat auf dem Gerät generieren. Das Zertifikat muss über eine gültige Hostbezeichnung verfügen.
- Jeder Benutzer muss das CA-Zertifikat (oder eine Kopie des selbstsignierten Zertifikats) zum Speicher für "Vertrauenswürdige Stammzertifizierungsstellen" seines Browsers hinzufügen.

Zum Starten von AKC über den CC-SG-Admin-Client müssen Sie über JRE™ 1.6.0_10 oder höher verfügen.

Standardanwendungen konfigurieren

Standardanwendungen

Sie können festlegen, welche Anwendung CC-SG standardmäßig für jeden Gerätetyp verwenden soll.

Zuordnungen der Standardanwendung anzeigen

So zeigen Sie die Zuordnungen der Standardanwendung an:

1. Wählen Sie "Administration > Anwendungen".
2. Klicken Sie auf die Registerkarte "Standardanwendungen", um die aktuellen Standardanwendungen für verschiedene Schnittstellen- und Porttypen anzuzeigen und zu bearbeiten. Hier aufgeführte Anwendungen werden als Standard bei der Konfiguration eines Knotens für den Zugriff über eine ausgewählte Schnittstelle festgelegt.

Standardanwendung für Schnittstellen- oder Porttypen einstellen

So legen Sie die Standardanwendung für einen Schnittstellen- oder Porttyp fest:

1. Wählen Sie "Administration > Anwendungen".
2. Klicken Sie auf die Registerkarte "Standardanwendungen".
3. Wählen Sie den Schnittstellen- oder Porttyp aus, dessen Standardanwendung Sie einstellen möchten.
4. Doppelklicken Sie auf den Pfeil bei "Anwendung", der in der Zeile aufgeführt ist. Der Wert wird in einem Dropdown-Menü angezeigt. Abgeblendete Werte können nicht geändert werden.
5. Wählen Sie die Standardanwendung aus, die für die Verbindung zum ausgewählten Schnittstellen- oder Porttyp verwendet werden soll.
   - Automatisch erkennen: CC-SG wählt automatisch eine geeignete Anwendung basierend auf dem Clientbrowser aus.
6. Klicken Sie zum Speichern der Änderungen auf OK. Diese Standardeinstellungen gelten nur für neue Ports. Um diese Einstellungen für Ports auf vorhandenen Geräten zu übernehmen, klicken Sie auf "Apply Selections to Existing Devices" (Auswahl für vorhandene Geräte übernehmen), wählen Sie die zu ändernden Geräte aus und klicken Sie auf OK.

Gerätefirmware verwalten

CC-SG speichert Firmware für Raritan-Geräte, die Sie zum Aktualisieren der Geräte verwenden können, die von CC-SG gesteuert werden. Der Firmwaremanager wird verwendet, um die Geräte-Firmwaredateien an CC-SG zu senden oder in CC-SG zu löschen. Sobald eine Firmwaredatei gesendet wurde, können Sie auf die Datei zugreifen, um eine Geräteaktualisierung durchzuführen. Siehe ***Gerät aktualisieren*** (auf Seite 99).

Upload

Sie können verschiedene Versionen von Gerätefirmware an CC-SG senden. Wenn neue Firmwareversionen verfügbar sind, werden sie auf der Website von Raritan veröffentlicht.

So senden Sie Firmware an CC-SG:

1. Wählen Sie "Administration > Firmware".
2. Klicken Sie auf "Hinzufügen", um eine neue Firmwaredatei hinzuzufügen. Ein Suchfenster wird geöffnet.

3. Wechseln Sie zur Firmwaredatei, die Sie an CC-SG senden möchten. Wählen Sie diese aus, und klicken Sie auf "Öffnen". Nach dem Senden wird die neue Firmware im Feld "Firmwarename" angezeigt.

Firmware löschen

So löschen Sie Firmware:

1. Wählen Sie "Administration > Firmware".
2. Klicken Sie auf den Pfeil neben der Dropdown-Liste "Firmwarename", und wählen Sie die zu löschende Firmware aus.
3. Klicken Sie auf "Löschen". Eine Bestätigungsmeldung wird angezeigt.
4. Klicken Sie auf "Ja", um die Firmware zu löschen.

CC-SG-Netzwerk konfigurieren

Im Konfigurationsmanager können Sie die Netzwerkeinstellungen für Ihr vom CC-SG verwaltetes Netzwerk konfigurieren.

Wichtig: Zum Ändern der IP-Adresse einer CC-SG-Einheit, die bereits *Mitglied einer Netzwerkumgebung* (siehe "*Was ist eine Netzwerkumgebung?*" auf Seite 311) ist, müssen Sie sie zuerst aus der Konfiguration der Netzwerkumgebung löschen. Andernfalls können Sie CC-SG nicht aus der Netzwerkumgebung löschen.

Netzwerkeinrichtung

CC-SG bietet zwei Modi für die Netzwerkeinrichtung:

- IP-Ausfallsicherungsmodus: Siehe ***Was ist der IP-Ausfallsicherungsmodus?*** (auf Seite 290)
- IP-Isolationsmodus: Siehe ***Was ist der IP-Isolationsmodus?*** (auf Seite 292)

Wichtig: Für neue Implementierungen wird der IP-Ausfallsicherungsmodus dringend empfohlen.

CC-SG ermöglicht auch entweder statische oder mit DHCP zugeordnete IP-Adressen. Weitere Informationen zu optimalen Verfahren zur Verwendung von DHCP mit CC-SG finden Sie unter ***Empfohlene DHCP-Konfigurationen für CC-SG*** (auf Seite 295).

CC-SG-LAN-Ports

CC-SG bietet zwei Haupt-LAN-Ports: Primäres LAN und Sekundäres LAN. Lesen Sie die Tabellen, um die Position des primären und sekundären LAN-Ports auf Ihrem CC-SG-Modell zu überprüfen.

V1-LAN-Ports:

Modell	Primäres LAN – Name	Primäres LAN – Position	Sekundäres LAN – Name	Sekundäres LAN – Position
V1-0 oder V1-1	LAN1	Linker LAN-Port	LAN2	Rechter LAN-Port

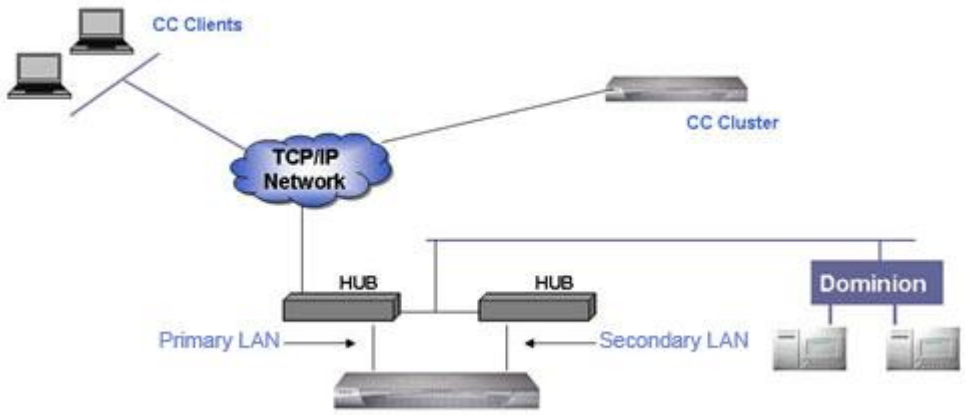
E1-LAN-Ports:

Modell	Primäres LAN – Name	Primäres LAN – Position	Sekundäres LAN – Name	Sekundäres LAN – Position
E1-0	Nicht beschriftet.	Oberer LAN-Port von 2 Ports in der Mitte der Einheitenrückseite	Nicht beschriftet.	Unterer LAN-Port von 2 Ports in der Mitte der Einheitenrückseite
E1-1	LAN1	Linker LAN-Port	LAN2	Rechter LAN-Port

Was ist der IP-Ausfallsicherungsmodus?

Im IP-Ausfallsicherungsmodus können Sie zwei CC-SG-LAN-Ports verwenden, um Ausfallsicherung und Redundanz für das Netzwerk zu implementieren. Es ist immer nur ein LAN-Port aktiv.

Weitere Informationen zur Position des primären und sekundären LAN-Ports auf jedem CC-SG-Modell finden Sie unter ***CC-SG-LAN-Ports*** (auf Seite 289).



Wenn das primäre LAN angeschlossen ist und ein Verbindungsintegritätssignal erhält, verwendet CC-SG diesen LAN-Port für die Kommunikation. Wenn das primäre LAN die Verbindungsintegrität verliert und das sekundäre LAN angeschlossen ist, wird CC-SG die zugeordnete IP-Adresse zu Ausfallsicherungszwecken auf das sekundäre LAN verlegen. Das sekundäre LAN wird verwendet, bis das primäre LAN erneut dienstbereit ist. Wenn das primäre LAN wieder dienstbereit ist, verwendet CC-SG automatisch wieder das primäre LAN.

Solange eine LAN-Verbindung einsatzbereit ist, sollte ein Client keine Dienstunterbrechung bei Ausfällen feststellen.

Einrichtung des IP-Ausfallsicherungsmodus:

Beim Implementieren des IP-Ausfallsicherungsmodus für Ihr CC-SG-Netzwerk gilt Folgendes:

- Beide CC-SG-LAN-Ports müssen an das gleiche LAN-Subnetzwerk angeschlossen sein.
- Sie können jeden LAN-Port an einen anderen Switch oder ein anderes Hub im gleichen Subnetzwerk für bessere Zuverlässigkeit anschließen. **Optional.**

So konfigurieren Sie den IP-Ausfallsicherungsmodus in CC-SG:

1. Wählen Sie "Administration > Konfiguration".

2. Klicken Sie auf die Registerkarte "Netzwerksetup".
3. Wählen Sie "IP Failover Mode" (IP-Ausfallsicherungsmodus) aus.
4. Geben Sie den CC-SG-Hostnamen in das Feld "Hostname" ein. Die Regeln zur Vergabe von Hostnamen werden unter ***Terminologie/Abkürzungen*** (auf Seite 2) beschrieben. Fügen Sie eine Top-Level-Domain hinzu, z. B. ".com". Die Top-Level-Domain muss zwischen 2 und 6 Zeichen umfassen.
5. Klicken Sie auf den Pfeil neben der Dropdown-Liste Konfiguration, und wählen Sie entweder DHCP oder Statisch.

   DHCP:

   - Wenn Sie "DHCP" auswählen, werden die Felder "Primärer DNS-Server", "Sekundärer DNS-Server", "Domänensuffix", "IP-Adresse", "Subnetzmaske" und "Standardgateway" automatisch ausgefüllt (falls Ihr DHCP-Server für die Bereitstellung dieser Informationen konfiguriert wurde), sobald Sie diese Netzwerkeinrichtung speichern und CC-SG neu starten.
   - Mithilfe der Informationen, die der DHCP-Server bereitstellt, wird CC-SG dynamisch beim DNS-Server registriert, wenn dieser dynamische Aktualisierungen annimmt.
   - Siehe ***Empfohlene DHCP-Konfigurationen für CC-SG*** (auf Seite 295).

   Statisch:

   - Wenn Sie "Statisch" auswählen, geben Sie den primären DNS-Server, den sekundären DNS-Server, das Domänensuffix, die IP-Adresse, die Subnetzmaske und das Standardgateway in die entsprechenden Felder ein.
6. Klicken Sie auf den Pfeil neben der Dropdown-Liste Adaptergeschwindigkeit, und wählen Sie in der Liste eine Geschwindigkeit aus. Stellen Sie sicher, dass Ihre Auswahl mit der Adapterporteinstellung des Switch übereinstimmt. Wählen Sie "Automatisch", wenn Ihr Switch mit einer Leitungsgeschwindigkeit von 1 Gbit/s arbeitet.
7. Wenn Sie "Auto" im Feld "Adapter Speed" ausgewählt haben, ist das Feld "Adapter Mode" deaktiviert und Full Duplex ist automatisch ausgewählt. Wenn Sie eine andere Adaptergeschwindigkeit als Automatisch ausgewählt haben, klicken Sie auf den Pfeil neben der Dropdown-Liste "Adaptermodus", und wählen Sie einen Duplexmodus in der Liste aus.
8. Klicken Sie auf "Konfiguration aktualisieren", um die Änderungen zu speichern. Ihre Änderungen werden erst nach dem nächsten Neustart von CC-SG wirksam.

   - Klicken Sie auf "Jetzt neu starten", wenn Sie CC-SG jetzt automatisch neu starten möchten.

- Klicken Sie auf "Später neu starten", wenn Sie CC-SG später neu starten möchten. Weitere Informationen finden Sie unter ***CC-SG neu starten*** (auf Seite 272).
  - Klicken Sie auf "Abbrechen", um zum Fensterbereich "Netzwerkeinrichtung" zurückzukehren, ohne die Änderungen zu speichern. Klicken Sie auf "Konfiguration aktualisieren" und dann auf "Jetzt neu starten" oder "Später neu starten", um die Änderungen zu speichern.

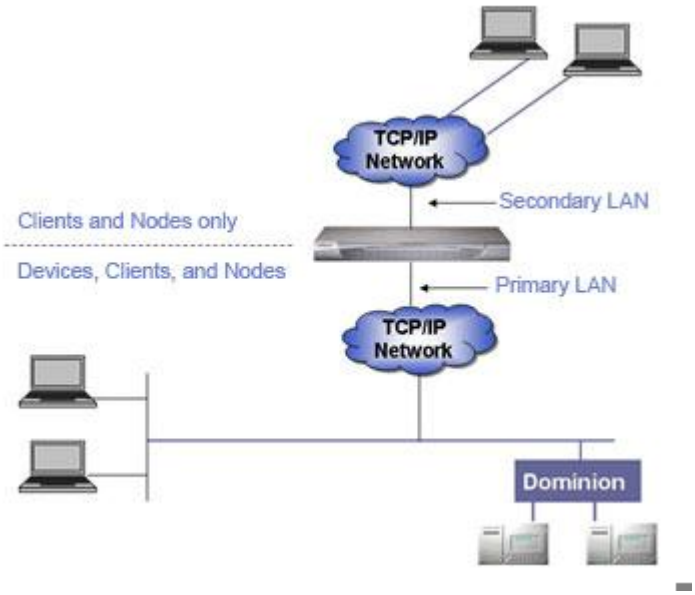
Hinweis: Ist CC-SG mit DHCP konfiguriert, können Sie nach einer erfolgreichen Registrierung bei einem DNS-Server über den Hostnamen auf CC-SG zugreifen.

Was ist der IP-Isolationsmodus?

Mit dem IP-Isolationsmodus können Sie Clients von Geräten isolieren, indem Sie sie in separate Subnetzwerke positionieren und die Clients dazu zwingen, über CC-SG auf die Geräte zuzugreifen. In diesem Modus verwaltet CC-SG den Verkehr zwischen den beiden unterschiedlichen IP-Domänen. Im IP-Isolationsmodus ist keine Ausfallsicherung verfügbar. Wenn eine LAN-Verbindung ausfällt, haben Benutzer keinen Zugriff.

Weitere Informationen zur Position des primären und sekundären LAN-Ports auf jedem CC-SG-Modell finden Sie unter ***CC-SG-LAN-Ports*** (auf Seite 289).

Hinweis: Clustering kann im IP-Isolationsmodus nicht konfiguriert werden.



Einrichtung des IP-Isolationsmodus:

Beim Implementieren des IP-Isolationsmodus für Ihr CC-SG-Netzwerk gilt Folgendes:

- Jeder CC-SG-LAN-Port muss an ein unterschiedliches Subnetzwerk angeschlossen sein.
- Raritan-Geräte dürfen nur an das primäre LAN angeschlossen werden.
- Zu isolierende Clients sind mit dem sekundären LAN verbunden. Clients, die nicht isoliert werden müssen, können mit dem primären LAN verbunden sein. Siehe ***Kombination aus Direktmodus und Proxymodus konfigurieren*** (auf Seite 298).

  Hinweis: Isolierte Clients im sekundären LAN verwenden den Proxymodus. Die Clients im primären LAN können den Direktmodus verwenden. Setzen Sie den Verbindungsmodus auf "Beides", um diese Kombination zu konfigurieren.

- Legen Sie in CC-SG im Fensterbereich Netzwerkeinrichtung höchstens ein Standardgateway fest. Verwenden Sie die Diagnostic Console, um bei Bedarf weitere statische Routen hinzuzufügen. Weitere Informationen finden Sie unter ***Static Routes bearbeiten*** (auf Seite 369).

So konfigurieren Sie den IP-Isolationsmodus in CC-SG:

1. Wählen Sie "Administration > Konfiguration".
2. Klicken Sie auf die Registerkarte "Netzwerksetup".
3. Wählen Sie "IP Isolation Mode" (IP-Isolationsmodus) aus.
4. Geben Sie den CC-SG-Hostnamen in das Feld "Hostname" ein. Die Regeln zur Vergabe von Hostnamen werden unter ***Terminologie/Abkürzungen*** (auf Seite 2) beschrieben. Wenn Sie zum Speichern der Konfiguration auf Konfiguration aktualisieren klicken, wird das Feld "Hostname" aktualisiert, um den vollständig qualifizierten Domänennamen (Fully-Qualified Domain Name, FQDN) anzuzeigen, wenn ein DNS und Domänensuffix konfiguriert wurden.
5. Konfigurieren Sie das primäre LAN in der linken und das sekundäre LAN in der rechten Spalte.
6. Klicken Sie auf den Pfeil neben der Dropdown-Liste Konfiguration, und wählen Sie entweder DHCP oder Statisch.

   DHCP:

- Wenn Sie "DHCP" auswählen, werden die Felder "Primärer DNS-Server", "Sekundärer DNS-Server", "Domänensuffix", "IP-Adresse", "Subnetzmaske" und "Standardgateway" automatisch ausgefüllt (falls Ihr DHCP-Server für die Bereitstellung dieser Informationen konfiguriert wurde), sobald Sie diese Netzwerkeinrichtung speichern und CC-SG neu starten.
- Mithilfe der Informationen, die der DHCP-Server bereitstellt, wird CC-SG dynamisch beim DNS-Server registriert, wenn dieser dynamische Aktualisierungen annimmt.
- Siehe ***Empfohlene DHCP-Konfigurationen für CC-SG*** (auf Seite 295).

Statisch:

- Wenn Sie Statisch auswählen, geben Sie einen Wert für den primären DNS-Server, den sekundären DNS-Server, das Domänensuffix, die IP-Adresse und die Subnetzmaske in die entsprechenden Felder ein.
- Legen Sie nur ein Standardgateway fest.

7. Klicken Sie auf den Pfeil neben der Dropdown-Liste Adaptergeschwindigkeit, und wählen Sie in der Liste eine Geschwindigkeit aus. Stellen Sie sicher, dass Ihre Auswahl mit der Adapterporteinstellung des Switch übereinstimmt. Wählen Sie "Automatisch", wenn Ihr Switch mit einer Leitungsgeschwindigkeit von 1 Gbit/s arbeitet.
8. Wenn Sie "Auto" im Feld "Adapter Speed" ausgewählt haben, ist das Feld "Adapter Mode" deaktiviert und Full Duplex ist automatisch ausgewählt. Wenn Sie eine andere Adaptergeschwindigkeit als Automatisch ausgewählt haben, klicken Sie auf den Pfeil neben der Dropdown-Liste "Adaptermodus", und wählen Sie einen Duplexmodus in der Liste aus.
9. Klicken Sie auf "Konfiguration aktualisieren", um die Änderungen zu speichern. CC-SG wird neu gestartet.

Empfohlene DHCP-Konfigurationen für CC-SG

Lesen Sie die folgenden empfohlenen DHCP-Konfigurationen. Stellen Sie sicher, dass Ihr DHCP-Server richtig eingerichtet ist, bevor Sie CC-SG zur Verwendung von DHCP konfigurieren.

- Konfigurieren Sie den DHCP-Server so, dass die IP-Adresse von CC-SG statisch zugeordnet wird.
- Konfigurieren Sie den DHCP- und DNS-Server so, dass sie CC-SG beim DNS-Server automatisch registrieren, wenn der DHCP-Server dem CC-SG eine IP-Adresse zuordnet.
- Konfigurieren Sie den DNS-Server so, dass es nicht authentifizierte dynamische Domain-Name-System (DDNS)-Registrierungsanforderungen von CC-SG annimmt.

Protokollaktivitäten konfigurieren

Sie können CC-SG so konfigurieren, dass Berichte auf externen Protokollservern erstellt werden, und Sie können festlegen, welche Nachrichtenebene in jedem Protokoll enthalten sein soll.

So konfigurieren Sie die CC-SG-Protokollaktivität:

1. Wählen Sie "Administration > Konfiguration".
2. Klicken Sie auf die Registerkarte "Protokolle".
3. Sie können in CC-SG einen externen Protokollserver angeben, indem Sie die IP-Adresse in das Feld "Serveradresse" unter "Primärer Server" eingeben.
4. Klicken Sie auf den Pfeil der Dropdown-Liste "Weiterleitungsebene", und wählen Sie eine Ereignisebene mit entsprechendem Schweregrad aus. Alle Ereignisse dieser oder der darüber liegenden Ebenen werden an den Protokollserver weitergeleitet.
5. Sie können einen zweiten externen Protokollserver konfigurieren, indem Sie die Schritte 3 und 4 für die Felder unter Sekundärer Server wiederholen.
6. Klicken Sie unter CommandCenter-Protokoll auf das Dropdown-Menü "Weiterleitungsebene", und wählen Sie eine Ebene aus. Alle Ereignisse auf dieser oder einer höheren Ebene werden an das interne Protokoll von CC-SG weitergeleitet.
7. Klicken Sie auf "Konfiguration aktualisieren", um die Änderungen zu speichern.

Interne CC-SG-Protokolle leeren

Sie können interne CC-SG-Protokolle löschen. Bei diesem Vorgang werden keine Ereignisse gelöscht, die auf Ihren externen Protokollservern aufgezeichnet sind.

Hinweis: Der Überwachungslistenbericht und der Fehlerprotokollbericht basieren auf dem internen CC-SG-Protokoll. Wenn Sie das interne CC-SG-Protokoll leeren, werden diese beiden Berichte ebenfalls geleert. Sie können diese Berichte auch einzeln leeren. Siehe **Berichtsdaten aus CC-SG leeren** *(auf Seite 250).*

So leeren Sie das interne CC-SG-Protokoll:

1. Wählen Sie "Administration > Konfiguration".
2. Klicken Sie auf die Registerkarte "Protokolle".
3. Klicken Sie auf "Leeren".
4. Klicken Sie auf "Ja".

CC-SG-Serverzeit und -datum konfigurieren

Uhrzeit und Datum von CC-SG müssen korrekt verwaltet werden, um die Glaubwürdigkeit der Funktionen zur Geräteverwaltung zu gewährleisten.

Wichtig: Die Konfiguration von Uhrzeit/Datum wird zum Planen von Aufgaben im Aufgabenmanager verwendet. Weitere Informationen finden Sie unter *Aufgabenmanager* (auf Seite 330). Die Uhrzeit, die auf Ihrem Client-PC eingestellt ist, unterscheidet sich eventuell von der auf CC-SG eingestellten Uhrzeit.

Nur der CC-Superuser und Benutzer mit ähnlichen Berechtigungen dürfen Uhrzeit und Datum konfigurieren.

In einer Clusterkonfiguration kann die Zeitzone nicht geändert werden.

So konfigurieren Sie die Serveruhrzeit und das Datum von CC-SG:

1. Wählen Sie "Administration > Konfiguration".
2. Klicken Sie auf die Registerkarte "Datum/Uhrzeit".
   a. So stellen Sie das Datum und die Uhrzeit manuell ein:
   - Datum: Zum Einstellen des Datums klicken Sie auf den Pfeil neben der Dropdown-Liste und wählen darin den Monat aus. Wählen Sie das Jahr mit der Schaltfläche "Pfeil-nach-oben/unten", und klicken Sie im Kalenderbereich auf den Tag.

- Uhrzeit: Zum Einstellen der Uhrzeit klicken Sie auf die Schaltfläche "Pfeil-nach-oben/unten", um die Stunde, Minuten und Sekunden festzulegen. Klicken Sie anschließend auf die Dropdown-Liste "Zeitzone", um die Zeitzone auszuwählen, in der CC-SG betrieben wird.

a. So stellen Sie das Datum und die Uhrzeit mittels NTP ein: Markieren Sie das Kontrollkästchen "Network Time Protocol aktivieren" unten im Fenster, und geben Sie die IP-Adresse für den primären NTP-Server und dem sekundären NTP-Server in die entsprechenden Felder ein.

Hinweis: Zum Synchronisieren des Datums und der Uhrzeit von angeschlossenen Computern mit dem Datum und der Uhrzeit eines zugewiesenen NTP-Servers wird das Network Time Protocol (NTP) verwendet. Wird CC-SG mit NTP konfiguriert, kann es zur konsistenten Verwendung der korrekten Uhrzeit seine eigene Uhrzeit mit dem öffentlich verfügbaren NTP-Referenzserver synchronisieren.

3. Klicken Sie auf Konfiguration aktualisieren, um die Uhrzeit- und Datumsänderungen auf CC-SG anzuwenden.
4. Klicken Sie auf Aktualisieren, um die neue Serverzeit im Feld "Aktuelle Uhrzeit" zu aktualisieren.
5. Wählen Sie "Systemwartung > Neu starten", um CC-SG neu zu starten.

Verbindungsmodi: Direkt und Proxy

Verbindungsmodi

CC-SG bietet drei Verbindungsmodi für In-Band- und Out-of-Band-Verbindungen: Direkt, Proxy und Beides.

- Im Direktmodus können Sie eine Verbindung direkt zu einem Knoten oder Port herstellen, ohne Daten durch CC-SG zu leiten. Der Direktmodus bietet im Allgemeinen schnellere Verbindungen.
- Im Proxymodus können Sie eine Verbindung zu einem Knoten oder Port herstellen, indem Sie alle Daten durch CC-SG leiten. Der Proxymodus erhöht die Last auf Ihren CC-SG-Server, wodurch eventuell langsamere Verbindungen verursacht werden. Der Proxymodus wird jedoch empfohlen, wenn Ihnen die Sicherheit der Verbindung sehr wichtig ist. Sie müssen die TCP-Ports 80, 8080, 443 und 2400 des CC-SG in der Firewall geöffnet lassen.

Hinweis: Ab CC-SG 4.2 unterstützt der Proxymodus die Verschlüsselung von KVM-Daten bei Verwendung von Dominion KXII der Version 2.1.10 oder höher. In dieser Konfiguration werden KVM-Daten gemäß der Sicherheitseinstellung auf dem KXII-Gerät verschlüsselt. Die Verschlüsselung wird nur für Dominion KXII-Geräte der Version 2.1.10 unterstützt.

- Im Beides-Modus können Sie CC-SG so konfigurieren, dass eine Kombination aus dem Direkt- und Proxymodus verwendet wird. Im Beides-Modus ist der Proxymodus die Standardeinstellung. Sie können CC-SG jedoch so konfigurieren, den Direktmodus zu verwenden, wenn Verbindungen mit Client-IP-Adressen aus festgelegten Bereichen hergestellt werden.

Hinweis: Einige Schnittstellen funktionieren nur im Direktmodus, obwohl Sie CC-SG für die Verwendung des Proxymodus konfiguriert haben. Zu diesen Schnittstellen gehören ILO, RSA, Microsoft RDP, DRAC, Web Browser und VMware Viewer. Java RDP-Schnittstellen können im Proxymodus verwendet werden. Siehe *Schnittstellen* (auf Seite 123).

Direktmodus für alle Client-Verbindungen konfigurieren

So konfigurieren Sie den Direktmodus für alle Client-Verbindungen:

1. Wählen Sie "Administration > Konfiguration".
2. Klicken Sie auf die Registerkarte "Verbindungsmodus".
3. Wählen Sie "Direktmodus".
4. Klicken Sie auf "Konfiguration aktualisieren".

Proxymodus für alle Client-Verbindungen konfigurieren

So konfigurieren Sie den Proxymodus für alle Client-Verbindungen:

1. Wählen Sie "Administration > Konfiguration".
2. Klicken Sie auf die Registerkarte "Verbindungsmodus".
3. Wählen Sie "Proxymodus".
4. Klicken Sie auf "Konfiguration aktualisieren".

Kombination aus Direktmodus und Proxymodus konfigurieren

Wenn Sie CC-SG zur Verwendung einer Kombination aus Direktmodus und Proxymodus konfigurieren, ist der Proxymodus der Standardverbindungsmodus. Der Direktmodus wird für die Client-IP-Adressen verwendet, die Sie festlegen.

So konfigurieren Sie eine Kombination aus Direktmodus und Proxymodus:

1. Wählen Sie "Administration > Konfiguration".
2. Klicken Sie auf die Registerkarte "Verbindungsmodus".

3. Wählen Sie "Beides".
4. Legen Sie in den Feldern "Netzwerkadresse" und "Netzmaske" den Client-IP-Adressbereich fest, der eine Verbindung zu Knoten und Ports über den Direktmodus herstellen soll. Klicken Sie dann auf "Hinzufügen".
5. Klicken Sie auf "Konfiguration aktualisieren".

Geräteeinstellungen

Sie können Einstellungen, die für alle Geräte gelten, sowie die Standardportnummer für jeden Gerätetyp konfigurieren.

So konfigurieren Sie die Standardportnummer für Geräte:

1. Wählen Sie "Administration > Konfiguration".
2. Klicken Sie auf die Registerkarte "Geräteeinstellungen".
3. Wählen Sie einen Gerätetyp in der Tabelle aus, und doppelklicken Sie auf den Wert für den Standardport.
4. Geben Sie den neuen Wert für den Standardport ein.
5. Klicken Sie auf "Konfiguration aktualisieren", um die Änderungen zu speichern.

So konfigurieren Sie eine Zeitlimitdauer für Geräte:

1. Wählen Sie "Administration > Konfiguration".
2. Klicken Sie auf die Registerkarte "Geräteeinstellungen".
3. Geben Sie eine neue Zeitlimitdauer in das Feld "Heartbeat (Sek.)" ein. Es können Werte im Bereich von 30 Sekunden bis 50.000 Sekunden eingegeben werden.
4. Klicken Sie auf "Konfiguration aktualisieren", um die Änderungen zu speichern.

So aktivieren oder deaktivieren Sie eine Warnmeldung für alle Stromversorgungs-Steuervorgänge:

Markieren Sie das Kontrollkästchen "Warnmeldung für alle Stromversorgungs-Steuerungsvorgänge anzeigen", um eine Warnmeldung zu aktivieren, die einen Benutzer vor einem angeforderten Stromversorgungs-Steuerungsvorgang warnt. Die Meldung wird nur dem Benutzer angezeigt, der den Stromversorgungs-Steuerungsvorgang eingeleitet hat. Der Benutzer kann den Stromversorgungs-Steuerungsvorgang abbrechen oder bestätigen, indem er auf "Nein" bzw. auf "Ja" klickt.

1. Wählen Sie "Administration > Konfiguration".
2. Klicken Sie auf die Registerkarte "Geräteeinstellungen".

3. Aktivieren Sie das Kontrollkästchen "Warnmeldung für alle Stromversorgungs-Steuerungsvorgänge anzeigen", um die Warnmeldung zu aktivieren. Deaktivieren Sie das Kontrollkästchen, um die Warnmeldung zu deaktivieren.
4. Klicken Sie auf "Konfiguration aktualisieren", um die Änderungen zu speichern.

Aktivieren der AKC-Download-Serverzertifikat-Validierung

Wenn Sie den AKC verwenden, können Sie wählen, ob Sie die Funktion "Enable AKC Download Server Certificate Validation" (AKC-Download-Serverzertifikat-Validierung aktivieren) verwenden möchten oder nicht.

Option 1: Do Not Enable AKC Download Server Certificate Validation (AKC-Download-Serverzertifikat-Validierung nicht aktivieren [Standardeinstellung])

Wenn Sie die AKC-Download-Serverzertifikat-Validierung nicht aktivieren, müssen alle Dominion-Gerätebenutzer und CC-SG Bookmark- und Access-Client-Benutzer:

- Stellen Sie sicher, dass die Cookies von der IP-Adresse des Geräts, auf das zugegriffen wird, nicht blockiert werden.
- Die Benutzer von Windows Vista-, Windows 7- und Windows 2008-Servern müssen sicherstellen, dass die IP-Adresse des Geräts, auf das zugegriffen wird, in der Zone "Vertrauenswürdige Sites" hinzugefügt wurde und dass der "Geschützte Modus" nicht aktiv ist, wenn auf das Gerät zugegriffen wird.

Option 2: Enable AKC Download Server Certificate Validation (Übersicht zur AKC-Download-Serverzertifikat-Validierung aktivieren)

Wenn Sie die AKC-Download-Serverzertifikat-Validierung aktivieren:

- Administratoren müssen ein gültiges Zertifikat auf das Gerät hochladen oder ein selbstsigniertes Zertifikat auf dem Gerät generieren. Das Zertifikat muss über eine gültige Hostbezeichnung verfügen.
- Jeder Benutzer muss das CA-Zertifikat (oder eine Kopie des selbstsignierten Zertifikats) zum Speicher für "Vertrauenswürdige Stammzertifizierungsstellen" seines Browsers hinzufügen.

So installieren Sie das selbstsignierte Zertifikat unter Windows Vista® oder Windows 7®:

1. Fügen Sie die CommandCenter Secure Gateway-IP-Adresse in der Zone "Vertrauenswürdige Sites" hinzu, und stellen Sie sicher, dass der "Geschützte Modus" nicht aktiv ist.

2. Starten Sie Internet Explorer®, und geben Sie die CommandCenter Secure Gateway-IP-Adresse als URL ein. Eine Meldung "Zertifikatfehler" wird angezeigt.
3. Wählen Sie "Zertifikate anzeigen" aus.
4. Klicken Sie auf der Registerkarte "Allgemein" auf "Zertifikat installieren". Das Zertifikat wird dann zum Speicher für "Vertrauenswürdige Stammzertifizierungsstellen" hinzugefügt.
5. Nachdem das Zertifikat installiert wurde, kann die CommandCenter Secure Gateway-IP-Adresse aus der Zone für "Vertrauenswürdige Sites" entfernt werden.

So aktivieren Sie die AKC-Download-Serverzertifikat-Validierung:

1. Wählen Sie "Device Settings > Device Services" (Geräteeinstellungen > Gerätedienste). Die Seite "Device Service Settings" (Gerätediensteinstellungen) wird geöffnet.
2. Aktivieren oder deaktivieren (Standardeinstellung) Sie das Kontrollkästchen "Enable AKC Download Server Certificate Validation" (AKC-Download-Serverzertifikat-Validierung).
3. Klicken Sie auf OK.

Benutzerdefinierte JRE-Einstellungen konfigurieren

Benutzer, die ohne die angegebene JRE-Mindestversion auf CC-SG zuzugreifen versuchen, erhalten eine Warnmeldung. Prüfen Sie in der Kompatibilitätsmatrix, welche JRE-Mindestversion unterstützt wird. Wählen Sie "Administration > Kompatibilitätsmatrix".

Das Fenster "Warnhinweis zur JRE-Inkompatibilität" wird angezeigt, wenn ein Benutzer, der sich bei CC-SG anzumelden versucht, nicht über die angegebene JRE-Version verfügt. Das Fenster stellt mehrere Optionen zum Herunterladen der JRE-Standardmindestversionen bereit. Sie können die Meldung so ändern, dass sie Text und Links zu Optionen zum Herunterladen enthält. Benutzer können eine neue JRE-Version herunterladen oder mit der derzeit installierten JRE-Version weiter auf CC-SG zugreifen.

So aktivieren oder deaktivieren Sie die benutzerdefinierte JRE für die Anmeldung:

1. Sichern Sie CC-SG, und speichern Sie die Sicherungsdatei an einem Remotestandort, bevor Sie diese Funktion aktivieren oder deaktivieren. Siehe ***CC-SG sichern*** (auf Seite 265).
2. Wählen Sie "Administration > Konfiguration".
3. Klicken Sie auf die Registerkarte "Benutzerdefinierte JRE".

4. Aktivieren Sie das Kontrollkästchen "Benutzerdefinierte JRE für Anmeldung aktivieren", um die Option zu aktivieren. Deaktivieren Sie da Kontrollkästchen, um die Option zu deaktivieren.
5. Geben Sie die erforderliche JRE-Mindestversion im Feld "Erforderliche JRE-Mindestversion" ein. Sie müssen die vollständige Versionsnummer mit mindestens drei Teilen eingeben. 1.6.0 ist beispielsweise eine korrekte Versionsnummer. 1.6 ist keine korrekte Versionsnummer. Verwenden Sie für JRE-"Aktualisierungsversionen" einen Unterstrich. 1.6.0_5 ist z. B. eine korrekte Versionsnummer für JRE Version 1.6.0 Update 5.
6. Klicken Sie auf "Aktualisieren".

So passen Sie die Meldung im Fenster "Warnhinweis zur JRE-Inkompatibilität" an:

1. Wählen Sie "Administration > Konfiguration".
2. Klicken Sie auf die Registerkarte "Benutzerdefinierte JRE".
3. Geben Sie die Meldung, die im Fenster "Warnhinweis zur JRE-Inkompatibilität" angezeigt werden soll, mithilfe von HTML-Code ein.
4. Klicken Sie auf "Aktualisieren".

So stellen Sie die Standardmeldung und die JRE-Mindestversion wieder her:

1. Wählen Sie "Administration > Konfiguration".
2. Klicken Sie auf die Registerkarte "Benutzerdefinierte JRE".
3. Klicken Sie auf "Standard wiederherstellen".
4. Klicken Sie auf "Aktualisieren".

So löschen Sie die Standardmeldung und die JRE-Mindestversion:

1. Wählen Sie "Administration > Konfiguration". Klicken Sie auf die Registerkarte "Benutzerdefinierte JRE".
2. Klicken Sie auf "Löschen".

SNMP konfigurieren

Mit Simple Network Management Protocol (SNMP) sendet CC-SG SNMP-Traps (Ereignisbenachrichtigungen) zu einem SNMP-Manager im Netzwerk. Sie sollten Erfahrung im Umgang mit der SNMP-Infrastruktur haben, um CC-SG zur Verwendung mit SNMP zu konfigurieren.

CC-SG unterstützt außerdem SNMP-Get/Set-Anfragen mit Lösungen von Drittanbietern wie HP OpenView. Zur Unterstützung dieser Anfragen müssen Sie SNMP-Agentenkennungsdaten angeben, beispielsweise die folgenden MIB-II Systemgruppenobjekte: sysContact, sysName und sysLocation. Diese Kennzeichen bieten Kontakt-, administrative und Standortinformationen für den verwalteten Knoten. Weitere Informationen finden Sie unter RFC 1213.

So konfigurieren Sie SNMP in CC-SG:

1. Wählen Sie "Administration > Konfiguration".
2. Klicken Sie auf die Registerkarte "SNMP".
3. Markieren Sie das Kontrollkästchen "Enable SNMP Daemon" (SNMP-Dämon aktivieren), um SNMP-Vorgänge zu aktivieren.
4. Kennzeichnen Sie den SNMP-Agenten, der auf CC-SG ausgeführt wird, für Unternehmensverwaltungslösungen von Drittanbietern, indem Sie unter Agent-Konfiguration Informationen zum Agenten bereitstellen. Geben Sie einen Port für den Agenten ein. Der Standardwert ist 161. Geben Sie eine Zeichenfolge für "Community mit Lesezugriff" ein (Standardwert "public") sowie eine für "Community mit Lese/Schreibzugriff" (Standardwert "private"). Mehrere Community-Zeichenfolgen sind erlaubt, müssen dann jedoch durch ein Komma getrennt werden. Geben Sie Werte für Systemkontakt, Systemname und Systemstandort ein, um Informationen zum verwalteten Knoten bereitzustellen.
5. Klicken Sie auf "Agentenkonfiguration aktualisieren", um die Änderungen zu speichern.
6. Markieren Sie das Kontrollkästchen "SNMP-Traps aktivieren", um das Senden von SNMP-Traps von CC-SG zu einem SNMP-Host zu aktivieren.
7. Geben Sie im Bereich "Trap-Ziele" die von SNMP-Hosts verwendete IP-Adresse vom Trap-Zielhost und die Portnummer ein. Der Standardport lautet 162.
8. Geben Sie im Bereich "Trap-Ziele" eine Zeichenfolge für Community und die Version (v1 oder v2) ein, die von SNMP-Hosts verwendet wird.

9. Markieren Sie die Kontrollkästchen neben den Traps, die von CC-SG an die SNMP-Hosts gesendet werden sollen: Unter "Trap-Quellen" finden Sie eine Liste der in zwei Kategorien unterteilten SNMP-Traps: Systemprotokoll-Traps, die Benachrichtigungen zum Status der CC-Einheit selbst enthalten, wie beispielsweise einen Festplattenfehler, und Anwendungsprotokoll-Traps für Benachrichtigungen, die von Ereignissen in der CC-Anwendung erstellt werden, wie beispielsweise Änderungen des Benutzerkontos. Zum Aktivieren von Traps nach Typ aktivieren Sie die Kontrollkästchen "Systemprotokoll" und "Anwendungsprotokoll". Einzelne Traps können durch Aktivieren/Deaktivieren ihrer entsprechenden Kontrollkästchen aktiviert oder deaktiviert werden. Verwenden Sie das Kontrollkästchen in der Spalte "Ausgewählt", um alle Traps zu aktivieren, oder deaktivieren Sie alle Kontrollkästchen. Eine Liste der bereitgestellten SNMP-Traps finden Sie in den MIB-Dateien. Weitere Informationen finden Sie unter "MIB-Dateien".
10. Klicken Sie auf "Hinzufügen", um diesen Zielhost zur Liste der konfigurierten Hosts hinzuzufügen. In dieser Liste können beliebig viele Manager festgelegt werden.
11. Klicken Sie auf "Trap-Konfiguration aktualisieren", um die Änderungen zu speichern.

MIB-Dateien

Da CC-SG eigene Raritan-Traps sendet, müssen alle SNMP-Manager mit einer benutzerdefinierten MIB-Datei, die Raritan-Trap-Definitionen enthält, aktualisiert werden. Siehe ***SNMP-Traps*** (auf Seite 431). Sie finden die benutzerdefinierte MIB-Datei auf der Support-Website von Raritan.

CC-SG-Cluster konfigurieren

Ein CC-SG-Cluster verwendet zwei CC-SG-Knoten: einen primären Knoten und einen sekundären Knoten, der zur Sicherheit dient, falls der primäre Knoten ausfällt. Für beide Knoten werden gemeinsame Daten für aktive Benutzer und Verbindungen verwendet, und alle Statusdaten werden zwischen den beiden Knoten repliziert.

Geräte in einem CC-SG-Cluster müssen die IP-Adresse des primären Knotens von CC-SG kennen, damit sie diesen über Statusänderungen informieren können. Fällt der primäre Knoten aus, übernimmt der sekundäre Knoten sofort alle Funktionen des primären Knotens. Dafür ist eine Initialisierung der CC-SG-Anwendung und der Benutzersitzungen erforderlich. Alle vorhandenen Sitzungen, die vom primären Knoten des CC-SG ausgehen, werden beendet. Alle mit dem primären Knoten verbundenen Geräte erkennen, dass der primäre Knoten nicht reagiert und reagieren auf Anforderungen des sekundären Knotens.

Anforderungen für CC-SG-Cluster

- Der primäre und sekundäre Knoten in einem Cluster müssen mit der gleichen Firmware und mit dem gleichen Hardware-Modell (V1 oder E1) ausgeführt werden.
- Das CC-SG-Netzwerk muss sich zur Verwendung von Clustering im IP-Ausfallsicherungsmodus befinden. Clustering funktioniert nicht, wenn eine IP-Isolationsmodus-Konfiguration ausgewählt wurde. Siehe ***Netzwerkeinrichtung* (auf Seite 288).**
- Die Einstellungen für das Datum, die Uhrzeit und die Zeitzone werden nicht vom primären Knoten auf den sekundären Knoten übertragen. Sie müssen diese Einstellungen auf jedem CC-SG konfigurieren, bevor Sie den Cluster erstellen.

Auf einen CC-SG-Cluster zugreifen

Nachdem ein Cluster erstellt wurde, können Benutzer direkt auf den primären Knoten zugreifen. Wenn sie den Browser auf den sekundären Knoten richten, werden sie umgeleitet.

Die Umleitung funktioniert nicht bei einem bereits heruntergeladenen Administrations-Client-Applet, weil der Webbrowser geschlossen und eine neue Sitzung geöffnet werden muss und dabei auf das neue primäre System verwiesen werden muss.

Der SSH-Zugriff auf CC-SG muss auf den entsprechenden primären Knoten erfolgen.

Cluster erstellen

Vor dem Erstellen eines Clusters sollten Sie die Konfiguration auf beiden CC-SG-Einheiten sichern.

So erstellen Sie einen Cluster:

1. Wählen Sie "Administration > Clusterkonfiguration".
2. Das CC-SG, auf das Sie aktuell zugreifen, wird im Feld "Primary Secure Gateway IP Address/Hostname" (Primäre(r) IP-Adresse/Hostname von Secure Gateway) angezeigt. Außerdem wird angezeigt, das es als primärer Knoten verwendet werden wird.
3. Geben Sie einen sekundären oder einen Sicherungsknoten im Feld "Backup Secure Gateway IP Address/Hostname" (IP-Adresse/Hostname des Sicherungs-Secure Gateway) an. Das CC-SG muss dieselbe Firmware-Version und denselben Hardwaretyp aufweisen wie der primäre Knoten. Sie können dabei wie folgt vorgehen:

- Klicken Sie auf "Secure Gateways erkennen", um alle CC-SG-Einheiten in dem von Ihnen zurzeit verwendeten Subnetz zu durchsuchen und anzuzeigen. Klicken Sie anschließend in der Tabelle mit den erkannten CC-SG-Einheiten auf eine CC-SG-Einheit im Status "Eigenständig", um sie auszuwählen.
- Sie können eine CC-SG-Einheit angeben, vielleicht aus einem anderen Subnetz, indem Sie eine IP-Adresse oder einen Hostnamen in das Feld "Backup Secure Gateway IP Address/Hostname" (IP-Adresse/Hostname des Sicherungs-Secure Gateway) eingeben. Klicken Sie anschließend auf "Sicherungsprüfung", um sicherzustellen, dass dieselbe Firmwareversion und derselbe Hardwaretyp wie die des primären Knotens verwendet werden.

4. Geben Sie im Feld "Clustername" einen Namen für diesen Cluster ein.
5. Geben Sie einen gültigen Benutzernamen und ein Kennwort für den Sicherungsknoten in die Felder (Username for Backup Secure Gateway" (Benutzername für das Sicherungs-Secure Gateway) und "Password for Backup Secure Gateway" (Kennwort für das Sicherungs-Secure Gateway) ein.
6. Aktivieren Sie das Kontrollkästchen "Redirect by Hostname" (Nach Hostnamen umleiten), um anzugeben, dass der Zugriff auf die Umleitung sekundär zu primär über DNS stattfinden soll. **Optional.** Siehe ***Auf einen CC-SG-Cluster zugreifen*** (auf Seite 305). Wenn Sie Hostnamen anstatt IP-Adressen verwenden, sollte der DNS-Server über Reverse-Lookup-Datensätze für die IP-Adressen der CC-SG-Einheiten verfügen, um sicherzustellen, dass die Hostnamen aufgelöst werden können.
7. Klicken Sie auf "Cluster erstellen". Eine Meldung wird angezeigt.
8. Klicken Sie auf "Ja".

Wichtig: Wenn Sie die Clustererstellung gestartet haben, sollten Sie keine weiteren Funktionen in CC-SG durchführen, bis die Erstellung abgeschlossen ist.

9. Klicken Sie in allen Bildschirmmeldungen auf OK. Der Sicherungsknoten wird neu gestartet. Dieser Vorgang dauert einige Minuten.
10. Nachdem der Cluster erstellt wurde, wird in einer Meldung bestätigt, dass der Sicherungsknoten erfolgreich verbunden wurde.

Cluster-Einstellungen konfigurieren

In einer Clusterkonfiguration können Sie die Zeitzone nicht ändern.

So konfigurieren Sie die Clustereinstellungen:

1. Wählen Sie "Administration > Clusterkonfiguration".
2. Ändern oder Konfigurieren Sie die Einstellungen auf der Registerkarte "Konfiguration".
   - Ändern Sie gegebenenfalls den Clusternamen.
   - Geben Sie bei "Zeitintervall" ein, wie oft CC-SG seine Verbindung mit den anderen Knoten überprüfen soll. Der gültige Bereich liegt zwischen 5-20 Sekunden.

   Hinweis: Ein kurzes Zeitintervall erhöht den durch Heartbeat-Prüfungen verursachten Netzwerkverkehr. Sie sollten für Cluster mit weit voneinander entfernt liegenden Knoten lange Intervalle festlegen.

   - Geben Sie für Fehlergrenzwert die Anzahl der aufeinander folgenden Heartbeats an, die erfolgen muss, bevor ein CC-SG-Knoten als fehlgeschlagen eingestuft wird. Der gültige Bereich liegt zwischen 2-10 Heartbeats.
3. Klicken Sie zum Speichern der Änderungen auf "Aktualisieren".

Zwischen primärem und sekundärem Knotenstatus wechseln

Sie können die Funktionen des primären und sekundären Knotens austauschen, wenn sich der sekundäre oder Sicherungsknoten im Status "Joined" (Verbunden) befindet. Wenn sich der sekundäre Knoten im Status "Warten" befindet, ist ein Wechseln nicht möglich.

Nachdem die Rollen getauscht wurden, wechselt der vorherige primäre Knoten in den Status "Warten". Um die Clusterkonfiguration wiederherzustellen, verbinden Sie den wartenden Knoten als Sicherungsknoten.

Siehe ***Cluster wiederherstellen*** (auf Seite 308).

So schalten Sie die primären und sekundären Knoten um:

1. Wählen Sie "Administration > Clusterkonfiguration".
2. Klicken Sie auf der Registerkarte "Konfiguration" auf "Primären Knoten und Sicherungsknoten wechseln".
3. Verbinden sie den neuen sekundären Knoten als Sicherungsknoten. Siehe ***Cluster wiederherstellen*** (auf Seite 308).

Cluster wiederherstellen

Wenn ein Cluster aufgrund eines Knotenfehlers beschädigt ist oder sich der fehlerhafte sekundäre Knoten im Status "Warten" befindet, können Sie den Cluster erneut erstellen, um den primären und sekundären Knotenstatus wiederherzustellen.

Besteht zwischen dem primären und sekundären Knoten keine Kommunikation mehr, übernimmt der sekundäre Knoten die Rolle des primären Knotens. Wird die Konnektivität wieder hergestellt, sind ggf. zwei primäre Knoten vorhanden. Der Cluster kann nicht mit zwei primären Knoten wiederhergestellt werden. Die Wiederherstellung funktioniert nur, wenn ein primärer und ein Knoten im Wartemodus vorhanden ist.

Zum Wiederherstellen eines Clusters mit zwei primären Knoten stehen Ihnen zwei Optionen zur Verfügung. Melden Sie sich bei beiden primären Knoten an, löschen Sie in beiden den Cluster und erstellen Sie diesen anschließend erneut. Oder melden Sie sich bei einem der primären Knoten an und starten Sie ihn neu, sodass dieser in den Wartemodus wechselt. Folgen Sie anschließend den Anweisungen zum Wiederherstellen eines Clusters.

So stellen Sie einen Cluster wieder her:

1. Wählen Sie "Administration > Clusterkonfiguration".
2. Klicken Sie auf die Registerkarte "Recovery" (Wiederherstellung). Sie können den Cluster automatisch zur angegebenen Zeit neu erstellen lassen oder den Cluster sofort neu erstellen.
   - Klicken Sie auf "Rebuild Now" (Jetzt wiederherstellen), um den Cluster sofort wiederherzustellen.
   - Markieren Sie das Kontrollkästchen "Enable Automatic Rebuild" (Automatische Wiederherstellung aktivieren), und geben Sie in den Feldern "Anfangszeit" und "Endzeit" die Uhrzeit an, zu der der Cluster neu erstellt werden soll. Klicken Sie zum Speichern der Änderungen auf "Aktualisieren".

Hinweis: Wenn die CC-SG-Einheiten mit Cluster nicht dieselbe Zeitzone aufweisen, wenn der Fehler im primären Knoten auftritt, wird der sekundäre Knoten als neuer primärer Knoten verwendet. Die für die automatische Neuerstellung angegebene Zeit entspricht weiterhin der Zeitzone des alten primären Knotens.

Cluster löschen

Beim Löschen eines Clusters werden die für den Cluster eingegebenen Informationen vollständig gelöscht, und der primäre und sekundäre CC-SG-Knoten werden im Status "Eigenständig" wiederhergestellt. Außerdem werden alle Konfigurationsdaten, ausgenommen der Netzwerkeinstellungen (Personality Package), auf dem sekundären Knoten auf die Standartwerte zurückgesetzt, einschließlich dem CC-Super-Benutzerkennwort.

So löschen Sie einen Cluster:

1. Wählen Sie "Administration > Clusterkonfiguration".
2. Klicken Sie auf "Delete Cluster" (Cluster löschen).
3. Klicken Sie auf "Ja", um den Status des primären und sekundären Knotens zu löschen.
4. Nachdem der Cluster gelöscht wurde, wird eine Meldung angezeigt.

Cluster aktualisieren

Siehe ***Aktualisieren eines Clusters*** (auf Seite 276).

Clusterlizenzen

Sie können einen CC-SG-Cluster mit separaten, eigenständigen Lizenzen mit der gleichen Knotenkapazität oder mit einer Cluster-Kit-Lizenz betreiben.

Clusterlizenzen unterschieden sich insofern von eigenständigen Lizenzen, als sie die Host-IDs beider CC-SG-Einheiten im Cluster enthalten. Zum Betrieb beider CC-SG-Einheiten in einem Cluster ist nur ein Satz Lizenzen erforderlich.

Clusterlizenzen müssen zur primären CC-SG-Einheit hinzugefügt werden. Die Lizenz wird beim Erstellen des Clusters automatisch auf den Sicherungsknoten kopiert.

Beim Aktualisieren eines CC-SG-Clusters auf Version 5.0 oder höher müssen Sie die Anweisungen zur Firmwareaktualisierung ausführen, um sicherzustellen, dass auf allen CC-SGs ein identischer Satz Lizenzen erstellt wird. Siehe ***Aktualisieren eines Clusters*** (auf Seite 276).

Da jede CC-SG-Einheit im Cluster in der Lage sein muss, die Funktion des primären Knotens zu übernehmen, muss die Kapazität der lizenzierten Knoten auf allen Einheiten jederzeit identisch sein. Cluster-Kit-Lizenzen stellen dies automatisch sicher, weil sie vom primären Knoten auf den Sicherungsknoten kopiert werden. Bei Betrieb eines Clusters mit eigenständigen Lizenzen wird dies durch eine Kapazitätsprüfung der lizenzierten Knoten beim Zusammenfügen des Clusters erzwungen.

Die Host-ID der Sicherung wird bei Zusammenfügen des Clusters überprüft, um sicherzustellen, dass sie mit dem Inhalt der Lizenzdateien übereinstimmt. Stimmt die Host-ID nicht mit der Lizenz überein, wird die Sicherung nicht in den Cluster aufgenommen.

Bei der Ersterstellung eines Clusters mit einer Cluster-Kit-Lizenz bleibt die primäre CC-SG-Einheit so lange im einschränkten Betriebsmodus, bis die Sicherung erfolgreich zum Cluster hinzugefügt wurde.

Nach dem Wechsel des primären Knotens in den Betriebszustand kann der Cluster vorübergehend gelöscht und anschließend nach Bedarf zur Unterstützung von Wartungsmaßnahmen (z. B. Firmwareaktualisierungen) erneut erstellt werden. Der Cluster muss innerhalb einer Frist von 30 Tagen neu erstellt werden. Nach jedem temporären Löschen eines Clusters wird eine 30-tägige Frist gewährt.

Netzwerkumgebung konfigurieren

Was ist eine Netzwerkumgebung?

Eine Netzwerkumgebung besteht aus maximal 10 CC-SG-Einheiten. Nachdem Sie die Netzwerkumgebung im Administrations-Client eingerichtet haben, können Benutzer auf mehrere CC-SG-Einheiten in derselben Netzwerkumgebung zugreifen, wobei sie sich mithilfe des Zugriffs-Clients nur einmal anmelden müssen.

Bevor Sie die Konfiguration der Netzwerkumgebung einrichten oder verwalten, müssen Sie die Kriterien für die Netzwerkumgebung beachten:

- Eine CC-SG-Einheit kann nur zu einer Netzwerkumgebung gehören.
- Alle CC-SG-Einheiten in derselben Netzwerkumgebung müssen dieselbe Firmwareversion aufweisen.
- CC-SG-Einheiten in der Netzwerkumgebung müssen entweder eigenständige CC-SG-Einheiten oder primäre Knoten von CC-SG-Einheiten mit Cluster sein.
- Eine Netzwerkumgebung kann aus physischen und virtuellen CC-SG-Einheiten bestehen.

Netzwerkumgebung erstellen

Melden Sie sich bei einer CC-SG-Einheit an, für die Sie eine Netzwerkumgebung erstellen möchten und die noch nicht Mitglied einer Netzwerkumgebung ist. Nachdem Sie eine Netzwerkumgebung erstellt haben, nutzen alle Mitglieder der Netzwerkumgebung dieselben Netzwerkumgebungsinformationen. Wenn es sich bei einem Mitglied um den primären Knoten von CC-SG-Einheiten mit Cluster handelt, wird die IP-Adresse oder der Hostname des sekundären oder Sicherungsknotens ebenfalls in der Konfiguration der Netzwerkumgebung angezeigt.

So erstellen Sie eine Netzwerkumgebung:

1. Wählen Sie "Administration > Umgebung".
2. Geben Sie in das Feld "Netzwerkumgebungsname" einen Namen ein.
3. Klicken Sie auf "Netzwerkumgebung erstellen".
4. Die IP-Adresse oder der Hostname des aktuellen CC-SG wird bereits in der Tabelle "IP-Adresse/Hostname von Secure Gateway" angezeigt. Klicken Sie auf die Dropdown-Liste, um zwischen den vollständigen oder kurzen Hostnamen oder IP-Adressen umzuschalten.
5. Fügen Sie mindestens eine CC-SG-Einheit in die Tabelle ein.

a. Klicken Sie auf die nächste freie Zeile, oder drücken Sie die Tab-Taste oder die Pfeiltasten nach oben/unten.

b. Geben Sie die IP-Adresse oder den Hostnamen der neuen CC-SG-Einheit ein, die Sie hinzufügen möchten, und drücken Sie die Eingabetaste. Die Regeln zur Vergabe von Hostnamen werden unter ***Terminologie/Abkürzungen*** (auf Seite 2) beschrieben.

c. Wiederholen Sie die vorherigen Schritte, bis Sie alle CC-SG-Einheiten hinzugefügt haben.

6. Klicken Sie auf "Weiter".
   - Wenn eine oder mehrere CC-SG-Einheiten nicht gefunden werden, wird eine Meldung angezeigt, und die betreffenden CC-SG-Einheiten werden in der Tabelle gelb hervorgehoben. Löschen Sie diese Geräte, oder ändern Sie ihre IP-Adressen oder Hostnamen, und klicken Sie erneut auf "Weiter".
7. CC-SG zeigt eine Liste der CC-SG-Einheiten zusammen mit ihrer Firmwareversion und dem Status in der Tabelle "Konfiguration der Netzwerkumgebung" an.

   Hinweis: CC-SG-Einheiten, die nicht den **Kriterien für die Netzwerkumgebung** *(siehe "***Was ist eine Netzwerkumgebung?***" auf Seite 311) entsprechen, werden automatisch deaktiviert.*

8. Passen Sie die Konfiguration der Netzwerkumgebung gegebenenfalls an. **Optional.**
   - Um den Secure Gateway-Namen eines CC-SG zu ändern, klicken Sie auf den Namen, geben einen neuen Namen ein und drücken die Eingabetaste. Standardmäßig wird ein kurzer CC-SG-Hostname verwendet. Der Name wird den Benutzern des Zugriffs-Clients angezeigt, wenn sie zwischen den Mitgliedern der Netzwerkumgebung wechseln. Deshalb muss jeder Name eindeutig sein.
   - Zum Deaktivieren einer CC-SG-Einheit deaktivieren Sie das Kontrollkästchen "Aktivieren" neben der entsprechenden Einheit. Deaktivierte CC-SG-Einheiten werden als eigenständige Einheiten betrieben und werden den Benutzern des Zugriffs-Clients nicht als Mitglied der Netzwerkumgebung angezeigt.
   - Klicken Sie auf die Spaltenüberschrift, um die Tabelle in aufsteigender Reihenfolge nach diesem Attribut zu sortieren. Klicken Sie erneut auf die Spaltenüberschrift, um die Tabelle in absteigender Reihenfolge zu sortieren.
9. Um zum vorherigen Bildschirm zurückzukehren, klicken Sie auf "Zurück" und wiederholen die vorherigen Schritte. **Optional.**
10. Klicken Sie auf "Fertig stellen".

Hinweis: Raritan empfiehlt Folgendes:

(1) Konfigurieren Sie die Einstellung "Vertragliche Einschränkungen der Serviceleistungen" und den Text für alle Mitglieder der Netzwerkumgebung gleich. Siehe **Portal** *(auf Seite 322).*

(2) Verwenden Sie vertrauenswürdige/offizielle Zertifikate für jedes Mitglied der Netzwerkumgebung, wenn SSL aktiviert ist.

Netzwerkumgebung bearbeiten

Nachdem Sie die Konfiguration für eine Netzwerkumgebung auf einer CC-SG-Einheit eingerichtet haben, verwenden alle CC-SG-Einheiten in derselben Netzwerkumgebung dieselben Netzwerkumgebungsinformationen. Deshalb können Sie sich bei einer beliebigen CC-SG-Einheit in der Netzwerkumgebung anmelden, um die Konfiguration der Netzwerkumgebung zu ändern.

Hinweis: Alle Änderungen an Mitgliedern der Netzwerkumgebung werden gesendet, sobald Sie im Fenster "Konfiguration der Netzwerkumgebung" auf "Update senden" klicken. Benutzer, die aktuell bei der Netzwerkumgebung anmeldet sind, nehmen diese Änderungen jedoch erst wahr, nachdem sie sich abgemeldet und wieder angemeldet haben.

Mitglied zu einer Netzwerkumgebung hinzufügen

So fügen Sie der Netzwerkumgebung eine neue CC-SG-Einheit hinzu:

1. Wählen Sie "Administration > Umgebung".
2. Klicken Sie auf "Mitglied hinzufügen". Das Dialogfeld "Mitglied hinzufügen" wird angezeigt.
3. Fügen Sie die CC-SG-Einheiten hinzu. Die Anzahl der CC-SG-Einheiten, die hinzugefügt werden können, hängt von der Anzahl der vorhandenen Mitglieder in der Netzwerkumgebung ab. Eine Netzwerkumgebung kann maximal 10 Mitglieder enthalten.
   a. Klicken Sie auf die nächste freie Zeile, oder drücken Sie die Tab-Taste oder die Pfeiltasten nach oben/unten.
   b. Geben Sie die IP-Adresse oder den Hostnamen der neuen CC-SG-Einheit ein, die Sie hinzufügen möchten. Die Regeln zur Vergabe von Hostnamen werden unter ***Terminologie/Abkürzungen*** (auf Seite 2) beschrieben.
   c. Wiederholen Sie die vorherigen Schritte, bis Sie alle CC-SG-Einheiten hinzugefügt haben.
   d. Klicken Sie auf OK.

4. Wenn neue CC-SG-Einheiten den Kriterien der Netzwerkumgebung entsprechen und gefunden werden, werden sie in der Tabelle "Konfiguration der Netzwerkumgebung" angezeigt. Andernfalls wird eine Meldung angezeigt und das Dialogfeld "Mitglied hinzufügen" wieder aufgerufen. Nehmen Sie im Dialogfeld die erforderlichen Änderungen vor.
5. Markieren Sie das Kontrollkästchen "Aktiv" neben jeder neuen CC-SG-Einheit.
6. Um den Secure Gateway-Namen eines CC-SG zu ändern, klicken Sie auf den Namen, geben einen neuen Namen ein und drücken die Eingabetaste. Standardmäßig wird ein kurzer CC-SG-Hostname verwendet. **Optional.**
7. Klicken Sie auf "Update senden", um die Änderungen zu speichern und die neuesten Informationen der Netzwerkumgebung an die anderen Mitglieder zu senden.

Konfiguration der Netzwerkumgebung verwalten

Sie können alle CC-SG-Einheiten in der Konfiguration der Netzwerkumgebung deaktivieren oder umbenennen. Wenn Sie eine CC-SG-Einheit deaktivieren, steht sie in der Mitgliederliste der Netzwerkkonfiguration im Zugriffs-Client nicht mehr zur Verfügung. Sie können auch alle Mitgliederdaten in der Konfiguration der Netzwerkumgebung aktualisieren, wie z. B. die Firmwareversion oder den Gerätestatus.

So deaktivieren Sie CC-SG-Einheiten in der Netzwerkumgebung oder benennen sie um oder rufen die neuesten Daten ab:

1. Wählen Sie "Administration > Umgebung".
2. Klicken Sie auf die Spaltenüberschrift, um die Tabelle in aufsteigender Reihenfolge nach diesem Attribut zu sortieren. Klicken Sie erneut auf die Spaltenüberschrift, um die Tabelle in absteigender Reihenfolge zu sortieren. **Optional.**
3. Verwalten Sie nun die Mitglieder.
   - Zum Deaktivieren einer CC-SG-Einheit deaktivieren Sie das Kontrollkästchen "Aktiv" neben der entsprechenden Einheit.
   - Um den Secure Gateway-Namen zu ändern, klicken Sie auf den Namen, geben einen neuen Namen ein und drücken die Eingabetaste. Der Name muss eindeutig sein.
   - Zum Abrufen der neuesten Daten für alle CC-SG-Einheiten klicken Sie auf "Mitgliederdaten aktualisieren".

- Um die verbundenen Sitzungen von Benutzern beim Umschalten zu einer anderen CC-SG-Einheit zu beenden, markieren Sie das Kontrollkästchen "Aktive Sitzungen unterbrechen, wenn zwischen Secure Gateways gewechselt wird". Andernfalls deaktivieren Sie das Kontrollkästchen.

4. Klicken Sie auf "Update senden", um die Änderungen zu speichern und die neuesten Informationen der Netzwerkumgebung an die anderen Mitglieder zu senden.

Mitglied aus einer Netzwerkumgebung löschen

Wenn eine CC-SG-Einheit in einer Netzwerkumgebung nicht mehr erforderlich ist, können Sie sie in der Konfiguration der Netzwerkumgebung löschen oder deaktivieren. Andernfalls können Benutzer des Zugriffs-Clients nicht mehr auf diese Geräte zugreifen, wenn sie versuchen, auf diese Geräte umzuschalten. Ein Mitglied der Netzwerkumgebung ist beispielsweise in folgenden Fällen nicht mehr erforderlich:

- Wenn Sie die CC-SG-Einheit als CC-SG-Sicherungsknoten in einer Clusterkonfiguration einrichten, entspricht sie nicht den ***Kriterien der Netzwerkumgebung*** (siehe "***Was ist eine Netzwerkumgebung?***" auf Seite 311).
- Wenn Sie die CC-SG-Einheit zurücksetzen, wird die Konfiguration der Netzwerkumgebung für die Einheit gelöscht, und die Einheit wird auf die Werkseinstellungen zurückgesetzt.

Vergewissern Sie sich beim Löschen von Mitgliedern, dass mindestens zwei CC-SG-Einheiten in der Netzwerkumgebung verbleiben. Andernfalls löscht das CC-SG seine Netzwerkumgebung.

So löschen Sie eine CC-SG-Einheit aus der Netzwerkumgebung:

1. Wählen Sie "Administration > Umgebung".
2. Klicken Sie auf die zu löschende CC-SG-Einheit, und klicken Sie auf "Mitglied entfernen". Wiederholen Sie diesen Schritt, bis Sie alle gewünschten CC-SG-Einheiten gelöscht haben.
3. Klicken Sie auf "Update senden", um die Änderungen zu speichern und die neuesten Informationen der Netzwerkumgebung an die anderen Mitglieder zu senden.

Wichtig: Zum Ändern der IP-Adresse einer CC-SG-Einheit, die bereits *Mitglied einer Netzwerkumgebung* (siehe "*Was ist eine Netzwerkumgebung?*" auf Seite 311) ist, müssen Sie sie zuerst aus der Konfiguration der Netzwerkumgebung löschen. Andernfalls können Sie CC-SG nicht aus der Netzwerkumgebung löschen.

Netzwerkumgebung aktualisieren

Sie können den neuesten Status aller Mitglieder der Netzwerkumgebung im Fenster "Konfiguration der Netzwerkumgebung" sofort abrufen.

1. Wählen Sie "Administration > Umgebung".
2. Klicken Sie auf "Mitgliederdaten aktualisieren".
3. Klicken Sie auf "Update senden", um die Änderungen zu speichern und die neuesten Informationen der Netzwerkumgebung an die anderen Mitglieder zu senden.

Netzwerkumgebung löschen

So löschen Sie eine Netzwerkumgebung:

1. Melden Sie sich bei einer CC-SG-Einheit an, deren Konfiguration der Netzwerkumgebung Sie löschen möchten.
2. Wählen Sie "Administration > Umgebung".
3. Klicken Sie auf "Netzwerkumgebung löschen".
4. Klicken Sie zum Bestätigen des Löschvorgangs auf "Ja".

Sicherheitsmanager

Der Sicherheitsmanager verwaltet, wie CC-SG Benutzern den Zugriff bereitstellt. Im Sicherheitsmanager können Sie Authentifizierungsmethoden, SSL-Zugriff, AES-Verschlüsselung, Regeln für sichere Kennwörter, Sperrregeln, das Anmeldeportal, Zertifikate und Zugriffssteuerungslisten konfigurieren.

Remoteauthentifizierung

Weitere Informationen zum Konfigurieren von Servern für die Remoteauthentifizierung finden Sie unter ***Remoteauthentifizierung*** (auf Seite 225).

AES-Verschlüsselung

Sie können CC-SG so konfigurieren, dass eine AES-128- oder AES-256-Verschlüsselung zwischen dem Client und CC-SG-Server erforderlich ist. Wenn die AES-Verschlüsselung erforderlich ist, müssen alle Benutzer mit einem AES-fähigen Client auf CC-SG zugreifen. Wenn die AES-Verschlüsselung erforderlich ist und Sie versuchen, mit einem Browser, der nicht AES-fähig ist, auf CC-SG zuzugreifen, können Sie keine Verbindung mit CC-SG herstellen.

Browser auf AES-Verschlüsselung überprüfen

CC-SG unterstützt AES-128 und AES-256. Wenn Sie nicht wissen, ob Ihr Browser AES verwendet, wenden Sie sich an den Browserhersteller.

Sie können auch die folgende Website mit dem Browser, dessen Verschlüsselungsmethode Sie überprüfen möchten, besuchen: ***https://www.fortify.net/sslcheck.html*** ***https://www.fortify.net/sslcheck.html***. Diese Website erkennt die Verschlüsselungsmethode Ihres Browsers und zeigt einen Bericht an. Raritan ist dieser Website nicht angeschlossen.

Hinweis: Internet Explorer 6 unterstützt die AES-128- oder -256-Verschlüsselung nicht.

Voraussetzungen für AES-256 und unterstützte Konfigurationen

Die AES-256-Verschlüsselung wird nur von folgenden Webbrowsern unterstützt:

- Firefox 2.0.0.x und höher
- Internet Explorer 7

Hinweis: Internet Explorer 7 unterstützt die AES-128- oder -256-Verschlüsselung nur unter Windows Vista. Unter Windows XP wird keine AES-Verschlüsselung unterstützt.

Außer der Browserunterstützung müssen Sie für die AES-256-Verschlüsselung Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 6 installieren.

So aktivieren Sie die AES-256-Verschlüsselung über den Browser:

1. Laden Sie JCE Unlimited Strength Jurisdiction Policy Files 6 von ***http://java.sun.com/javase/downloads/index.jsp*** (***http://java.sun.com/javase/downloads/index.jsp***) herunter.
2. Extrahieren Sie die Dateien in Ihr Java-Verzeichnis unter `\lib\security\`. Beispiel: `C:\Programme\Java 1.6.0\lib\security\`.

AES-Verschlüsselung zwischen Client und CC-SG voraussetzen

Im Sicherheitsmanager können Sie CC-SG so konfigurieren, dass eine AES-Verschlüsselung für Sitzungen zwischen dem Client und CC-SG-Server vorausgesetzt wird.

1. Wählen Sie "Administration > Sicherheit".
2. Öffnen Sie die Registerkarte "Verschlüsselung".
3. Markieren Sie das Kontrollkästchen "AES-Verschlüsselung zwischen Client und Server voraussetzen".

4. In einer Meldung werden Sie darüber informiert, dass die Clients AES-Verschlüsselung zur Verbindung zu CC-SG verwenden müssen, sobald diese Option ausgewählt wurde. Klicken Sie zum Bestätigen auf OK.
   - Klicken Sie auf die Dropdown-Liste "Schlüssellänge", um die Verschlüsselungsebene auszuwählen: 128 oder 256.
   - Im Feld "CC-SG Port" wird 80 angezeigt.
   - Im Feld "Browser-Verbindungsprotokoll" ist HTTPS/SSL ausgewählt.
5. Klicken Sie zum Speichern der Änderungen auf "Aktualisieren".

Browser-Verbindungsprotokoll konfigurieren: HTTP oder HTTPS/SSL

Im Sicherheitsmanager können Sie CC-SG so konfigurieren, dass entweder normale HTTP-Verbindungen von Clients verwendet oder HTTPS/SSL-Verbindungen vorausgesetzt werden. Sie müssen CC-SG neu starten, damit diese Einstellungen übernommen werden können.

Die Standardeinstellung ist HTTPS/SSL.

So konfigurieren Sie ein Browser-Verbindungsprotokoll:

1. Wählen Sie "Administration > Sicherheit".
2. Öffnen Sie die Registerkarte "Verschlüsselung".
3. Wählen Sie die Option "HTTP" oder "HTTPS/SSL", um das Browser-Verbindungsprotokoll festzulegen, das Clients bei der Verbindung zu CC-SG verwenden sollen.
4. Klicken Sie zum Speichern der Änderungen auf "Aktualisieren".

Portnummer für SSH-Zugriff auf CC-SG einstellen

Im Sicherheitsmanager können Sie die Portnummer einstellen, die Sie für den SSH-Zugriff auf CC-SG verwenden möchten. Siehe ***SSH-Zugriff auf CC-SG*** (auf Seite 339).

So stellen Sie die Portnummer für SSH-Zugriff auf CC-SG ein:

1. Wählen Sie "Administration > Sicherheit".
2. Geben Sie auf der Registerkarte "Verschlüsselung" die Portnummer für den Zugriff auf CC-SG über SSH in das Feld "SSH-Serverport" ein.
3. Klicken Sie zum Speichern der Änderungen auf "Aktualisieren".

Anmeldeeinstellungen

Mit den Anmeldeeinstellungen können Sie die Einstellungen für sichere Kennwörter und Sperreinstellungen konfigurieren.

Anmeldeeinstellungen anzeigen

1. Wählen Sie "Administration > Sicherheit".
2. Klicken Sie auf die Registerkarte "Anmeldeeinstellungen".

Sichere Kennwörter für alle Benutzer voraussetzen

1. Wählen Sie "Administration > Sicherheit".
2. Klicken Sie auf die Registerkarte "Anmeldeeinstellungen".
3. Markieren Sie das Kontrollkästchen "Sichere Kennwörter für alle Benutzer erforderlich".
4. Wählen Sie eine maximale Kennwortlänge. Kennwörter müssen weniger als die maximale Anzahl an Zeichen enthalten.
5. Wählen Sie eine Länge der Kennwortchronik. Diese Zahl legt fest, wie viele vorherige Kennwörter in der Chronik gespeichert werden und nicht erneut verwendet werden können. Ist "Länge der Kennwortchronik" beispielsweise auf 5 festgelegt, können Benutzer keines ihrer vorherigen fünf Kennwörter verwenden.
6. Wählen Sie ein Kennwort-Ablaufintervall. Alle Kennwörter laufen nach einer festgelegten Anzahl an Tagen ab. Nachdem ein Kennwort abgelaufen ist, müssen Benutzer beim nächsten Anmelden ein neues Kennwort eingeben.
7. Wählen Sie "Anforderungen für sichere Kennwörter":
   - Kennwörter müssen mindestens einen kleingeschriebenen Buchstaben enthalten.
   - Kennwörter müssen mindestens einen großgeschriebenen Buchstaben enthalten.
   - Kennwörter müssen mindestens eine Zahl enthalten.
   - Kennwörter müssen mindestens ein Sonderzeichen (zum Beispiel ein Ausrufezeichen oder kaufmännisches Und) enthalten.
8. Klicken Sie zum Speichern der Änderungen auf "Aktualisieren".

CC-SG-Kennwörter

Alle Kennwörter müssen alle Kriterien erfüllen, die der Administrator konfiguriert. Nach der Konfiguration der Regeln für sichere Kennwörter müssen alle zukünftigen Kennwörter diese Kriterien erfüllen. Alle vorhandenen Benutzer müssen ihre Kennwörter beim nächsten Anmelden ändern, wenn die neuen Kriterien umfassender als die vorherigen sind. Die Regeln für sichere Kennwörter gelten nur für lokal gespeicherte Benutzerprofile. Die auf einem Authentifizierungsserver abgelegten Kennwortregeln müssen von diesem Authentifizierungsserver verwaltet werden.

Außerdem dürfen 4 aufeinander folgende Zeichen im Benutzernamen und Kennwort nicht übereinstimmen.

Regeln für sichere Kennwörter zwingen Benutzer beim Erstellen von Kennwörtern zur Beachtung strikter Richtlinien. Diese erschweren das Erraten von Kennwörtern und tragen damit zur Erhöhung der Kennwortsicherheit bei. Sichere Kennwörter sind standardmäßig nicht in CC-SG aktiviert. Ein sicheres Kennwort, das alle Parameter für sichere Kennwörter umfasst, ist für den CC-Superuser grundsätzlich erforderlich.

Sie können die Funktion "Tipp des Tages" verwenden, um Benutzer im Voraus davon zu unterrichten, dass die Regeln für sichere Kennwörter geändert und welche neuen Kriterien gelten werden.

Sperreinstellungen

Administratoren können CC-SG- und SSH-Benutzer nach einer festgelegten Anzahl an fehlgeschlagenen Anmeldeversuchen sperren. Sie können diese Funktion für lokal authentifizierte Benutzer, für Benutzer mit Remoteauthentifizierung oder für alle Benutzer aktivieren.

Hinweis: Standardmäßig wird das Konto admin bei drei fehlgeschlagenen Anmeldeversuchen für fünf Minuten gesperrt. Für admin kann die Anzahl der fehlgeschlagenen Anmeldeversuche nicht konfiguriert werden, die für die Sperre verwendet wird.

So aktivieren Sie die Sperre:

1. Wählen Sie "Administration > Sicherheit".
2. Klicken Sie auf die Registerkarte "Anmeldeeinstellungen".
3. Markieren Sie das Kontrollkästchen "Sperre für lokale Benutzer aktiviert", wenn für lokal authentifizierte Benutzer eine Sperre aktiviert werden soll. Markieren Sie das Kontrollkästchen "Sperre für Remotebenutzer aktiviert", wenn für Benutzer mit Remoteauthentifizierung eine Sperre aktiviert werden soll.

4. Die Standardanzahl für fehlgeschlagene Anmeldeversuche ist drei. Danach wird der Benutzer gesperrt. Sie können den Wert ändern, indem Sie eine Zahl zwischen 1 und 10 eingeben.
5. Wählen Sie eine Sperrstrategie aus:
   - Sperre für Zeitraum: Legen Sie den Zeitraum in Minuten fest, den Benutzer gesperrt werden, bevor sie sich wieder anmelden können. Der Standardwert ist fünf Minuten. Sie können einen Zeitraum von 1 Minute bis zu 1440 Minuten (24 Stunden) festlegen. Ist die Zeit abgelaufen, kann sich der Benutzer wieder anmelden. Administratoren können während dieses Sperrzeitraums den Wert jederzeit überschreiben, sodass der Benutzer sich wieder bei CC-SG anmelden kann.
   - Sperre, bis Administrator Zugriff zulässt: Benutzer werden gesperrt, bis ein Administrator die Sperre für das Benutzerkonto aufhebt.
6. Geben Sie in das Feld "E-Mail-Benachrichtigung über Sperre" eine E-Mail-Adresse ein. Die Benachrichtigung wird an diese E-Mail-Adresse gesendet, wenn eine Sperre verhängt wurde. Ist das Feld leer, wird keine Benachrichtigung gesendet. **Optional.**
7. Geben Sie in das Feld "Telefonnummer" des Administrators eine Telefonnummer ein. Die Telefonnummer wird in der E-Mail-Benachrichtigung, die bei einer Sperre gesendet wird, angezeigt. **Optional.**
8. Klicken Sie zum Speichern der Änderungen auf "Aktualisieren".

So deaktivieren Sie die Sperre:

Wenn Sie die Sperre deaktivieren, dürfen sich alle Benutzer, die zurzeit in CC-SG gesperrt sind, wieder anmelden.

1. Wählen Sie "Administration > Sicherheit".
2. Öffnen Sie die Registerkarte "Anmeldeeinstellungen".
3. Deaktivieren Sie das Kontrollkästchen "Sperre für lokale Benutzer aktiviert", wenn die Sperre für lokal authentifizierte Benutzer deaktiviert werden soll. Deaktivieren Sie das Kontrollkästchen "Sperre für Remotebenutzer aktiviert", wenn die Sperre für Benutzer mit Remoteauthentifizierung deaktiviert werden soll.
4. Klicken Sie zum Speichern der Änderungen auf "Aktualisieren".

Gleichzeitige Anmeldung von Benutzern zulassen

Sie können mehrere gleichzeitige CC-SG-Sitzungen mit demselben Benutzernamen zulassen.

1. Wählen Sie "Administration > Sicherheit".
2. Klicken Sie auf die Registerkarte "Anmeldeeinstellungen".

- Markieren Sie das Kontrollkästchen "Superuser", wenn Sie mehr als eine gleichzeitige Anmeldung mit dem CC-Superuser-Konto zulassen möchten..
- Markieren Sie das Kontrollkästchen "Systemadministratoren", wenn Sie gleichzeitige Anmeldungen von Benutzern der Benutzergruppe "Systemadministratoren" zulassen möchten.
- Markieren Sie das Kontrollkästchen "Alle anderen Benutzer", wenn gleichzeitige Anmeldungen für alle anderen Benutzer zulässig sein sollen.

3. Klicken Sie zum Speichern der Änderungen auf "Aktualisieren".

Leerlaufzeitgeber konfigurieren

Sie können den Leerlaufzeitgeber konfigurieren, um festzulegen, wie lange eine CC-SG-Sitzung inaktiv bleiben kann, bevor der Benutzer bei CC-SG abgemeldet wird.

Wenn ein Benutzer Verbindungen zu Knoten offen hat, wird die Sitzung als aktiv betrachtet, und der Benutzer wird nicht abgemeldet, wenn der Leerlaufzeitgeber abläuft.

So konfigurieren Sie den Leerlaufzeitgeber:

1. Wählen Sie "Administration > Sicherheit".
2. Klicken Sie auf die Registerkarte "Anmeldeeinstellungen".
3. Geben Sie das gewünschte Zeitlimit in das Feld "Leerlaufzeit" ein.
4. Klicken Sie zum Speichern der Änderungen auf "Aktualisieren".

Portal

Über Portaleinstellungen können Administratoren ein Logo und eine Zugriffsvereinbarung konfigurieren, die Benutzern beim Zugriff auf CC-SG angezeigt werden.

So konfigurieren Sie die Portaleinstellungen:

1. Wählen Sie "Administration > Sicherheit".
2. Öffnen Sie die Registerkarte "Portal".

Logo

Sie können eine kleine Grafikdatei an CC-SG senden, die als Banner auf der Anmeldeseite verwendet wird. Die Logogröße darf maximal 998 x 170 Pixel betragen.

So senden Sie ein Logo:

1. Klicken Sie auf der Registerkarte "Portal" im Bereich "Logo" auf "Durchsuchen". Ein Dialogbildschirm "Öffnen" wird angezeigt.

2. Wählen Sie die Grafikdatei aus, die Sie als Logo verwenden möchten, und klicken Sie auf "Öffnen".
3. Klicken Sie auf "Vorschau", um das Logo anzuzeigen. Die ausgewählte Grafikdatei wird rechts angezeigt.
4. Klicken Sie zum Speichern der Änderungen auf "Aktualisieren".

Vertragliche Einschränkungen der Serviceleistungen

Sie können links neben den Anmeldefeldern auf dem Anmeldebildschirm eine Nachricht anzeigen. Der Platz wurde für die vertraglichen Einschränkungen der Serviceleistungen oder eine Vereinbarung reserviert, die Benutzer vor dem Zugriff auf CC-SG annehmen müssen. Die Annahme der vertraglichen Einschränkungen der Serviceleistungen durch den Benutzer wird in den Protokolldateien und dem Überwachungslistenbericht erfasst.

So fügen Sie vertragliche Einschränkungen der Serviceleistungen zum CC-SG-Anmeldebildschirm hinzu:

1. Markieren Sie das Kontrollkästchen "Die vertraglichen Einschränkungen der Serviceleistungen müssen akzeptiert werden", damit Benutzer das Kontrollkästchen für die Vereinbarung auf dem Anmeldebildschirm markieren müssen, bevor sie ihre Anmeldedaten eingeben können.
2. So geben Sie Ihre Meldung ein:
   a. Markieren Sie das Kontrollkästchen "Vertragliche Einschränkungen" der Serviceleistungen - Meldung:, wenn Sie den Bannertext direkt eingeben möchten.
      - Geben Sie die Meldung in das angezeigte Feld ein. Der Text darf höchstens 10.000 Zeichen umfassen.
      - Klicken Sie auf das Dropdown-Menü "Schriftart", und wählen Sie die Schriftart für die Meldung aus.
      - Klicken Sie auf das Dropdown-Menü "Größe", und wählen Sie die Schriftgröße für die Meldung aus.
   b. Markieren Sie "Vertragliche Einschränkungen der Serviceleistungen - Datei", wenn Sie eine Nachricht aus einer Textdatei (.txt) verwenden möchten.

- Klicken Sie auf "Durchsuchen". Ein Fenster wird angezeigt.
- Wählen Sie im Fenster die Textdatei mit der Nachricht aus, die Sie verwenden möchten, und klicken Sie auf "Öffnen". Der Text darf höchstens 10.000 Zeichen umfassen.
- Klicken Sie auf "Vorschau", um den Text, der in der Datei enthalten ist, anzuzeigen. Die Vorschau wird im Feld für die Bannermeldung oben angezeigt.

3. Klicken Sie zum Speichern der Änderungen auf "Aktualisieren". Die Neuigkeiten werden auf dem Anmeldebildschirm angezeigt, sobald ein Benutzer das nächste Mal auf CC-SG zugreift.

Zertifikate

Auf der Registerkarte Zertifikat können Sie eine Anforderung für die Zertifikatsignatur (certificate signing request, CSR), die zur Beantragung eines digitalen Identitätszertifikats an eine Zertifizierungsstelle gesendet wird, und ein selbstsigniertes Zertifikat erstellen oder Zertifikate und die entsprechenden privaten Schlüssel importieren und exportieren.

Zertifikate – Aufgaben

Hinweis: Die Schaltfläche unten im Bildschirm zeigt abhängig von der ausgewählten Zertifikatsoption Exportieren, Importieren oder Erzeugen an.

So exportieren Sie das aktuelle Zertifikat und den privaten Schlüssel:

1. Wählen Sie "Administration > Sicherheit".
2. Klicken Sie auf die Registerkarte "Zertifikat".
3. Wählen Sie "Aktuelles Zertifikat und privaten Schlüssel exportieren".
4. Klicken Sie auf "Exportieren". Das Zertifikat wird im Fensterbereich "Zertifikat" und der private Schlüssel im Fensterbereich "Privater Schlüssel" angezeigt.
5. Markieren Sie in jedem Fensterbereich den Text, und drücken Sie dann Strg+C, um den Text zu kopieren. Anschließend können Sie den Text an jeder beliebigen Stelle einfügen.

So erzeugen Sie eine Anforderung für Zertifikatsignatur und importieren ein eingefügtes Zertifikat und einen privaten Schlüssel:

Die CSR wird an den Zertifikatserver übermittelt, der ein signiertes Zertifikat ausgibt. Außerdem wird ein Stammzertifikat vom Zertifikatserver exportiert und in einer Datei gespeichert. Nach dem Erhalt des signierten Zertifikats von der Zertifizierungsstelle für Zertifikate können Sie das signierte Zertifikat, das Stammzertifikat und den privaten Schlüssel importieren.

1. Wählen Sie "Administration > Sicherheit".
2. Klicken Sie auf die Registerkarte "Zertifikat".
3. Klicken Sie auf "Anforderung für Zertifikatsignatur erzeugen" und dann auf "Erzeugen". Das Fenster "Anforderung für Zertifikatsignatur erzeugen" wird angezeigt.
4. Geben Sie die angeforderten Daten in die Felder ein.
   a. Verschlüsselungsmodus: Wenn nach Auswahl von "Administration" > "Sicherheit" > "Verschlüsselung" die Option "AES-Verschlüsselung zwischen Client und Server voraussetzen" ausgewählt wird, ist AES-128 die Standardeinstellung. Ist AES nicht erforderlich, ist DES 3 die Standardeinstellung.
   b. Länge des privaten Schlüssels: Der Standardwert beträgt 1024.
   c. Gültigkeitsdauer (in Tagen): maximal 4 numerische Zeichen.
   d. Ländercode: CSR-Tag ist Country Name.
   e. Bundesland oder Kanton: Maximal 64 Zeichen. Geben Sie den vollständigen Namen des Bundeslands oder Kantons ein. Abkürzungen sind nicht zulässig.
   f. Stadt/Ort: CSR-Tag ist Locality Name. Maximal 64 Zeichen.
   g. Name des registrierten Unternehmens: CSR-Tag ist Organization Name. Maximal 64 Zeichen.
   h. Abteilung: CSR-Tag ist Organization Unit Name. Maximal 64 Zeichen.
   i. Vollständiger Name der Domäne (FQDN): CSR-Tag ist Common Name.
   j. E-Mail-Adresse des Administrators: Geben Sie die E-Mail-Adresse des Administrators ein, der für die Zertifikatsanforderung verantwortlich ist.
   k. Zusätzliches Kennwort: Maximal 64 Zeichen.
5. Klicken Sie zum Erzeugen der Anforderung für Zertifikatsignatur auf OK. Die CSR und der private Schlüssel werden in den entsprechenden Feldern im Fenster "Zertifikat" angezeigt.

6. Markieren Sie den Text im Kästchen "Zertifikatsanforderung", und drücken Sie dann Strg+C, um den Text zu kopieren. Öffnen Sie einen ASCII-Editor wie Editor, und fügen Sie die Anforderung für Zertifikatsignatur in eine Datei ein, die Sie dann mit der Erweiterung .cer speichern.
7. Markieren Sie den Text im Kästchen "Privater Schlüssel", und drücken Sie dann Strg+C, um den Text zu kopieren. Öffnen Sie einen ASCII-Editor wie Editor, und fügen Sie den privaten Schlüssel in eine Datei ein, die Sie dann mit der Erweiterung .txt speichern.
8. Übermitteln Sie die .cer-Datei an den Zertifikatserver, um ein signiertes Zertifikat zu erhalten.
9. Laden Sie das Stammzertifikat vom Zertifikatserver herunter oder exportieren Sie es. Speichern Sie das Zertifikat dann in einer Datei mit der Erweiterung .cer. Dieses Zertifikat unterscheidet sich von dem signierten Zertifikat, das vom Zertifikatserver im nächsten Schritt ausgegeben wird.
10. Klicken Sie neben "Zertifizierungsstellendatei" auf "Durchsuchen", und wählen Sie die Stammzertifikatdatei aus.
11. Wählen Sie nach Erhalt des signierten Zertifikats vom Zertifikatserver die Option "Eingefügtes Zertifikat und privaten Schlüssel importieren".
12. Kopieren Sie den Text des signierten Zertifikats, und drücken Sie dann Strg+V, um den Text im Kästchen "Zertifikat" einzufügen.
13. Kopieren Sie den Text des privaten Schlüssels, der bereits als TXT-Datei gespeichert wurde, und drücken Sie dann Strg+V, um den Text im Kästchen "Privater Schlüssel" einzufügen.
14. Geben Sie raritan im Feld Kennwort ein, wenn die CSR von CC-SG erzeugt wurde. Wurde die CSR von einer anderen Anwendung erzeugt, verwenden Sie das Kennwort für diese Anwendung.

Hinweis: Ist das importierte Zertifikat von einer Stamm- oder Substamm-Zertifizierungsstelle signiert, schlägt die Verwendung eines Stamm- oder Substamm-Zertifikats fehl. Sie können dieses Problem beheben, indem Sie das Stamm- und Substamm-Zertifikat in eine Datei kopieren und dann importieren.

▶ So erzeugen Sie ein selbstsigniertes Zertifikat:

1. Wählen Sie "Administration > Sicherheit".
2. Klicken Sie auf die Registerkarte "Zertifikat".
3. Markieren Sie "Selbstsigniertes Zertifikat erzeugen", und klicken Sie dann auf "Erzeugen". Das Fenster "Selbstsigniertes Zertifikat erzeugen" wird geöffnet.
4. Geben Sie die angeforderten Daten in die Felder ein.

a. Verschlüsselungsmodus: Wenn nach Auswahl von "Administration" > "Sicherheit" > "Verschlüsselung" die Option "AES-Verschlüsselung zwischen Client und Server voraussetzen" ausgewählt wird, ist AES-128 die Standardeinstellung. Ist AES nicht erforderlich, ist DES 3 die Standardeinstellung.

b. Länge des privaten Schlüssels: Der Standardwert beträgt 1024.

c. Gültigkeitsdauer (in Tagen): maximal 4 numerische Zeichen.

d. Ländercode: CSR-Tag ist Country Name.

e. Bundesland oder Kanton: Maximal 64 Zeichen. Geben Sie den vollständigen Namen des Bundeslands oder Kantons ein. Abkürzungen sind nicht zulässig.

f. Stadt/Ort: CSR-Tag ist Locality Name. Maximal 64 Zeichen.

g. Name des registrierten Unternehmens: CSR-Tag ist Organization Name. Maximal 64 Zeichen.

h. Abteilung: CSR-Tag ist Organization Unit Name. Maximal 64 Zeichen.

i. Vollständiger Name der Domäne (FQDN): CSR-Tag ist Common Name.

j. E-Mail-Adresse des Administrators: Geben Sie die E-Mail-Adresse des Administrators ein, der für die Zertifikatsanforderung verantwortlich ist.

k. Zusätzliches Kennwort: Maximal 64 Zeichen.

5. Klicken Sie zum Erzeugen des Zertifikats auf OK. Das Zertifikat und der private Schlüssel werden im Fenster "Zertifikat" in den entsprechenden Feldern verschlüsselt angezeigt.

Zugriffssteuerungsliste

In einer IP-Zugriffssteuerungsliste sind die Bereiche von Client-IP-Adressen festgelegt, für die Sie den Zugriff auf CC-SG verweigern oder zulassen möchten. Jeder Eintrag in der Zugriffssteuerungsliste wird eine Regel, die bestimmt, ob ein Benutzer in einer bestimmten Gruppe und mit einer bestimmten IP-Adresse auf CC-SG zugreifen kann. Sie können auch Regeln einstellen, die für das gesamte CC-SG-System (wählen Sie ein System anstelle einer Benutzergruppe) auf einer Betriebssystemebene gelten. Beim Erstellen von Regeln können Sie die Regeln in der Liste anordnen, um die Reihenfolge festzulegen, in der sie angewendet werden. Regeln am Listenanfang haben Vorrang vor Regeln, die weiter unten in der Liste stehen.

So zeigen Sie die Zugriffssteuerungsliste an:

1. Wählen Sie "Administration > Sicherheit".

2. Klicken Sie auf die Registerkarte "Zugriffssteuerungsliste".

So fügen Sie der Zugriffssteuerungsliste eine Regel hinzu:

1. Wählen Sie "Administration > Sicherheit".
2. Klicken Sie auf die Registerkarte "Zugriffssteuerungsliste".
3. Klicken Sie auf das Symbol zum Einfügen einer neuen Zeile , um eine neue Zeile in die Tabelle einzufügen.
4. Legen Sie einen Bereich von IP-Adressen fest, auf den die Regel angewendet werden soll. Geben Sie hierzu den Wert für die erste IP-Adresse in das Feld "Von IP-Adresse" und den Wert für die letzte IP-Adresse in das Feld "Bis IP-Adresse" ein.
5. Klicken Sie auf den Pfeil neben der Dropdown-Liste Gruppe, um eine Benutzergruppe auszuwählen, auf die die Regel angewendet werden soll. Wenn Sie "System" auswählen, wird die Regel auf das gesamte CC-SG-System angewendet.
6. Klicken Sie auf den Pfeil neben der Dropdown-Liste Aktion, und wählen Sie "Zulassen" oder "Verweigern" aus, um festzulegen, ob die im IP-Bereich festgelegten Benutzer auf CC-SG zugreifen können.
7. Klicken Sie zum Speichern der Änderungen auf "Aktualisieren".

So fügen Sie der Zugriffssteuerungsliste eine Regel hinzu, die den Zugriff auf einer Betriebssystemebene zulässt oder verweigert:

1. Wählen Sie "Administration > Sicherheit".
2. Klicken Sie auf die Registerkarte "Zugriffssteuerungsliste".
3. Klicken Sie auf das Symbol zum Einfügen einer neuen Zeile , um eine neue Zeile in die Tabelle einzufügen.
4. Legen Sie einen Bereich von IP-Adressen fest, auf den die Regel angewendet werden soll. Geben Sie hierzu den Wert für die erste IP-Adresse in das Feld "Von IP-Adresse" und den Wert für die letzte IP-Adresse in das Feld "Bis IP-Adresse" ein.
5. Wählen Sie "Gruppe > System".
6. Klicken Sie auf den Pfeil neben der Dropdown-Liste Aktion, und wählen Sie "Zulassen" oder "Verweigern" aus, um festzulegen, ob die im IP-Bereich festgelegten Benutzer auf CC-SG zugreifen können.
7. Klicken Sie zum Speichern der Änderungen auf "Aktualisieren".

So ändern Sie die Reihenfolge, in der CC-SG Regeln anwendet:

1. Wählen Sie "Administration > Sicherheit".
2. Klicken Sie auf die Registerkarte "Zugriffssteuerungsliste".
3. Wählen Sie die Regel aus, die Sie in der Liste nach oben oder unten verschieben möchten.
4. Klicken Sie auf den Pfeil nach oben oder unten, bis sich die Regel an der richtigen Position befindet.
5. Klicken Sie zum Speichern der Änderungen auf "Aktualisieren".

So entfernen Sie eine Regel aus der Zugriffssteuerungsliste:

1. Wählen Sie "Administration > Sicherheit".
2. Klicken Sie auf die Registerkarte "Zugriffssteuerungsliste".
3. Wählen Sie die Regel aus, die Sie entfernen möchten, und klicken Sie dann auf das Symbol zum Entfernen einer Zeile.
4. Klicken Sie zum Speichern der Änderungen auf "Aktualisieren".

Benachrichtigungsmanager

Mit dem Benachrichtigungsmanager können Sie einen externen SMTP-Server so konfigurieren, dass Benachrichtigungen in CC-SG gesendet werden können. Benachrichtigungen werden verwendet, um Folgendes per E-Mail zu senden: geplante Berichte; Berichte, falls Benutzer gesperrt wurden, sowie Statusberichte erfolgreicher oder fehlgeschlagener geplanter Aufgaben. Weitere Informationen finden Sie unter ***Aufgabenmanager*** (auf Seite 330). Nach der Konfiguration des SMTP-Servers können Sie eine Test-E-Mail an den festgelegten Empfänger senden und ihn über das Testergebnis informieren.

Externe SMTP-Server konfigurieren

1. Wählen Sie "Administration > Benachrichtigungen".
2. Aktivieren Sie das Kontrollkästchen "SMTP-Benachrichtigung aktivieren".
3. Geben Sie den SMTP-Host in das Feld SMTP-Host ein. Die Regeln zur Vergabe von Hostnamen werden unter ***Terminologie/Abkürzungen*** (auf Seite 2) beschrieben.
4. Geben Sie eine gültige SMTP-Portnummer im Feld SMTP-Port ein.
5. Geben Sie einen gültigen Kontonamen in das Feld "Kontoname" ein, der zur Anmeldung beim SMTP-Server verwendet werden kann. **Optional.** Wenn diese Kontoinformationen erforderlich sind, wenden Sie sich an den Administrator des E-Mail-Servers.

6. Geben Sie das Kennwort für das Konto in die Felder "Kennwort" und "Kennwort erneut eingeben" ein. **Optional.** Wenn diese Kontoinformationen erforderlich sind, wenden Sie sich an den Administrator des E-Mail-Servers.
7. Geben Sie eine gültige E-Mail-Adresse im Feld "Von" ein, die kennzeichnet, dass die Nachricht von CC-SG ist.
8. Geben Sie in das Feld "Sendewiederholungen" die Anzahl von Wiederholungen ein, die die E-Mail erneut gesendet werden soll, falls der Vorgang fehlschlägt.
9. Geben Sie die Anzahl der Minuten von 1 bis 60 in das Feld "Intervall für Sendewiederholungen (Minuten)" ein, die verstreichen soll, bevor die E-Mail erneut gesendet wird.
10. Markieren Sie das Feld "SSL verwenden", wenn Sie die E-Mail sicher über Secure Sockets Layer (SSL) senden möchten.
11. Klicken Sie auf "Konfiguration testen", um eine Test-E-Mail an das angegebene SMTP-Konto zu senden. Sie sollten sicherstellen, dass die E-Mail empfangen wird.
12. Klicken Sie auf "Konfiguration aktualisieren", um die Änderungen zu speichern.

Aufgabenmanager

Planen Sie tägliche, wöchentliche, monatliche oder jährliche CC-SG-Aufgaben mit dem Aufgabenmanager. Eine Aufgabe kann so geplant werden, dass sie nur einmal oder regelmäßig an einem bestimmten Wochentag oder in regelmäßigen Zeitabständen durchgeführt wird. Dazu gehören beispielsweise Gerätesicherungen alle drei Wochen an einem Freitag oder eine E-Mail mit einem bestimmten Bericht jeden Montag an einen oder mehrere Empfänger.

Hinweis: Der Aufgabenmanager verwendet die Serverzeit, die in CC-SG zum Planen eingerichtet ist, und nicht die Zeit auf Ihrem Client-PC. Die Serverzeit wird oben rechts auf jeder CC-SG-Seite angezeigt.

Aufgabenarten

Die folgenden Aufgaben können geplant werden:

- Synchronisierung mit Active Directory
- CC-SG sichern
- Gerätekonfiguration sichern (einzelne Geräte oder Gerätegruppen)
- Geräteverwaltung unterbrechen und fortsetzen
- Gerätekonfiguration kopieren (einzelne Geräte oder Gerätegruppen)
- Gruppenstromversorgungssteuerung
- Ausgangs-Stromversorgungssteuerung
- Protokolle löschen
- Gerät neu starten
- Gerätekonfiguration wiederherstellen (gilt nicht für Gerätegruppen)
- Gerätefirmware aktualisieren (einzelne Geräte oder Gerätegruppen)
- Alle Berichte erstellen

Aufeinander folgende Aufgaben planen

Sie können Aufgaben aufeinander folgend planen, um sicherzustellen, dass das erwartete Verhalten wirklich eingetreten ist. Sie können die Aufgabe "Gerätefirmware aktualisieren" beispielsweise für eine bestimmte Gerätegruppe planen, dann direkt danach das Erstellen eines Anlagenverwaltungsberichts planen, um sicherzustellen, dass die richtige Version der Firmware verwendet wurde.

E-Mail-Benachrichtigungen für Aufgaben

Nach dem Durchführen einer Aufgabe kann eine E-Mail-Nachricht an einen bestimmten Empfänger gesendet werden. Sie können im Benachrichtigungsmanager angeben, wohin und wie die E-Mail gesendet wird (z. B. sicher über SSL). Weitere Informationen finden Sie unter ***Benachrichtigungsmanager*** (auf Seite 329).

Geplante Berichte

Geplante Berichte werden per E-Mail an die festgelegten Empfänger gesendet. Sie können entweder CSV oder HTML für die Version des per E-Mail versendeten Berichts angeben.

Alle Berichte mit dem Status "Fertig gestellt" werden im CC-SG für 30 Tage im HTML-Format gespeichert. Sie können die fertig gestellten Berichte im HTML-Format anzeigen, indem Sie im Menü "Berichte" die Option "Geplante Berichte" auswählen. Weitere Informationen finden Sie unter ***Geplante Berichte*** (auf Seite 261).

Aufgaben suchen und anzeigen

Sie können Aufgaben in einer Liste anzeigen, die nach von Ihnen gewählten Kriterien gefiltert wird. Zu jeder Aufgabe können Sie Aufgabendetails und Aufgabenverlauf anzeigen.

Hinweis: Wird eine Aufgabe geändert oder aktualisiert, wird der Verlauf ungültig und das Datum letzte Ausführung ist leer.

So zeigen Sie eine Aufgabe an:

1. Wählen Sie "Administration > Aufgaben".
2. Sie können nach Aufgaben suchen, indem Sie mit den Pfeiltasten nach oben und unten den Datumsbereich der Aufgabe auswählen, die Sie anzeigen möchten.
3. Sie können die Liste weiter filtern, indem Sie in jeder Liste eine oder mehrere (Strg-Taste + klicken) Aufgaben, Statusangaben oder Eigentümer auswählen.
4. Klicken Sie auf "Aufgaben anzeigen", um die gefilterte Liste der Aufgaben anzuzeigen.

So zeigen Sie den Aufgabenverlauf einer Aufgabe an:

- Markieren Sie die Aufgabe und klicken Sie auf "Aufgabenverlauf".

So zeigen Sie die Aufgabendetails einer Aufgabe an:

- Doppelklicken Sie auf eine Aufgabe, um ein Dialogfeld mit den Aufgabendetails zu öffnen.

Aufgaben planen

In diesem Abschnitt werden die meisten planbaren Aufgaben behandelt. Weitere Informationen zum Planen von Firmware-Aktualisierungen für Geräte finden Sie unter ***Firmware-Aktualisierung für Geräte planen*** (auf Seite 335).

So planen Sie eine Aufgabe:

1. Wählen Sie "Administration > Aufgaben".
2. Klicken Sie auf "Neu".
3. Geben Sie auf der Registerkarte Hauptfenster einen Namen und eine Beschreibung für die Aufgabe ein. Namen können zwischen 1 und 32 alphanumerische Zeichen sowie Unterstriche enthalten. Leerzeichen sind nicht zulässig.
4. Klicken Sie auf die Registerkarte "Aufgabendaten".

5. Klicken Sie auf die Dropdown-Liste "Aufgabenvorgang", und wählen Sie Wählen Sie die zu planende Aufgabe. Beachten Sie, dass die erforderlichen Felder von der ausgewählten Aufgabe abhängen. In den folgenden Abschnitten finden Sie weitere Informationen zu jeder Aufgabe.
   - **Synchronisierung mit Active Directory:** Siehe ***Alle AD-Module synchronisieren*** (auf Seite 238)
   - **CommandCenter sichern**: Siehe ***CC-SG sichern*** (auf Seite 265)
   - **Gerätekonfiguration sichern:** Siehe ***Gerätekonfiguration sichern*** (auf Seite 100)
   - **Geräteverwaltung unterbrechen/fortsetzen:** Siehe ***CC-SG-Verwaltung eines Geräts unterbrechen*** (auf Seite 106) und ***Verwaltung fortsetzen*** (siehe "***Geräteverwaltung fortsetzen***" auf Seite 107) zum Unterbrechen und Fortsetzen der Verwaltung einzelner Geräte. Weitere Informationen über das Planen einer Aufgabe zum Unterbrechen und Fortsetzen der Verwaltung mehrerer Geräte oder Gerätegruppen finden Sie unter ***Geräteverwaltung mit einer geplanten Aufgabe unterbrechen und fortsetzen*** (auf Seite 107).
   - **Gerätekonfiguration kopieren:** Siehe ***Gerätefunktion kopieren*** (siehe "***Gerätekonfiguration kopieren***" auf Seite 105)
   - **Gruppenstromversorgungssteuerung:** Siehe Stromversorgung für Knotengruppe steuern
   - **Ausgangs-Stromversorgungssteuerung:** Siehe **CC-SG-Benutzerhandbuch**.
   - **Power IQ-Synchronisierung**: Siehe ***Synchronisierung von Power IQ und CC-SG*** (auf Seite 404).
   - **Protokolle löschen:** Siehe ***Protokollaktivitäten konfigurieren*** (auf Seite 295).
   - **Geräte neu starten:** Siehe ***Gerät neu starten*** (auf Seite 106)
   - **Gerätekonfiguration wiederherstellen:** Siehe ***Gerätekonfiguration wiederherstellen*** (auf Seite 101) (gilt nicht für Gerätegruppen)
   - **Gerätefirmware aktualisieren (einzelne Geräte oder Gerätegruppen):** Siehe ***Firmware-Aktualisierung für Geräte planen*** (auf Seite 335)
   - **Alle Berichte erstellen:** Siehe ***Berichte*** (auf Seite 248).
6. Klicken Sie auf die Registerkarte "Serie". Die Registerkarte "Serie" ist für die Aufgabe "Gerätefirmware aktualisieren" deaktiviert.
7. Klicken Sie im Feld "Zeitraum" auf das Optionsfeld, das dem Zeitraum entspricht, nach dem die geplante Aufgabe wieder ausgeführt wird.

a. Einmal: Wählen Sie über die Pfeile nach oben und unten die Startzeit für die Aufgabe aus.

b. Periodisch: Wählen Sie über die Pfeile nach oben und unten die Startzeit für die Aufgabe aus. Geben Sie im Feld "Wiederholungsanzahl" an, wie oft die Aufgabe ausgeführt werden soll. Geben Sie den Zeitraum im Feld "Wiederholungsintervall" ein, der zwischen Wiederholungen liegen soll. Klicken Sie auf das Dropdown-Menü, und wählen Sie die Zeiteinheit in der Liste aus. Um die Aufgabe so einzustellen, dass sie auf unbestimmte Zeit im ausgewählten Intervall ausgeführt wird, oder bis Sie die Aufgabe ändern oder löschen, aktivieren Sie das Kontrollkästchen "Ununterbrochen – bis die Aufgabe geändert oder abgebrochen wird". Die Wiederholungsanzahl ist deaktiviert. Legen Sie das Wiederholungsintervall fest.

c. Täglich: Klicken Sie auf das Optionsfeld "Täglich", wenn die Aufgabe jeden Tag der Woche wiederholt werden soll. Klicken Sie auf das Optionsfeld "Werktags", wenn die Aufgabe täglich von Montag bis Freitag wiederholt werden soll.

d. Wöchentlich: Wählen Sie über die Pfeile nach oben und unten aus, wie viele Wochen zwischen dem Ausführen der Aufgaben verstreichen sollen, und aktivieren Sie das Kontrollkästchen neben jedem Tag, an dem die Aufgabe in jeder Woche, in der sie ausgeführt wird, wiederholt werden soll.

e. Monatlich: Geben Sie das Datum, an dem die Aufgabe ausgeführt werden soll, im Feld "Tage" ein, und aktivieren Sie das Kontrollkästchen neben jedem Monat, in dem die Aufgabe an dem bestimmten Datum wiederholt werden soll.

f. Jährlich: Klicken Sie auf das Dropdown-Menü, und wählen Sie den Monat, in dem die Aufgabe ausgeführt werden soll, in der Liste aus. Wählen Sie über die Pfeile nach oben und unten den Tag im Monat aus, an dem die Aufgabe ausgeführt werden soll.

8. Bei den Aufgabenwerten Täglich, Wöchentlich, Monatlich und Jährlich müssen Sie eine Start- und Endzeit für die Aufgabe im Bereich Serienbereich eingeben. Wählen Sie die Zeiten "Start um" und "Startdatum" über die Pfeile nach oben und unten aus. Klicken Sie auf das Optionsfeld neben "Kein Enddatum", wenn die Aufgabe wie angegeben unbegrenzt ausgeführt werden soll, oder klicken Sie auf das Optionsfeld neben "Enddatum" wählen Sie über die Pfeile nach oben und unten das Datum aus, ab dem die Aufgabe nicht mehr wiederholt werden soll.

9. Klicken Sie auf die Registerkarte "Wiederholen".

10. Schlägt eine Aufgabe fehl, kann sie von CC-SG zu einem späteren Zeitpunkt wie auf der Registerkarte Wiederholen angegeben wiederholt werden. Geben Sie im Feld Wiederholungsanzahl an, wie oft CC-SG versuchen soll, die Aufgabe zu wiederholen. Geben Sie den Zeitraum, der zwischen Wiederholungen liegen soll, im Feld Wiederholungsintervall ein. Klicken Sie auf das Dropdown-Menü, und wählen Sie die Zeiteinheit in der Liste aus.

Wichtig: Wenn Sie eine Aufgabe zur Aktualisierung von SX- oder KX-Geräten planen, sollte das Wiederholungsintervall größer als 20 Minuten sein, da es ca. 20 Minuten dauert, diese Geräte erfolgreich zu aktualisieren.

11. Klicken Sie auf die Registerkarte "Benachrichtigung".
12. Sie können E-Mail-Adressen angeben, die bei erfolgreichen oder fehlgeschlagenen Aufgaben eine Benachrichtigung erhalten. Standardmäßig wird die E-Mail-Adresse des Benutzers verwendet, der zurzeit angemeldet ist. Die E-Mail-Adressen der Benutzer werden im Benutzerprofil konfiguriert. Um eine weitere E-Mail-Adresse hinzuzufügen, klicken Sie auf "Hinzufügen", geben Sie die E-Mail-Adresse in das angezeigte Fenster ein, und klicken Sie dann auf OK. Standardmäßig wird eine E-Mail gesendet, wenn die Aufgabe erfolgreich durchgeführt wurde. Aktivieren Sie die Option "Bei Fehler", um Empfänger über fehlgeschlagene Aufgaben zu unterrichten.
13. Klicken Sie zum Speichern der Änderungen auf OK.

Firmware-Aktualisierung für Geräte planen

Sie können eine Aufgabe planen, um mehrere Geräte des gleichen Typs, z. B. KX oder SX, innerhalb einer Gerätegruppe zu aktualisieren. Sobald die Aufgabe beginnt, ist im Menü Berichte > Geplante Berichte der Bericht „Gerätefirmware aktualisieren“ verfügbar. In diesem Bericht können Sie den Aktualisierungsstatus in Echtzeit verfolgen. Dieser Bericht wird auch per E-Mail gesandt, wenn Sie die Option auf der Registerkarte Benachrichtigung festlegen.

Im Raritan-Benutzerhandbuch des jeweiligen Geräts finden Sie Informationen über die geschätzten Aktualisierungszeiten.

So planen Sie eine Firmwareaktualisierung für Geräte:

1. Wählen Sie "Administration > Aufgaben".
2. Klicken Sie auf "Neu".
3. Geben Sie auf der Registerkarte Hauptfenster einen Namen und eine Beschreibung für die Aufgabe ein. Mit dem von Ihnen gewählten Namen werden die Aufgabe und der Bericht, der der Aufgabe zugewiesen ist, gekennzeichnet.
4. Klicken Sie auf die Registerkarte "Aufgabendaten".

5. Legen Sie die Details für die Geräteaktualisierung fest:
   a. Aufgabenvorgang: Wählen Sie Gerätefirmware aktualisieren.
   b. Gerätegruppe: Wählen Sie die Gerätegruppe, die die Geräte enthält, die Sie aktualisieren möchten.
   c. Gerätetyp: Wählen Sie den Gerätetyp, den Sie aktualisieren möchten. Wenn Sie mehr als einen Gerätetyp aktualisieren müssen, müssen Sie für jeden Typ eine Aufgabe planen.
   d. Gleichzeitige Aktualisierungen: Legen Sie die Anzahl der Geräte fest, die mit der Dateiübertragungsaufgabe der Aktualisierung gleichzeitig beginnen sollen. Die Höchstanzahl beträgt 10. Nach jeder Dateiübertragung wird eine neue Dateiübertragung begonnen. Auf diese Weise wird sichergestellt, dass nur die maximale Anzahl an gleichzeitigen Aktualisierungen zur selben Zeit durchgeführt wird.
   e. Aktualisierungsdatei: Wählen Sie die Firmwareversion, auf die Sie aktualisieren möchten. Es werden nur die verfügbaren Aktualisierungsdateien, die für den ausgewählten Gerätetyp geeignet sind, als Optionen angezeigt.
6. Legen Sie den Zeitraum für die Aktualisierung fest:
   a. Startdatum/Startzeit: Wählen Sie das Datum und die Uhrzeit, zu der die Aufgabe beginnen soll. Das Startdatum und die Startzeit müssen in der Zukunft liegen.
   b. Aktualisierungszeitfenster beschränken und Spätester Startzeitpunkt (Datum/Uhrzeit) für Aktualisierung: Wenn Sie alle Aktualisierungen innerhalb eines festgelegten Zeitfensters beenden müssen, verwenden Sie diese Felder, um das Datum und die Uhrzeit festzulegen, nach der keine neuen Aktualisierungen beginnen können. Wählen Sie Aktualisierungszeitfenster beschränken, um das Feld Spätester Startzeitpunkt (Datum/Uhrzeit) für Aktualisierung zu aktivieren.
7. Legen Sie fest, welche Geräte in welcher Reihenfolge aktualisiert werden. Platzieren Sie Geräte mit einer höheren Priorität an den Anfang der Liste.
   a. Wählen Sie in der Liste Verfügbar alle Geräte aus, die Sie aktualisieren möchten. Klicken Sie auf Hinzufügen, um das jeweilige Gerät in die Liste Ausgewählt zu verschieben.
   b. Wählen Sie in der Liste Ausgewählt ein Gerät aus, und verschieben Sie es mit den Pfeiltasten an die Position in der Reihenfolge, an der es aktualisiert werden soll.
8. Legen Sie fest, ob fehlgeschlagene Aktualisierungen wiederholt werden sollen.
   a. Klicken Sie auf die Registerkarte "Wiederholen".

b. Wiederholungsanzahl: Geben Sie an, wie oft CC-SG eine fehlgeschlagene Aktualisierung wiederholen soll.

c. Wiederholungsintervall: Geben Sie die Zeitdauer an, die zwischen den Versuchen verstreichen soll. Standardmäßig können 30, 60 und 90 Minuten ausgewählt werden. Dies sind die optimalen Wiederholungsintervalle.

9. Legen Sie E-Mail-Adressen fest, die Benachrichtigungen über eine erfolgreiche und fehlgeschlagene Ausführung empfangen sollen. Standardmäßig wird die E-Mail-Adresse des Benutzers verwendet, der zurzeit angemeldet ist. Die E-Mail-Adressen der Benutzer werden im Benutzerprofil konfiguriert.

   a. Klicken Sie auf die Registerkarte "Benachrichtigung".

   b. Klicken Sie auf "Hinzufügen", geben Sie die E-Mail-Adresse in das eingeblendete Fenster ein, und klicken Sie dann auf OK.

   c. Wählen Sie Bei Fehler, wenn eine E-Mail gesendet werden soll, falls eine Aktualisierung fehlschlägt.

   d. Wählen Sie Bei Erfolg, wenn eine E-Mail gesendet werden soll, falls alle Aktualisierungen erfolgreich abgeschlossen werden.

10. Klicken Sie zum Speichern der Änderungen auf OK.

    Nach dem Beginn der Aufgabenausführung können Sie den Bericht „Gerätefirmware aktualisieren“ jederzeit während des geplanten Zeitraums öffnen, um den Status der Aktualisierungen anzuzeigen. Siehe ***Bericht "Gerätefirmware aktualisieren"*** (auf Seite 262).

Geplante Aufgaben ändern

Sie können eine geplante Aufgabe vor ihrer Ausführung ändern.

So ändern Sie eine geplante Aufgabe:

1. Wählen Sie die zu ändernde Aufgabe.
2. Klicken Sie auf "Bearbeiten".
3. Ändern Sie die Aufgabenspezifikationen nach Bedarf. Weitere Informationen zu Registerkartenbeschreibungen finden Sie unter ***Aufgaben planen*** (auf Seite 332) und ***Firmware-Aktualisierung für Geräte planen*** (auf Seite 335).
4. Klicken Sie zum Speichern der Änderungen auf "Aktualisieren".

Aufgaben neu planen

Die Funktion "Speichern unter" im Aufgabenmanager erlaubt Ihnen, eine abgeschlossene Aufgabe, die Sie erneut ausführen möchten, neu zu planen. Dies ist auch eine praktische Möglichkeit, um eine neue Aufgabe zu erstellen, die einer abgeschlossenen Aufgabe ähnelt.

So planen Sie eine Aufgabe neu:

1. Wählen Sie "Administration > Aufgaben".
2. Wählen Sie auf der Seite "Aufgabenmanager" die neu zu planende Aufgabe aus. Suchen Sie mit Filterkriterien nach der Aufgabe.
3. Klicken Sie auf "Speichern unter".
4. Im angezeigten Fenster "Aufgabe speichern unter" werden die Registerkarten mit den Daten der zuvor konfigurierten Aufgabe gefüllt.
5. Ändern Sie die Aufgabenspezifikationen nach Bedarf. Weitere Informationen zu Registerkartenbeschreibungen finden Sie unter ***Aufgaben planen*** (auf Seite 332) und ***Firmware-Aktualisierung für Geräte planen*** (auf Seite 335).
6. Klicken Sie zum Speichern der Änderungen auf OK.

Aufgaben planen, die einer anderen Aufgabe ähneln

Sie können eine zuvor konfigurierte Aufgabe als "Vorlage" verwenden, um eine neue Aufgabe mit ähnlichen Spezifikationen zu planen.

So planen Sie eine Aufgabe, die einer anderen Aufgabe ähnelt:

- Weitere Informationen finden Sie unter ***Aufgaben neu planen*** (auf Seite 338).

Aufgaben löschen

Sie können eine Aufgabe löschen, um sie aus dem Aufgabenmanager zu entfernen. Sie können keine Aufgaben löschen, die gerade ausgeführt werden.

So löschen Sie eine Aufgabe:

- Wählen Sie die Aufgabe aus und klicken Sie auf "Löschen".

SSH-Zugriff auf CC-SG

Verwenden Sie SSH-Clients (Secure Shell) wie Putty oder OpenSHH-Client, um auf eine Befehlszeilenschnittstelle auf SSH-Server (v2) auf CC-SG zuzugreifen. Nur ein Teil der CC-SG-Befehle zur Verwaltung von Geräten und CC-SG wird über SSH ausgegeben.

Der Benutzer des SSH-Clients wird von CC-SG authentifiziert, in dem vorhandene Authentifizierungs- und Autorisierungsrichtlinien auf den SSH-Client angewendet werden. Die für den SSH-Client verfügbaren Befehle werden von den Berechtigungen für die Benutzergruppen bestimmt, denen der Benutzer des SSH-Clients angehört.

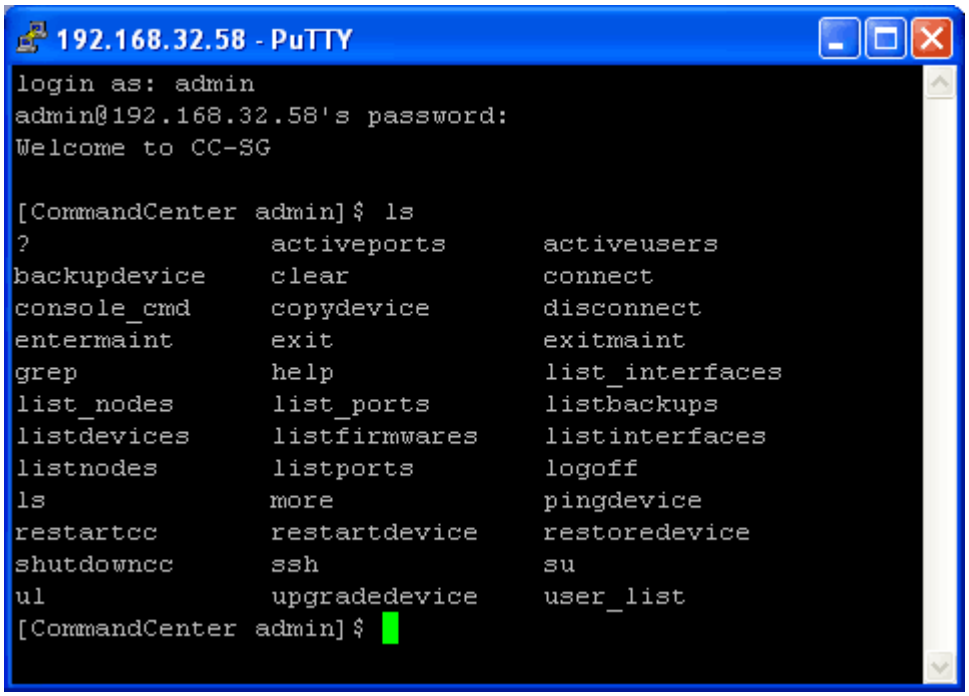
Administratoren, die über SSH auf CC-SG zugreifen, können einen CC-Superuser-SSH-Benutzer nicht abmelden, können jedoch alle anderen Benutzer von SSH-Clients, einschließlich Systemadministratoren, abmelden.

So greifen Sie auf CC-SG über SSH zu:

1. Starten Sie einen SSH-Client wie PuTTy.
2. Geben Sie die IP-Adresse von CC-SG an.
3. Geben Sie die SSH-Portnummer an. Der Standardwert lautet 22. Sie können den Port für den SSH-Zugriff im Sicherheitsmanager konfigurieren. Weitere Informationen finden Sie unter ***Sicherheitsmanager*** (auf Seite 316).
4. Öffnen Sie die Verbindung.
5. Melden Sie sich mit Ihrem CC-SG-Benutzernamen und -Kennwort an.
6. Eine Shell-Eingabeaufforderung wird angezeigt.

So zeigen Sie alle SSH-Befehle an:

- Geben Sie "ls" ein, um alle verfügbaren Befehle anzuzeigen.



Hilfe zu SSH-Befehlen erhalten

Sie können eine eingeschränkte Hilfe zu allen Befehlen gleichzeitig erhalten. Sie können auch eine ausführliche Hilfe zu jeweils einem Befehl anfordern.

So erhalten Sie Hilfe zu einem einzelnen SSH-Befehl:

1. Geben Sie bei der Shell-Eingabeaufforderung den Befehl ein, zu dem Sie Hilfe wünschen, gefolgt von einem Leerzeichen und `-h`. Beispiel:

   ```
   connect -h
   ```

2. Auf dem Bildschirm werden Informationen zum Befehl, zu den Parametern und zur Nutzung angezeigt.

So erhalten Sie Hilfe für alle SSH-Befehle:

1. Geben Sie bei der Shell-Eingabeaufforderung den folgenden Befehl ein:

   ```
   help
   ```

2. Für jeden SSH-Befehl wird auf dem Bildschirm eine kurze Beschreibung und ein Beispiel angezeigt.

SSH-Befehle und Parameter

In der folgenden Tabelle sind alle verfügbaren SSH-Befehle aufgeführt. Sie müssen über die entsprechenden Berechtigungen in CC-SG verfügen, um auf jeden Befehl zugreifen zu können.

Einige Befehle verfügen über zusätzliche Parameter, die Sie eingeben müssen, um den Befehl auszuführen. Weitere Informationen zur Eingabe von Befehlen finden Sie unter ***Tipps zu Befehlen*** (auf Seite 345).

So listen Sie aktive Ports auf:

```
activeports
```

So listen Sie aktive Benutzer auf:

```
activeusers
```

So sichern Sie eine Gerätekonfiguration:

```
backup device <[-host <Host>] | [-id <Geräte-ID>]>
backup_name [description]
```

So löschen Sie den Bildschirm:

```
clear
```

So stellen Sie eine Verbindung zu einem seriellen Port her:

Wenn <Portname> oder <Gerätename> Leerzeichen enthalten, sollten die Namen zwischen Anführungszeichen gestellt werden.

```
connect [-d <Gerätename>] [-e <Escape-Zeichen>] <[-i
<Schnittstellen-ID>] | [-n <Portname>] | [Port-ID]>
```

So kopieren Sie eine Gerätekonfiguration von einem Gerät auf das andere. Nur SX-Geräte mit derselben Port-Anzahl:

```
copydevice <[-b <Sicherungs-ID>] | [source_device_host]>
target_device_host
```

So schließen Sie eine Port-Verbindung:

```
disconnect <[-u <Benutzername>] [-p <Port-ID>] [-id
<Verbindungs-ID>]>
```

So rufen Sie den Wartungsmodus auf:

```
entermaint  minutes [message]
```

So beenden Sie den Wartungsmodus:

```
exitmaint
```

So suchen Sie nach Text eines Piped Output Stream:

```
grep search_term
```

So zeigen Sie den Hilfebildschirm für alle Befehle an:

```
help
```

So führen Sie alle verfügbaren Sicherungen für Gerätekonfigurationen auf:

```
listbackups <[-id <Geräte-ID>] | [host]>
```

So listen Sie alle verfügbaren Geräte auf:

```
listdevices
```

So führen Sie Firmwareversionen auf, die zur Aktualisierung verfügbar sind:

```
listfirmwares [[-id <Geräte-ID>] | [host]]
```

So führen Sie alle Schnittstellen auf:

```
listinterfaces [-id <Knoten-ID>]
```

So führen Sie alle Knoten auf:

```
listnodes
```

So führen Sie alle Ports auf:

```
listports  [[-id <Geräte-ID>] | [host]]
```

So melden Sie einen Benutzer ab:

```
logoff  [-u <Benutzername>] message
```

So führen Sie alle Befehle auf:

```
ls
```

So legen Sie die Paginierung fest:

```
more [-p <Seitengröße>]
```

So pingen Sie ein Gerät an:

```
pingdevice <[-id <Geräte-ID>] | [host]>
```

So starten Sie CC-SG neu:

```
restartcc minutes [message]
```

So starten Sie ein Gerät neu:

```
restartdevice <[-id <Geräte-ID>] | [host]>
```

So stellen Sie eine Gerätekonfiguration wieder her:

```
restoredevice <[-host <Host>] | [-id <Geräte-ID>]>
[backup_id]
```

So fahren Sie CC-SG herunter:

```
shutdowncc minutes [message]
```

So öffnen Sie eine SSH-Verbindung zu einem SX-Gerät:

```
ssh  [-e <Escape-Zeichen>] <[-id <Geräte-ID>] | [host]>
```

So ändern Sie einen Benutzer:

```
su [-u <Benutzername>]
```

So aktualisieren Sie die Firmware eines Geräts:

```
upgradedevice <[-id <Geräte-ID>] | [host]>
```

So führen Sie alle aktuellen Benutzer auf:

```
userlist
```

So beenden Sie die SSH-Sitzung:

```
exit
```

Tipps zu Befehlen

- Bei Befehlen, die eine IP-Adresse weiterleiten (z. B. `upgradedevice`), können Sie den Hostnamen für eine IP-Adresse einsetzen. Die Regeln zur Vergabe von Hostnamen werden unter ***Terminologie/Abkürzungen*** (auf Seite 2) beschrieben.
- Die Befehle `copydevice` und `restartdevice` gelten nur für einige Raritan-Geräte. Dominion SX und IPMI-Server werden von diesen Befehlen nicht unterstützt.
- Teile eines Befehls in eckigen Klammern sind optional. Sie brauchen diesen Teil des Befehls nicht zu verwenden.
- Einige Befehle enthalten zwei Segmente, die durch das "Oder"-Zeichen getrennt sind: |

  Sie müssen einen der aufgeführten Befehlsteile eingeben, jedoch nicht beide.
- Teile eines Befehls in eckigen Klammern zeigen den Text, den Sie eingeben müssen. Geben Sie nicht die eckigen Klammern ein. Beispiel:

Befehlssyntax	Geräte-ID-Wert	Sie sollten Folgendes eingeben:
`ssh -id <Geräte-ID>`	100	`ssh -id 100`

- Das Standard-Escapezeichen ist eine Tilde gefolgt von einem Punkt. Beispiel:

  `~.`

  Weitere Informationen zur Verwendung des Escapezeichens und des Beenden-Befehls finden Sie unter ***SSH-Verbindungen beenden*** (auf Seite 348).

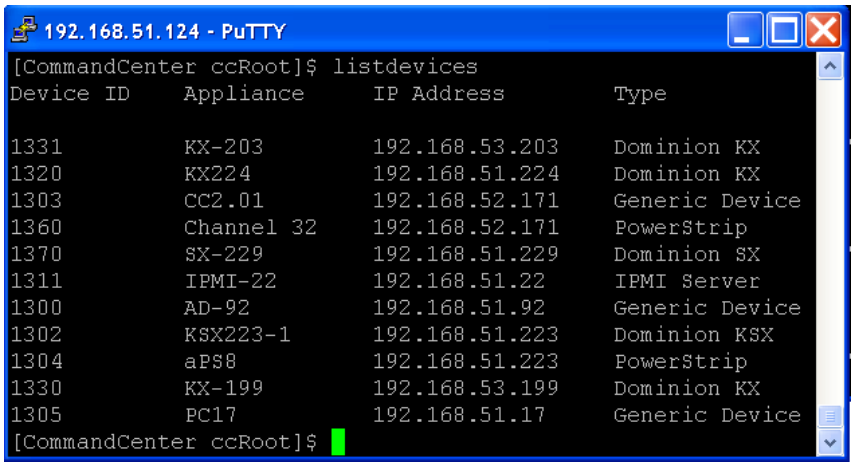
Möglicherweise treten bei der Verwendung des Escapezeichens im Linux-Terminal oder Client Probleme auf. Raritan empfiehlt, dass Sie beim Erstellen einer neuen Portverbindung ein neues Escapezeichen definieren. Der Befehl lautet `connect [-e <Escapezeichen>] [Port_ID]`. Wenn Sie beispielsweise beim Verbinden des Ports mit der ID 2360 "m" als Escapezeichen definieren, geben Sie `connect -e m 2360` ein.

SSH-Verbindung zu einem seriellen Gerät herstellen

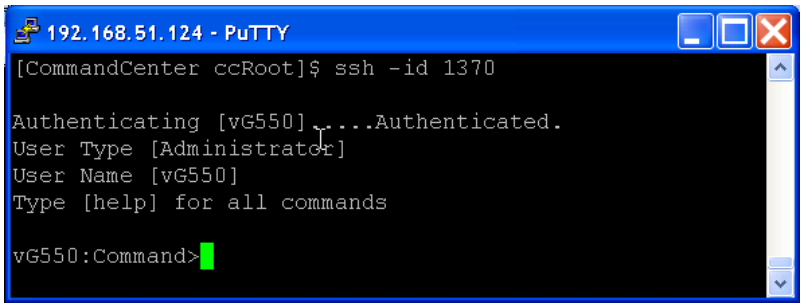
Sie können eine SSH-Verbindung zu einem seriellen Gerät herstellen, um administrative Aufgaben auf dem Gerät durchzuführen. Nach dem Verbindungsaufbau stehen die administrativen Befehle zur Verfügung, die vom seriellen Gerät unterstützt werden.

Hinweis: Stellen Sie vor der Verbindung sicher, dass das serielle Gerät zu CC-SG hinzugefügt wurde.

1. Geben Sie `listdevices` ein, um sicherzustellen, dass das serielle Gerät zu CC-SG hinzugefügt wurde.



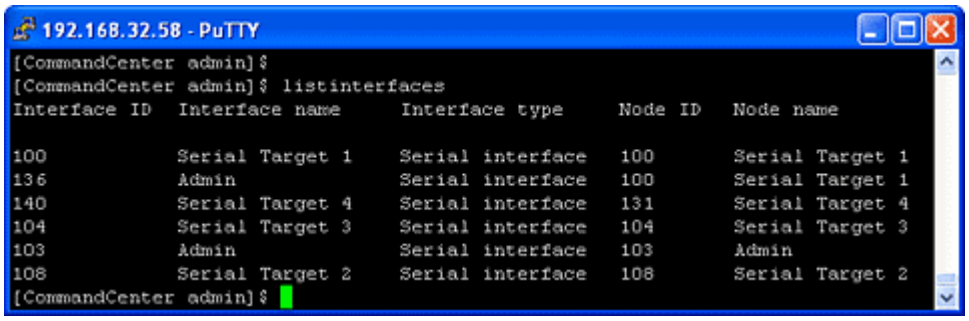
2. Stellen Sie eine Verbindung zum Gerät her, indem Sie `ssh -id <Geräte-ID>` eingeben.
   Für das oben gezeigte Beispiel können Sie eine Verbindung zu SX-229 herstellen, indem Sie `ssh -id 1370` eingeben.



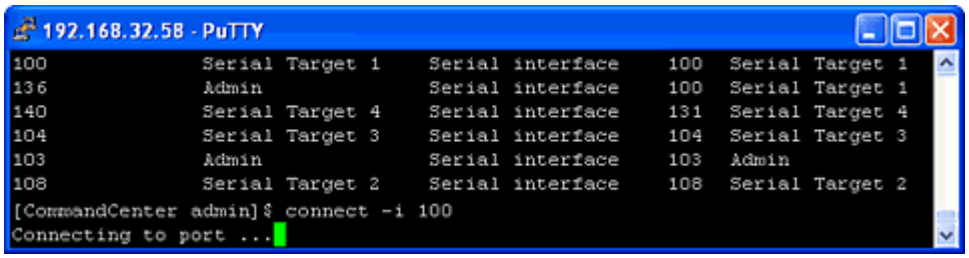
Verbindung zum Knoten mit SSH über serielle Out-of-Band-Schnittstelle herstellen

Sie können SSH verwenden, um eine Verbindung zu einem Knoten über die zugewiesene serielle Out-of-Band-Schnittstelle herzustellen. Die SSH-Verbindung ist im Proxymodus.

1. Geben Sie `listinterfaces` ein, um die Knoten-IDs und verknüpften Schnittstellen anzuzeigen.



2. Geben Sie `connect -i <Schnittstellen-ID>` ein, um eine Verbindung zu dem Knoten herzustellen, der mit der Schnittstelle verknüpft ist.



3. Bei der angezeigten Eingabeaufforderung können Sie bestimmte Befehle oder Aliasse eingeben.

Befehl	Alias	Beschreibung
`quit`	`q`	Trennt die Verbindung, und wechselt zur SSH-Eingabeaufforderung.
`get_write`	`gw`	Richtet den Schreibzugriff ein. SSH-Benutzer können Befehle auf dem Zielserver ausführen, während Browser-Benutzer den Vorgang nur beobachten können.
`get_history`	`gh`	Ruft die Verlaufsdaten ab. Zeigt die letzten Befehle und Ergebnisse für den Zielserver an.
`send_break`	`sb`	Sendet einen Pausebefehl. Unterbricht die Schleife auf dem Zielserver, die vom

Befehl	Alias	Beschreibung
		Browser-Benutzer gestartet wurde.
`help`	`?,h`	Zeigt das Hilfefenster an.

SSH-Verbindungen beenden

Sie können nur zu CC-SG SSH-Verbindungen herstellen, oder Sie können eine Verbindung zu CC-SG herstellen und dann eine Verbindung zu einem Port, Gerät oder Knoten herstellen, der/das von CC-SG verwaltet wird. Es gibt verschiedene Möglichkeiten, diese Verbindungen zu beenden, je nachdem, welchen Teil Sie beenden möchten.

So beenden Sie die gesamte Verbindung zu CC-SG:

Dieser Befehl beendet die gesamte SSH-Verbindung, einschließlich Port-, Gerät- oder Knotenverbindungen über CC-SG.

- Geben Sie bei der Eingabeaufforderung den folgenden Befehl ein und drücken Sie die Eingabetaste:

```
exit
```

So beenden Sie eine Verbindung zu einem Port, Gerät oder Knoten, während die Verbindung zu CC-SG aufrecht erhalten wird:

Sie können die Verbindung zu einem Port, Gerät oder Knoten mit dem Escapezeichen beenden, während die SSH-Verbindung zu CC-SG aufrecht erhalten wird.

Das Standard-Escapezeichen ist eine Tilde gefolgt von einem Punkt.

- Geben Sie bei der Eingabeaufforderung den folgenden Befehl ein und drücken Sie die Eingabetaste:

```
~.
```

Möglicherweise treten bei der Verwendung des Escapezeichens im Linux-Terminal oder Client Probleme auf. Raritan empfiehlt, dass Sie beim Erstellen einer neuen Portverbindung ein neues Escapezeichen definieren. Der Befehl lautet `connect [-e <Escapezeichen>] [Port_ID]`. Wenn Sie beispielsweise beim Verbinden des Ports mit der ID 2360 "m" als Escapezeichen definieren, geben Sie `connect -e m 2360` ein.

Serieller Administrationsport

Der serielle Administrationsport am CC-SG kann direkt an ein serielles Raritan-Gerät wie Dominion SX oder Dominion KSX angeschlossen werden.

Sie können mit einem Terminalemulationsprogramm wie HyperTerminal oder PuTTy über die IP-Adresse eine Verbindung zum SX- oder KSX-Gerät herstellen. Stellen Sie im Terminalemulationsprogramm eine Baudrate ein, die mit der Baudrate des SX- oder KSX-Geräts identisch ist.

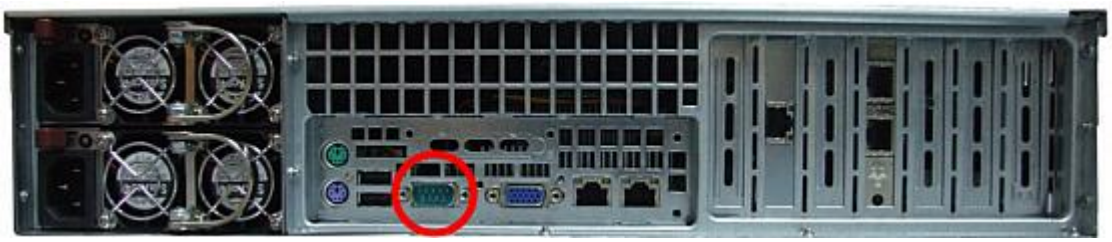
SX-Anforderungen:

Verwenden Sie einen ASCSDB9F-Adapter, um die CC-SG-Einheit mit dem SX zu verbinden. Nutzen Sie die Standard-Einstellungen für den SX-Port: 9600 bps, Parität = Keine/8, Flusssteuerung = Keine, Emulation = VT100.

V1 – Serieller Administrationsport:

E1 – Serieller Administrationsport:

- ODER -



Terminalemulationsprogramme

HyperTerminal ist auf vielen Windows-Betriebssystemen verfügbar. HyperTerminal ist nicht auf Windows Vista verfügbar.

PuTTy ist ein kostenloses Programm, das Sie im Internet herunterladen können.

CC-SG-Seriennummer auffinden

So finden Sie Ihre CC-SG-Seriennummer:

1. Melden Sie sich beim Administrations-Client an.
2. Wählen Sie "Hilfe > Info zu Raritan Secure Gateway".
3. Es öffnet sich ein neues Fenster mit Ihrer CC-SG-Seriennummer.

Web Services-API

Sie müssen die Endbenutzerbedingungen annehmen, bevor Sie CC-SG einen WS-API-Client hinzufügen können. Sie können bis zu fünf WS-API-Clients hinzufügen. Weitere Informationen zur Verwendung der API finden Sie im CC-SG Web Services API Handbuch.

So fügen Sie eine WS-API hinzu:

1. Wählen Sie "Zugang > WS-API hinzufügen". Die Option ist nur für Benutzer mit der Berechtigung CC-Setup und -Steuerung verfügbar.
2. Lesen Sie die Endbenutzerbedingungen.
   - Sie können den Text zum Speichern kopieren und einfügen, oder "Secure Gateway > Drucken" auswählen.
   - Nach der abgeschlossenen Konfiguration sind diese Bedingungen auch im Menü Zugang verfügbar.
3. Klicken Sie auf Annehmen. Das Fenster Neue WS-API-Konfiguration wird geöffnet.
4. Geben Sie die Daten ein, die für den WP-Client erforderlich sind.
   - WS-Client-Name: Maximal 64 Zeichen.
   - Lizenzschlüssel: Ihr Lizenzschlüssel von Raritan. Jede CC-SG-Einheit muss über einen eindeutigen Lizenzschlüssel verfügen.
   - IP-Adresse/Hostname: Maximal 64 Zeichen.
   - HTTPS-WS-Port: Feld mit Lesezugriff. CC-SG verwendet den Port 9443, wenn eine Vertrauensfestlegung erstellt wird.
   - Name des lizenzierten Anbieters: Maximal 64 Zeichen.

5. Erzeugen Sie ein selbstsigniertes Zertifikat.
   a. Verschlüsselungsmodus: Wenn nach Auswahl von "Administration" > "Sicherheit" > "Verschlüsselung" die Option "AES-Verschlüsselung zwischen Client und Server voraussetzen" ausgewählt wird, ist AES-128 die Standardeinstellung. Ist AES nicht erforderlich, ist DES 3 die Standardeinstellung.
   b. Länge des privaten Schlüssels: Der Standardwert beträgt 1024.
   c. Gültigkeitsdauer (in Tagen): maximal 4 numerische Zeichen.
   d. Ländercode: CSR-Tag ist Country Name.
   e. Bundesland oder Kanton: Maximal 64 Zeichen. Geben Sie den vollständigen Namen des Bundeslands oder Kantons ein. Abkürzungen sind nicht zulässig.
   f. Stadt/Ort: CSR-Tag ist Locality Name. Maximal 64 Zeichen.
   g. Name des registrierten Unternehmens: CSR-Tag ist Organization Name. Maximal 64 Zeichen.
   h. Abteilung: CSR-Tag ist Organization Unit Name. Maximal 64 Zeichen.
   i. Vollständiger Name der Domäne (FQDN): CSR-Tag ist Common Name.
   j. E-Mail-Adresse des Administrators: Geben Sie die E-Mail-Adresse des Administrators ein, der für die Zertifikatsanforderung verantwortlich ist.
   k. Zusätzliches Kennwort: Maximal 64 Zeichen.

   Hinweis: Das zusätzliche Kennwort wird intern von CC-SG verwendet, um das Zertifikat zu generieren. Sie müssen sich dieses Kennwort nicht merken.

   l. Kennwort: Geben Sie ein Keystore-Kennwort ein. Verwenden Sie dieses Kennwort zum Öffnen der .P12-Datei, die Sie in Schritt 7 speichern. Wenn Sie das generierte Zertifikat kopieren und stattdessen in Ihren eigenen Keystore importieren, müssen Sie sich dieses Keystore-Kennwort nicht merken.
6. Klicken Sie auf Zertifikat erzeugen. Der Text wird im Kästchen "Zertifikat" angezeigt.
7. Klicken Sie auf "In Datei speichern", um das Zertifikat in einer P12-Datei zu speichern. Oder kopieren Sie das generierte Zertifikat und importieren Sie es in Ihren eigenen Keystore.
8. Klicken Sie auf "Speichern", um die Änderungen zu speichern.

CC-NOC

Ab CC-SG, Version 4.2, kann nicht mehr von CC-SG aus auf CC-NOC zugegriffen werden.

Kapitel 16 Diagnosekonsole

Die Diagnosekonsole ist eine nicht grafische, menübasierte Schnittstelle, die lokalen Zugriff auf CC-SG bereitstellt. Sie können auf die Diagnosekonsole über einen seriellen oder KVM-Port zugreifen. Weitere Informationen finden Sie unter ***Auf die Diagnosekonsole über VGA-/Tastatur-/Mausport zugreifen*** (auf Seite 353). Sie können auf die Diagnosekonsole auch über SSH-Clients (Secure Shell) wie Putty oder OpenSSH-Client zugreifen. Weitere Informationen finden Sie unter ***Über SSH auf die Diagnosekonsole zugreifen*** (auf Seite 353).

Die Diagnosekonsole bietet zwei Benutzeroberflächen:

1. Statuskonsole: Weitere Informationen finden Sie unter ***Die Statuskonsole*** (auf Seite 354).
2. Administratorkonsole. Weitere Informationen finden Sie unter ***Die Administratorkonsole*** (auf Seite 361).

Hinweis: Wenn Sie über SSH auf die Diagnosekonsole zugreifen, übernehmen die Statuskonsole und Administratorkonsole die in Ihrem SSH-Client konfigurierten Anzeigeeinstellungen sowie die Tastaturbindungen. Diese Anzeigeeinstellungen unterscheiden sich eventuell von denen in dieser Dokumentation.

In diesem Kapitel

Auf die Diagnosekonsole zugreifen 353
Statuskonsole 354
Administratorkonsole 361

Auf die Diagnosekonsole zugreifen

Auf die Diagnosekonsole über VGA-/Tastatur-/Mausport zugreifen

1. Schließen Sie einen VGA-Monitor sowie eine PS2-Tastatur und -Maus auf der Rückseite der CC-SG-Einheit an.
2. Drücken Sie die Eingabetaste, um eine Anmeldeaufforderung auf dem Bildschirm anzuzeigen.

Über SSH auf die Diagnosekonsole zugreifen

1. Starten Sie einen SSH-Client wie PuTTy auf einem Client-PC, der über Netzwerkkonnektivität zu CC-SG verfügt.
2. Geben Sie eine IP-Adresse oder einen IP-Hostnamen von CC-SG ein, wenn CC-SG mit einem DNS-Server registriert wurde.

3. Legen Sie 23 für den Port fest. Der SSH-Standardport lautet 22. Wenn Sie den Port nicht auf 23 ändern, greift der SSH-Client auf die Befehlszeilenschnittstelle des CC-SG und nicht auf die Diagnosekonsole zu.
4. Klicken Sie auf die Schaltfläche zum Verbinden. Ein Fenster zur Eingabe der Anmeldeinformationen wird angezeigt.

Statuskonsole

Die Statuskonsole

- Über die Statuskonsole können Sie den Zustand von CC-SG, die verschiedenen Dienste, die von CC-SG verwendet werden, sowie das angeschlossene Netzwerk überprüfen.
- Für die Statuskonsole ist standardmäßig kein Kennwort erforderlich.
- Sie können CC-SG so konfigurieren, dass die Statuskonsoleninformationen über eine Webschnittstelle bereitgestellt werden. Sie müssen dazu die entsprechenden Optionen für die Webstatuskonsole aktivieren. Siehe ***Auf die Statuskonsole über den Webbrowser zugreifen*** (auf Seite 355). Die über das Web zur Verfügung gestellten Statuskonsoleninformationen können mithilfe eines Kontos und Kennworts geschützt werden.

Auf die Statuskonsole zugreifen

Es gibt mehrere Möglichkeiten, die Statuskonsoleninformationen anzuzeigen: VGA-/Tastatur-/Mausport, SSH oder Webbrowser.

Auf die Statuskonsole über VGA-/Tastatur-/Mausport oder SSH zugreifen

So greifen Sie auf die Statuskonsole über VGA-/Tastatur-/Mausport oder SSH zu:

1. Öffnen Sie die Diagnostikonsole. Siehe ***Auf die Diagnosekonsole zugreifen*** (auf Seite 353).
2. Geben Sie beim Anmeldebildschirm "status" ein.
3. Die aktuellen Systeminformationen werden angezeigt.

Auf die Statuskonsole über den Webbrowser zugreifen

Um die Statuskonsoleninformationen über das Web abzurufen, müssen Sie die entsprechenden Optionen in der Diagnosekonsole aktivieren. Außerdem muss der Webserver aktiv und betriebsbereit sein.

1: Aktivieren Sie die entsprechenden Optionen für die Webstatuskonsole in der Diagnostikkonsole:

1. Wählen Sie "Operation > Diagnostic Console Config".
2. Wählen Sie in der Liste "Ports" die Option "Web".
3. Aktivieren Sie in der Liste "Status" das Kontrollkästchen "Status" neben "Web".
4. Klicken Sie auf Speichern.

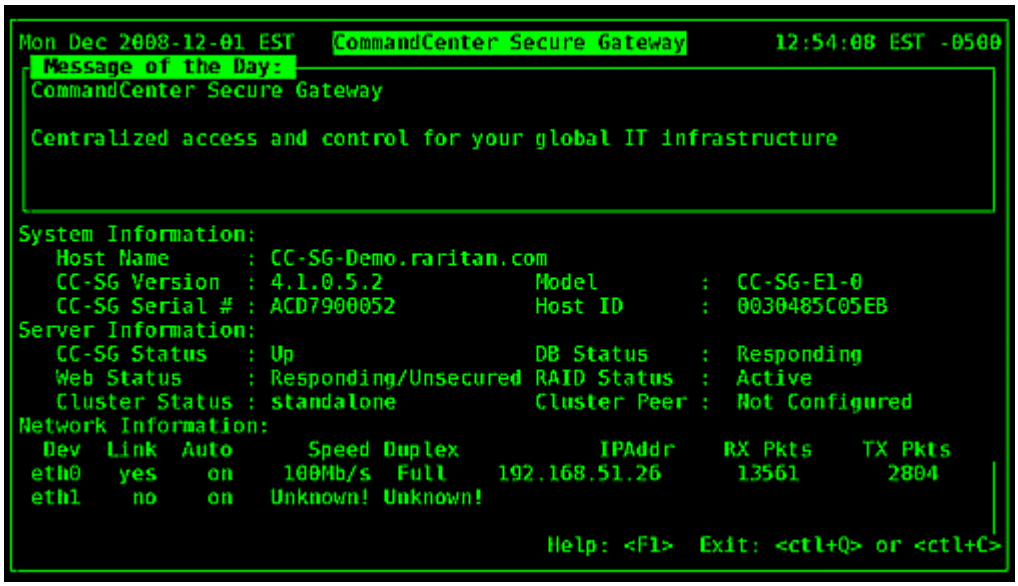
2: Öffnen Sie die Statuskonsole über den Webbrowser:

1. Verwenden Sie einen unterstützten Internetbrowser, und geben Sie folgenden URL ein: `http(s)://<IP-Adresse>/status/`, wobei `<IP-Adresse>` für die IP-Adresse von CC-SG steht. Der Schrägstrich (/) nach "/status" ist obligatorisch. Beispiel: `https://10.20.3.30/status/`.
2. Es wird eine Statusseite geöffnet. Diese Seite enthält dieselben Informationen wie die Statuskonsole.

Statuskonsoleninformationen

Statuskonsole über VGA-/Tastatur-/Mausport oder SSH

Nachdem Sie "status" an der Anmeldeaufforderung eingegeben haben, wird die schreibgeschützte Statuskonsole angezeigt.



In diesem Fenster werden Informationen dynamisch angezeigt, damit Sie den Zustand Ihres Systems bestimmen und prüfen können, ob CC-SG und die Unterkomponenten funktionieren. Die Informationen auf diesem Bildschirm werden ca. alle fünf Sekunden aktualisiert.

Die Statuskonsole enthält vier Hauptbereiche:

- CC-SG-Name, Datum und Uhrzeit
- Tipp des Tages
- System-, Server- und Netzwerkstatus
- Navigationstastenerinnerung

CC-SG-Name, Datum und Uhrzeit

Der CC-SG-Name ändert sich nicht, so dass Benutzer wissen, dass sie mit einer CC-SG-Einheit verbunden sind.

Die Datums- und Zeitangabe oben im Fenster stellt den Zeitpunkt dar, an dem die CC-SG-Daten das letzte Mal abgerufen wurden. Das Datum und die Uhrzeit stimmen mit den auf dem CC-SG-Server gespeicherten Zeitwerten überein.

Tipp des Tages

Das Feld "Tipp des Tages" (MOTD) zeigt die ersten fünf Zeilen des MOTD an, die auf dem CC-SG-Administrations-Client eingegeben wurden. Jede Zeile enthält maximal 78 Zeichen. Spezielle Formatierungen werden nicht unterstützt.

System-, Server- und Netzwerkstatus

Dieser Bereich des Bildschirms enthält Informationen zum Status der verschiedenen CC-SG-Komponenten. In der folgenden Tabelle werden die Informationen und Status für CC-SG und die CC-SG-Datenbank beschrieben:

Informationen	Beschreibung	
Hostname	Vollständiger Name der Domäne (FQDN) des CC-SG. Er enthält sowohl den Hostnamen des Geräts sowie den dazugehörigen Domänennamen.	
CC-SG-Version	Die aktuelle Firmwareversion des CC-SG. Sie beseht aus einem 5-Tupel-Wert.	
Seriennummer des CC-SG	Die Seriennummer des CC-SG.	
Modell	Modelltyp des CC-SG.	
Host-ID	Eine Nummer für die Lizenzierung der CC-SG-Einheit.	
CC-SG-Status	Der Status des CC-SG-Servers, der die meisten Benutzeranforderungen verarbeitet. Die verfügbaren Status lauten wie folgt:	
	Verfügbar	CC-SG ist verfügbar und kann Benutzeranforderungen akzeptieren.
	Nicht verfügbar	CC-SG wird möglicherweise gestoppt oder wird neu gestartet. Hält der Status "Nicht verfügbar" an, versuchen Sie, CC-SG neu zu starten.
	Restarting (Neu starten)	CC-SG wird neu gestartet.
DB-Status	Der CC-SG-Server verwendet eine interne Datenbank (DB) für seine Operationen. Diese Datenbank muss verfügbar sein und auf Anfragen reagieren, damit CC-SG funktioniert. Die verfügbaren Status lauten wie folgt:	
	Responding (Antwortet)	Die CC-SG-Datenbank ist verfügbar.
	Verfügbar	Einige Datenbankroutinen werden ausgeführt, aber lokale Anforderungen werden nicht beantwortet.
	Restoring (Wiederherstell	CC-SG stellt sich gerade wieder selbst her, und die Datenbankabfragen werden

Informationen	Beschreibung	
	ung läuft)	vorübergehend ausgesetzt.
	Nicht verfügbar	Der Datenbankserver wurde noch nicht gestartet.
Webstatus	Die meisten Zugriffe auf den CC-SG-Server erfolgen über das Web. Dieses Feld zeigt den Status des Webservers an. Die verfügbaren Status lauten wie folgt:	
	Responding/Unsecured (Antwortet/Nicht sicher)	Der Webserver ist verfügbar und beantwortet (nicht sichere) http-Anforderungen.
	Responding/Secured (Antwortet/Sicher)	Der Webserver ist verfügbar und beantwortet (sichere) https-Anforderungen.
	Verfügbar	Einige Webserverprozesse werden ausgeführt, aber lokale Anforderungen werden nicht beantwortet.
	Nicht verfügbar	Der Webserver ist zurzeit nicht verfügbar.
RAID-Status	CC-SG speichert seine Daten auf zwei gespiegelten Datenträgern (RAID-1). Die verfügbaren Status für RAID-Datenträger lauten:	
	Aktiv	RAID ist vollständig funktional.
	Degraded (Herabgestuft)	Bei mindestens einem Datenträgerlaufwerk treten Probleme auf. Wenden Sie sich an den technischen Support von Raritan.
Clusterstatus	CC-SG kann zusammen mit einem anderen CC-SG verwendet werden, um einen Cluster zu bilden. Siehe ***CC-SG-Cluster konfigurieren*** (auf Seite 304). Wenn "Eigenständig" angezeigt wird, ist CC-SG nicht in einer Clusterkonfiguration enthalten. Andernfalls wird der Status des Clusters angezeigt.	
Cluster-Peer	Wenn CC-SG in einer Clusterkonfiguration enthalten ist, wird die IP-Adresse der anderen CC-SG-Einheit im Cluster angezeigt.	
Netzwerkinformationen	Für jede Netzwerkschnittstelle steht eine Tabelle mit Bildlauf zur Verfügung, welche die entsprechenden Informationen enthält.	
	Dev	Der interne Name der Schnittstelle.
	Link	Der Status der Verbindungsintegrität, d. h., ob dieser Port über ein intaktes Kabel mit einem funktionierenden Ethernet-Switch-Port verbunden ist.
	Automatisch	Gibt an, ob die automatische Aushandlung für diesen Port verwendet wird.

Informationen	Beschreibung	
	Speed	Die Geschwindigkeit dieser Schnittstelle: 10, 100 oder 1000 Mbit/s.
	Duplex	Gibt an, ob die Schnittstelle Voll- der Halbduplex verwendet.
	IPAddr	Die aktuelle Ipv4-Adresse dieser Schnittstelle.
	RX -Pkts	Die Anzahl der auf dieser Schnittstelle empfangenen IP-Pakete, seit dem CC-SG gestartet wurde.
	TX -Pkts	Die Anzahl der auf diese Schnittstelle übertragenen IP-Pakete, seit dem CC-SG gestartet wurde.

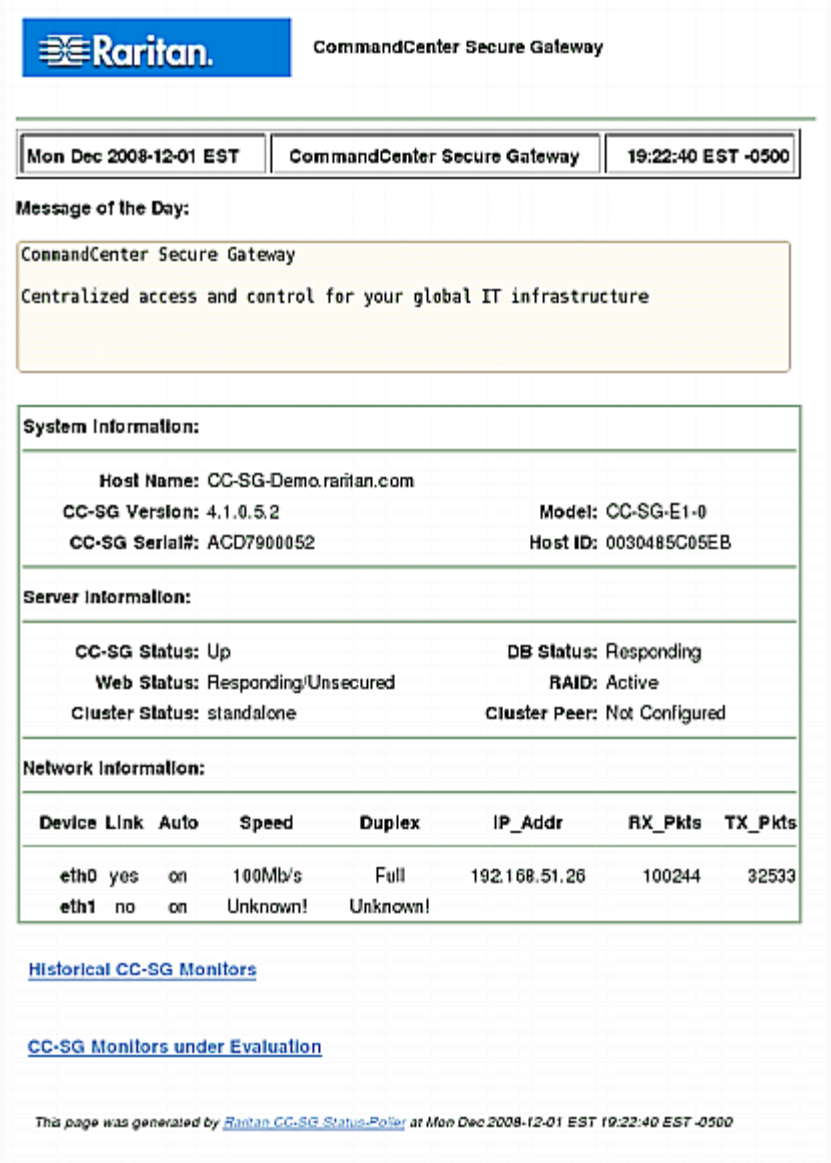
Navigationstastenerinnerung

Die untere Zeile auf dem Bildschirm zeigt die Tastenkombinationstasten für das Aufrufen der Hilfe und das Beenden der Statuskonsole an. Die Statuskonsole reagiert nur auf die folgenden Tasteneingaben.

- Drücken Sie F1, um den Hilfebildschirm aufzurufen. Dieser Bildschirm zeigt die verfügbaren Optionen und die Version der Diagnosekonsole an.
- Drücken Sie Strg+L, um den aktuellen Bildschirm zu löschen und die Informationen zu aktualisieren. Sie können den Bildschirm höchstens einmal pro Sekunde aktualisieren.
- Drücken Sie Strg+Q oder Strg+C, um die Statuskonsole zu beenden.
- Drücken Sie die Pfeiltasten, um den Bildlauf des Netzwerkinformationsbildschirms horizontal und vertikal auszuführen, wenn die Daten für den Bildschirm zu lang sind.

Statuskonsole über den Webbrowser

Nachdem Sie über den Webbrowser eine Verbindung zur Statuskonsole hergestellt haben, wird die schreibgeschützte Statuskonsole-Webseite angezeigt.



Die Webseite zeigt dieselben Informationen wie die Statuskonsole an und aktualisiert die Informationen ebenfalls ca. alle fünf Sekunden. Weitere Informationen zu den Links für CC-SG-Monitore unten auf der Webseite finden Sie unter ***Berichte zu Historical Data Trending (Trendermittlung für Datenhistorie) anzeigen*** (auf Seite 386) und ***CC-SG-Laufwerksüberwachung*** (auf Seite 441).

Administratorkonsole

Die Administratorkonsole

Über die Administratorkonsole können Sie Anfangsparameter festlegen, Erstkonfigurationen für das Netzwerk bereitstellen, Protokolldateien debuggen, einige eingeschränkte Diagnosefunktionen ausführen und CC-SG neu starten.

Die Standard-Anmeldeinformationen für die Administratorkonsole sind:

- Benutzername: admin
- Kennwort: raritan

Wichtig: Das Konto "admin" der Diagnosekonsole unterscheidet sich von dem Konto "admin" und Kennwort des CC-Superusers, die für den Java-basierten CC-SG-Administrations-Client und HTML-basierten Zugriffs-Client verwendet werden. Wenn Sie ein Kennwort ändern, wird das andere davon nicht betroffen.

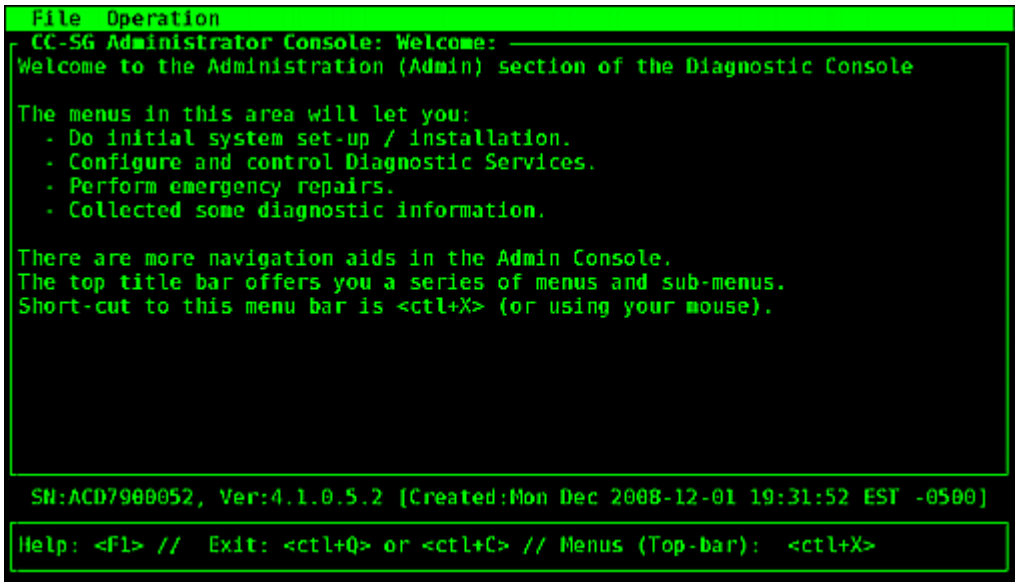
Auf die Administratorkonsole zugreifen

Die Informationen, die in der Administratorkonsole angezeigt werden, sind statisch. Werden Konfigurationsänderungen über den Administrations-Client von CC-SG oder die Diagnosekonsole vorgenommen, müssen Sie sich bei der Administratorkonsole erneut anmelden, nachdem die Änderungen übernommen wurden, um sie in der Administratorkonsole anzuzeigen.

So greifen Sie auf die Administratorkonsole zu:

1. Geben Sie beim Anmeldebildschirm "admin" ein.
2. Geben Sie Ihr CC-SG-Kennwort ein. Das Standardkennwort lautet "raritan". Nach der ersten Anmeldung läuft dieses Kennwort ab, und Sie müssen ein neues festlegen. Geben Sie dieses Kennwort ein, und geben Sie bei Aufforderung ein neues Kennwort ein. Weitere Informationen zur Bestimmung der Kennwortstärke finden Sie unter ***Kennworteinstellungen der Diagnosekonsole*** (auf Seite 381).

Der Hauptbildschirm der Administratorkonsole wird angezeigt.



Bildschirm der Administratorkonsole

Der Bildschirm der Administratorkonsole enthält vier Hauptbereiche.

- **Menüleiste:**

  Wenn Sie die Menüleiste aktivieren, können Sie die Funktionen der Administratorkonsole ausführen. Drücken Sie Strg+X, um die Menüleiste zu aktivieren, oder klicken Sie mit der Maus auf eine Menüoption, wenn Sie über den SSH-Client auf die Administratorkonsole zugreifen.

  Das Dateimenü enthält eine alternative Option, um die Diagnosekonsole zu beenden. Das Menü "Vorgang" enthält vier Menübefehle mit mindestens einem Untermenü. Informationen zu jedem Menübefehl und Untermenü finden Sie in den Abschnitten zur Administratorkonsole.

- **Hauptfensterbereich:**

  Der Inhalt hängt vom ausgewählten Vorgang ab.

- **Statusleiste:**

  Die Statusleiste befindet sich direkt über der Navigationstastenleiste. Sie enthält wichtige Systeminformationen, einschließlich die Seriennummer und Firmwareversion des CC-SG sowie die Uhrzeit, wann die im Hauptfensterbereich angezeigten Informationen geladen oder aktualisiert wurden. Screenshots dieser Informationen sind hilfreich, wenn Sie dem technischen Support von Raritan mögliche Probleme melden.

- **Navigationstastenleiste**:

  Siehe ***Die Administratorkonsole navigieren*** (auf Seite 363).

Die Administratorkonsole navigieren

Sie navigieren mit Tastenkombinationen in der Administratorkonsole. In einigen Sitzungen können Sie auch mit der Maus navigieren. Gegebenenfalls funktioniert die Maus jedoch nicht bei allen SSH-Clients oder bei der KVM-Konsole.

TASTENKOMBINATION	BESCHREIBUNG:
Strg+X	Aktiviert die Menüleiste. Wählen Sie die Menübefehle aus dem Menü aus, um verschiedene Funktionen der Administratorkonsole auszuführen.
F1	Aufrufen des Hilfebildschirms. Dieser Bildschirm zeigt die verfügbaren Optionen und die Version der Diagnosekonsole an.
Strg+C oder Strg+Q	Beenden der Diagnosekonsole.
Strg+L	Löschen des Bildschirms und erneutes Anzeigen der Informationen (die Informationen werden jedoch nicht aktualisiert).
Tabulatortaste	Wechseln zur nächsten verfügbaren Option.
Leertaste	Auswählen der aktuellen Option.
Eingabetaste	Auswählen der aktuellen Option.
Pfeiltaste	Bewegen zu anderen Feldern innerhalb einer Option.

Konfiguration der Diagnosekonsole bearbeiten

Die Diagnosekonsole kann über den seriellen Port (COM1), den KVM-Port oder über SSH-Clients aufgerufen werden. Wenn Sie auf die Statuskonsole zugreifen möchten, können Sie auch den Webzugriff verwenden.

Sie können für jeden Porttyp konfigurieren, ob Benutzer sich über "status" oder "admin" anmelden können und ob Field Support über den Port auf die Diagnosekonsole zugreifen kann. Bei SSH-Clients können Sie konfigurieren, welche Portnummer verwendet werden sollte. Dies ist jedoch nur möglich, falls kein anderer CC-SG-Dienst den gewünschten Port verwendet. Wenn Sie über das Web auf die Statuskonsole zugreifen, können Sie ein Konto angeben, das sich von anderen Konten im System unterscheidet, um den Zugriff einzuschränken. Andernfalls kann jeder Benutzer, der über das Web auf CC-SG zugreift, die Statuskonsole-Webseite öffnen.

Wichtig: Stellen Sie sicher, dass Sie nicht den Admin- oder Field Support-Zugriff sperren.

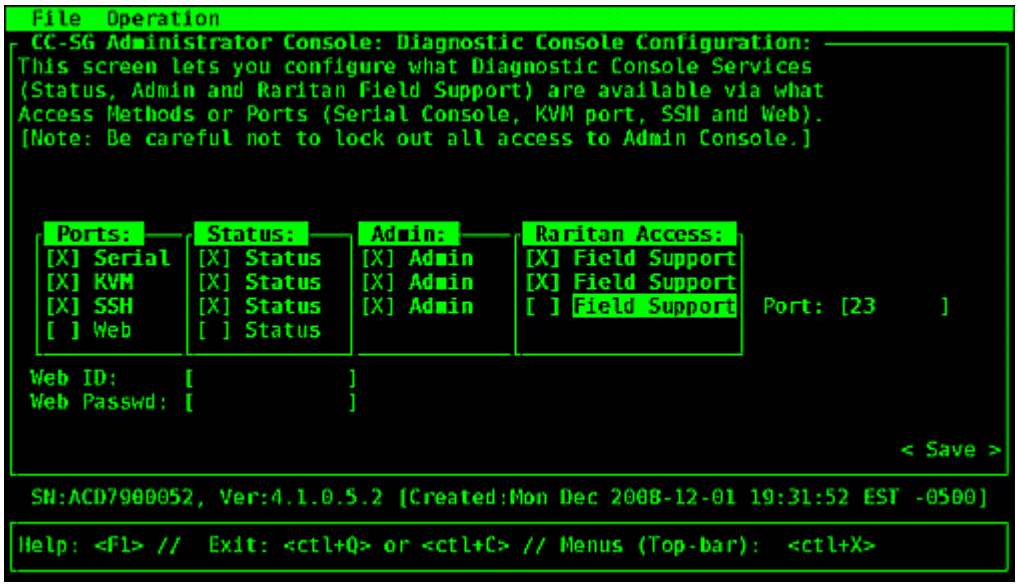
So bearbeiten Sie die Konfiguration der Diagnosekonsole:

1. Wählen Sie "Operation > Diagnostic Console Config".
2. Bestimmen Sie, wie die Diagnosekonsole konfiguriert und auf die Diagnosekonsole zugegriffen werden soll.

   Es stehen vier Zugriffsmethoden für die Diagnosekonsole zur Verfügung: Serieller Port (COM1), KVM-Konsole, SSH (IP-Netzwerk) und Web. Die Diagnosekonsole bietet drei Dienste: Status-Anzeige, Administratorkonsole, Raritan Field Support. In diesem Fenster können Sie auswählen, welche Dienste über die verschiedenen Zugriffsmethoden zur Verfügung stehen.

   Wenn die Optionen für Web und Status aktiviert sind, ist die Statuskonsole-Webseite immer verfügbar, solange der Webserver verfügbar und betriebsbereit ist. Um den Zugriff auf die Statuskonsole-Webseite einzuschränken, geben Sie ein Konto und ein Kennwort ein.
3. Geben Sie die Portnummer für den SSH-Zugriff auf die Diagnosekonsole in das Feld Port ein. Der Standardport lautet 23.

4. Klicken Sie auf Speichern.



Netzwerkschnittstellenkonfiguration bearbeiten (Network Interfaces)

Über die Netzwerkschnittstellenkonfiguration können Sie Erstkonfigurationsaufgaben wie die Einstellung des Hostnamens und der IP-Adresse von CC-SG durchführen.

1. Wählen Sie "Operation > Network Interfaces > Network Interface Config".
2. Wurden die Netzwerkschnittstellen bereits konfiguriert, wird ein Warnhinweis angezeigt, dass Sie den Administrations-Client von CC-SG zur Konfiguration der Schnittstellen verwenden sollten. Klicken Sie zum Fortfahren auf YES.
3. Geben Sie Ihren Hostnamen im Feld Host Name ein. Nach dem Speichern wird das Feld aktualisiert, um den vollständig qualifizierten Domänennamen (Fully-Qualified Domain Name, FQDN), falls bekannt, anzuzeigen. Die Regeln zur Vergabe von Hostnamen werden unter ***Terminologie/Abkürzungen*** (auf Seite 2) beschrieben.
4. Wählen Sie im Modusfeld entweder "IP Isolation" (IP-Isolation) oder "IP Failover" (IP-Ausfallsicherung) aus. Siehe ***Netzwerkeinrichtung* (auf Seite 288).**
5. Wählen Sie im Konfigurationsfeld entweder DHCP oder Static aus.

- Wenn Sie "DHCP" auswählen und Ihr DHCP-Server richtig konfiguriert ist, werden die DNS-Informationen, das Domänensuffix, die IP-Adresse, das Standardgateway und die Subnetzmaske automatisch ausgefüllt, nachdem Sie "Speichern" ausgewählt und die Administratorkonsole verlassen und erneut aufgerufen haben.
- Wenn Sie Static ausgewählt haben, geben Sie Werte für IP Address (erforderlich), Netmask (erforderlich), Default Gateway (optional), Primary DNS (optional) und Secondary DNS (optional) sowie den Domänennamen in Domain Suffix (optional) ein.
- Auch wenn die IP-Konfiguration einer Schnittstelle durch DHCP bestimmt wird, müssen die richtig formatierten Werte für "IP-Adresse" und "Netzmaske" bereitgestellt werden.

6. Wählen Sie über "Adaptergeschwindigkeit" eine Geschwindigkeit aus. Die Werte 10, 100 und 1000 MBit/s werden in einer Liste aufgeführt (in der nur ein Wert gleichzeitig angezeigt wird). Verwenden Sie die Pfeiltasten, um die Werte anzuzeigen. Drücken Sie die Leertaste, um die angezeigte Option auszuwählen. Für Geschwindigkeiten von 1 GB wählen Sie "AUTO".
7. Wenn Sie die Option "AUTO" nicht für "Adaptergeschwindigkeit" ausgewählt haben, klicken Sie auf "Adapter Duplex", und verwenden Sie die Pfeiltasten, um einen Duplexmodus (Voll- oder Halbduplex) in der Liste auszuwählen (falls vorhanden). Sie können den Duplexmodus jederzeit auswählen. Er gilt jedoch nur, wenn Adapter Speed nicht auf AUTO festgelegt ist.
8. Wiederholen Sie diese Schritte für die zweite Netzwerkschnittstelle, wenn der IP-Isolationsmodus aktiviert ist.
9. Klicken Sie auf Speichern. CC-SG wird erneut gestartet und meldet alle Benutzer der grafischen Benutzeroberfläche von CC-SG ab und beendet ihre Sitzungen. Ein Warnhinweis wird angezeigt, der auf die bevorstehende Netzwerkkonfiguration und die damit verbundenen Auswirkungen auf CC-SG-Benutzer hinweist. Wählen Sie zum Fortfahren <YES>.

   Der Systemstatus kann über ein Statusfenster der Diagnosekonsole überwacht werden. Am KVM-Port können Sie eine andere Terminalsitzung auswählen, indem Sie Alt+F2 drücken und sich mit "status" anmelden. Zeigen Sie die ursprüngliche Terminalsitzung wieder an, indem Sie Alt+F1 drücken. Sechs verfügbare Terminalsitzungen stehen über F1 bis F6 bereit.

IP-Adresse anpingen

Prüfen Sie mit der Ping-Funktion, ob alle Verbindungen zwischen Ihrem CC-SG-Computer und einer bestimmten IP-Adresse richtig funktionieren.

Hinweis: Einige Sites sperren Ping-Anfragen ausdrücklich. Stellen Sie sicher, dass das Zielnetzwerk und das dazwischenliegende Netzwerk Ping-Anfragen zulassen, wenn ein Ping-Versuch fehlschlägt.

1. Wählen Sie "Operation > Network Interfaces > Ping".
2. Geben Sie die IP-Adresse oder den Hostnamen (falls DNS richtig auf CC-SG konfiguriert ist) des Ziels in das Feld Ping Target ein.
3. Wählen Sie: **Optional.**

Option	Beschreibung
Show other received ICMP packets	Verbose-Ausgabe, die alle empfangenen ICMP-Pakete zusätzlich zu den ECHO_RESPONSE-Paketen aufführt. Tritt selten auf.
No DNS Resolution	Löst Adressen nicht in Hostnamen auf.
Record Route	Zeichnet die Route auf. Aktiviert die Option zur Aufzeichnung der IP-Route, durch die die Route des Pakets im IP-Header gespeichert wird.
Use Broadcast Address	Ermöglicht das Anpingen einer Broadcastnachricht.
Adaptive Timing	Anpassbares anpingen. Das Interpacket-Intervall passt sich an die Round-Trip-Zeit an, sodass sich effektiv nicht mehr als eine unbeantwortete Anfrage im Netzwerk befindet. Das Mindestintervall beträgt 200 ms.

4. Sie können Werte dafür eingeben, wie viele Sekunden der Ping-Befehl ausgeführt wird, wie viele Ping-Anfragen gesendet werden sowie die Größe der Ping-Pakete. Der Standardwert lautet 56, was 64 ICMP-Datenbyte in Verbindung mit 8 Byte ICMP-Headerdaten entspricht. Werden die Felder nicht ausgefüllt, werden die Standardwerte verwendet. **Optional.**
5. Klicken Sie auf "Ping". Wird als Ergebnis eine Reihe von Antworten angezeigt, funktioniert die Verbindung. Die Zeitangabe gibt an, wie schnell die Verbindung ist. Wenn statt einer Antwort der Fehler "timed out" angezeigt wird, ist die Verbindung zwischen Ihrem Computer und der Domäne unterbrochen. Weitere Informationen finden Sie unter ***Static Routes bearbeiten*** (auf Seite 369).
6. Drücken Sie Strg+C, um die Sitzung zu beenden.

Hinweis: Sie können die statistische Zusammenfassung der Sitzung mit Strg+Q anzeigen und das Ziel weiterhin anpingen.

Traceroute verwenden

Traceroute wird häufig zur Problembehandlung in Netzwerken verwendet. Indem Sie die Liste der Router anzeigen, die verwendet wurden, können Sie den Pfad von Ihrem Computer zu einem bestimmten Ziel im Netzwerk bestimmen. Aufgeführt werden alle Router, die das Paket weiterleiten, bis es am Ziel angekommen ist oder nicht am Ziel ankommt und fallen gelassen wird. Außerdem können Sie anzeigen, wie viel Zeit jede Teilstrecke von Router zu Router beansprucht hat. Sie können dadurch Routing-Probleme oder Firewalls kennzeichnen, die den Zugriff auf eine Site sperren.

So führen Sie traceroute für eine IP-Adresse oder einen Hostnamen durch:

1. Wählen Sie "Operation > Network Interfaces > Traceroute".
2. Geben Sie die IP-Adresse oder den Hostnamen des Ziels, das Sie prüfen möchten, im Feld "Traceroute Target" ein.
3. Wählen Sie: **Optional.**

Option	Beschreibung
Verbose	Verbose-Ausgabe, die alle empfangenen ICMP-Pakete außer TIME_EXCEEDED und UNREACHABLE aufführt.
No DNS Resolution	Löst Adressen nicht in Hostnamen auf.
Use ICMP (vs. normal UDP)	ICMP ECHO- anstelle von UDP-Datagrammen verwenden.

4. Geben Sie Werte dafür ein, wie viele Teilstrecken der Befehl "traceroute" bei ausgehenden Prüfpaketen verwendet (der Standardwert lautet 30), wie viele Teilstrecken der UDP-Zielport für Prüfpakete verwendet (der Standardwert lautet 33434) und wie groß die Traceroute-Pakete sein sollen. Werden die Felder nicht ausgefüllt, werden die Standardwerte verwendet. **Optional.**
5. Klicken Sie unten rechts im Fenster auf "Traceroute".
6. Drücken Sie Strg+C oder Strg+Q, um die Traceroute-Sitzung zu beenden. Eine Eingabeaufforderung "Return?" wird angezeigt. Drücken Sie die Eingabetaste, um zum Traceroute-Menü zu wechseln. Die Eingabeaufforderung Return? wird auch angezeigt, wenn Traceroute beendet wird, sobald die Ereignisse „destination reached“ oder „hop count exceeded“ eintreten.

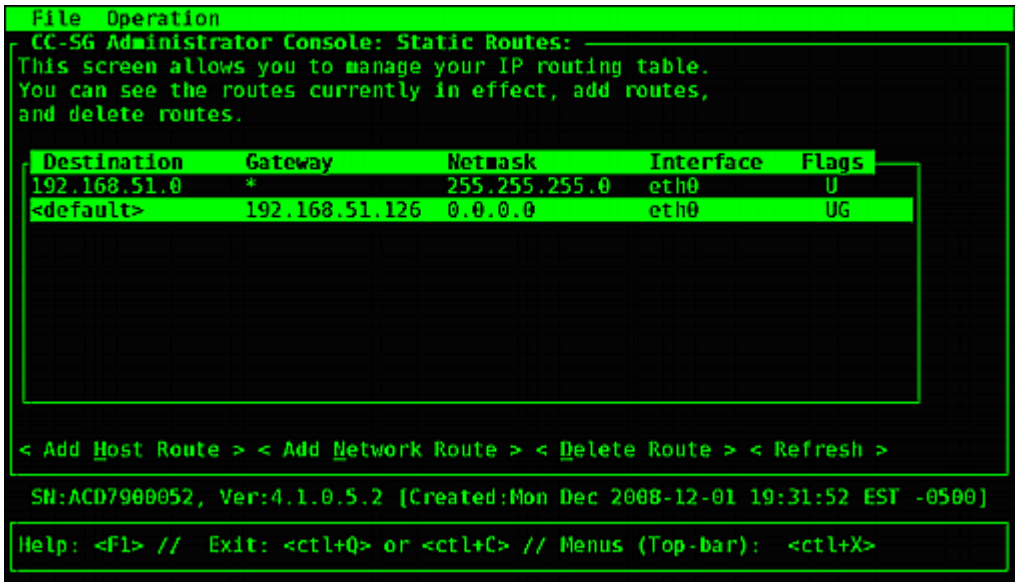
Static Routes bearbeiten

In Static Routes können Sie die aktuelle IP-Routing-Tabelle anzeigen und Routen bearbeiten, hinzufügen oder löschen. Die sorgfältige Verwendung und Platzierung statischer Routen kann die Leistung Ihres Netzwerks verbessern. Dabei sparen Sie Bandbreite für wichtige Geschäftsanwendungen. Klicken Sie mit der Maus, oder verwenden Sie die Tabulator- und Pfeiltasten zum Navigieren, und drücken Sie zum Auswählen eines Werts die Eingabetaste.

So zeigen Sie eine statisch Route an oder bearbeiten sie:

1. Wählen Sie "Operation > Network Interfaces > Static Routes".
2. Die Seite mit der aktuellen IP-Routingtabelle wird geöffnet. Sie können eine zugewiesene IP-Route zur Routingtabelle hinzufügen, indem Sie "Add Host Route" (Hostroute hinzufügen) oder "Add Network Route" (Netzwerkroute hinzufügen) auswählen. Die in der Routingtabelle vorhandenen Elemente können ausgewählt werden. Sie können auch eine Route aus der Tabelle löschen, indem Sie "Delete Route" (Route löschen) auswählen. Mithilfe der Schaltfläche "Aktualisieren" aktualisieren Sie die Routinginformationen in der Tabelle.
   - "Add Host Route" (Hostroute hinzufügen) verwendet eine Zielhost-IP-Adresse und eine Gateway-IP-Adresse und/oder einen Schnittstellennamen, die bzw. der in der Statuskonsole angezeigt wird.
   - "Add Network Route" (Netzwerkroute hinzufügen) ist ähnlich, verwendet jedoch ein Zielnetzwerk und eine Netzmaske.
   - Für jedes in der Tabelle ausgewählte oder markierte Element können Sie "Delete Route" (Route löschen) auswählen, um die Route zu löschen. Die einzige Ausnahme bildet die Route, die dem aktuellen Host und der aktuellen Schnittstelle zugewiesen ist, der bzw. die in CC-SG nicht gelöscht werden darf.

Obwohl Sie alle anderen Routes löschen können, einschließlich dem Standardgateway, wirkt sich das Löschen erheblich auf die Kommunikation mit CC-SG aus.



Protokolldateien in der Diagnosekonsole anzeigen

Sie können eine oder mehrere Protokolldateien in LogViewer anzeigen sowie mehrere Dateien gleichzeitig durchsuchen, um die Systemaktivität zu untersuchen.

Die Liste der Protokolldateien wird nur aktualisiert, wenn die verknüpfte Liste aktiviert wird. Dies tritt ein, wenn ein Benutzer beispielsweise in den Listenbereich der Protokolldateien wechselt oder eine neue Sortieroption ausgewählt wird. Es wird entweder ein Zeitstempel vor den Dateinamen angezeigt, um zu kennzeichnen, wann neue Daten für die Protokolldatei eingegangen sind, oder die Größe der Protokolldatei angezeigt.

Abkürzungen für Zeitstempel und Dateigröße:

Zeitstempel:

- s = Sekunden
- m = Minuten
- h = Stunden
- d = Tage

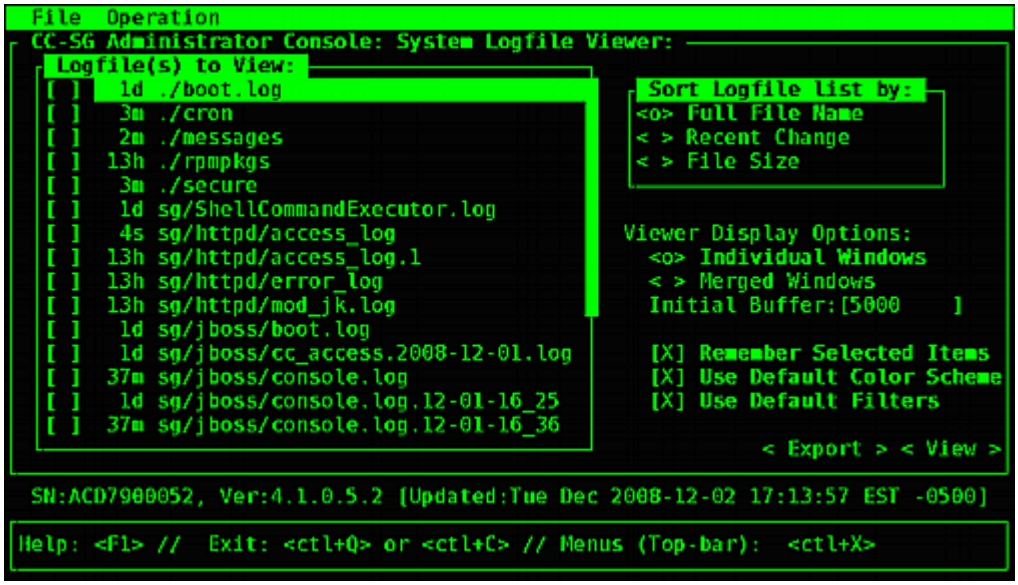
Dateigrößen:

- B = Byte
- K = Kilobyte (1.000 Byte)
- M = Megabyte (1.000.000 Byte)
- G = Gigabyte (1.000.000.000 Byte)

So zeigen Sie Protokolldateien an:

1. Wählen Sie "Operation > Admin > System Logfile Viewer".
2. Der Logviewer-Bildschirm ist in vier Hauptbereiche aufgeteilt.
   - Liste der Protokolldateien, die zurzeit im System verfügbar sind. Ist die Liste länger als das Anzeigefenster, können Sie mithilfe der Pfeiltasten durch die Liste blättern.
   - Sortierkriterien für Listen mit Protokolldateien. Protokolldateien können nach dem Dateinamen, dem letzten Änderungsdatum oder der Größe der Protokolldatei sortiert werden.
   - Viewer-Anzeigeoptionen.
   - Export-/Anzeigeoption.

3. Klicken Sie mit der Maus oder verwenden Sie die Pfeiltasten zum Navigieren und drücken Sie die Leertaste, um eine Protokolldatei auszuwählen und mit einem X zu kennzeichnen. Sie können mehrere Protokolldateien gleichzeitig anzeigen.



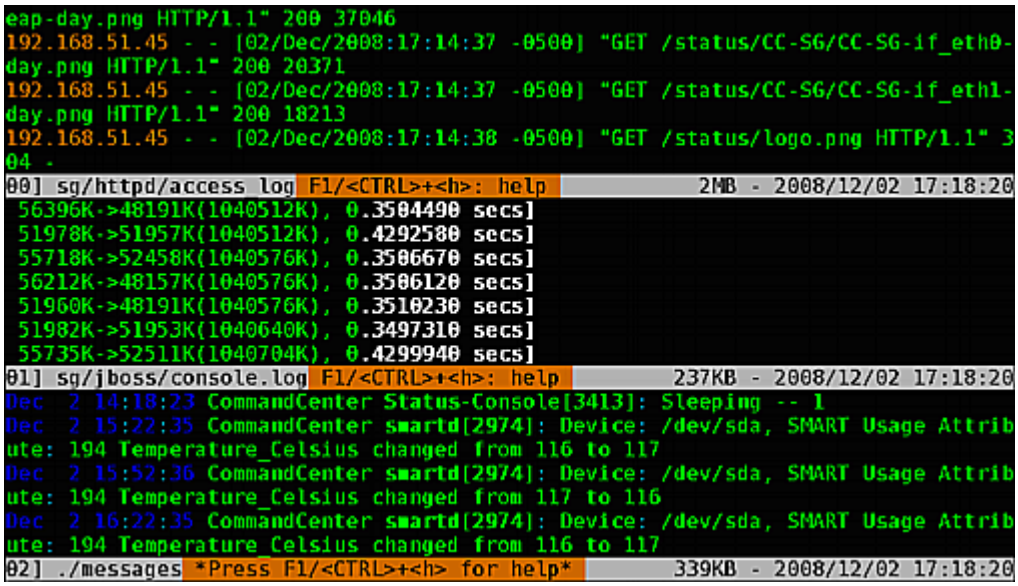
So sortieren Sie die Liste Logfiles to View:

Mit den Optionen unter "Sort Logfile list by" bestimmen Sie die Reihenfolge, in der Protokolldateien in der Liste "Logfile to View" angezeigt werden.

Option	Beschreibung
Individual Windows	Zeigt die ausgewählten Protokolle in einzelnen Unterfenstern an.
Merged Windows	Zeigt die ausgewählten Protokolle in einem Fenster an.
Initial Buffer	Legt die anfängliche Puffer- oder Verlaufsgröße fest. Der Standardwert beträgt 5000. Das System ist so konfiguriert, dass alle neuen Informationen zwischengespeichert werden.
Remember Selected Items	Ist dieses Feld markiert, wird die aktuelle Auswahl der Protokolldateien (falls vorhanden) gespeichert. Andernfalls wird die Auswahl zurückgesetzt, sobald eine neue Liste mit Protokolldateien erzeugt wird. Diese Option ist hilfreich, wenn Sie Dateien schrittweise bearbeiten möchten.
Use Default Color Scheme	Ist dieses Feld markiert, werden einige Protokolldateien mit einem standardmäßigen Farbschema angezeigt. Hinweis: Multitail-Befehle können verwendet werden, um das Farbschema zu ändern, nachdem die Protokolldateien angezeigt wurden.

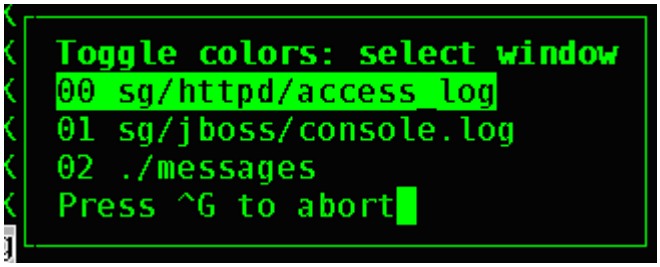
Option	Beschreibung
Use Default Filters	Ist dieses Feld markiert, werden auf bestimmte Protokolldateien automatisch Filter angewendet.
Export	Diese Option fasst alle ausgewählten Protokolldateien in einem Paket zusammen und stellt sie über Webzugriff zur Verfügung, damit sie abgerufen und an den technischen Support von Raritan weitergeleitet werden können. Der Zugriff auf den Inhalt dieses Pakets steht Kunden nicht zur Verfügung. Exportierte Protokolldateien stehen bis zu 10 Tage zur Verfügung, bevor sie automatisch vom System gelöscht werden.
Ansicht	Anzeigen der ausgewählten Protokolle.

Wird View mit der Option Individual Windows ausgewählt, zeigt LogViewer Folgendes an:



- Drücken Sie beim Anzeigen von Protokolldateien Q, Strg+Q oder Strg+C, um zum vorherigen Bildschirm zu wechseln.

- Sie können die Farben in einer Protokolldatei ändern, um wichtige Daten hervorzuheben. Geben Sie C ein, um die Farben einer Protokolldatei zu ändern, und wählen Sie ein Protokoll in der Liste aus.

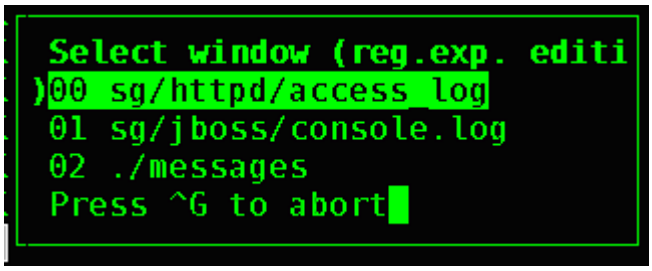


- Geben Sie I zur Anzeige von Systeminformationen ein.

Hinweis: Die Systemauslastung ist zu Beginn der Administratorkonsole-Sitzung statisch. Verwenden Sie das TOP-Dienstprogramm, um die Systemressourcen dynamisch zu überwachen.

So filtern Sie eine Protokolldatei mit einem regulären Ausdruck:

1. Geben Sie e ein, um einen regulären Ausdruck hinzuzufügen oder zu bearbeiten, und wählen Sie eine Protokolldatei in der Liste aus, falls Sie mehrere anzeigen.



2. Geben Sie A ein, um einen regulären Ausdruck hinzuzufügen. Wenn Sie beispielsweise Informationen zur WARN-Nachricht in der Protokolldatei sg/jboss/console.log anzeigen möchten, geben Sie "WARN" ein, und wählen Sie "match" aus.

Hinweis: Dieser Bildschirm zeigt auch das Default Filter Scheme für console.log an, das die meisten Java-Heap-Nachrichten entfernt.

CC-SG mit der Diagnosekonsole neu starten

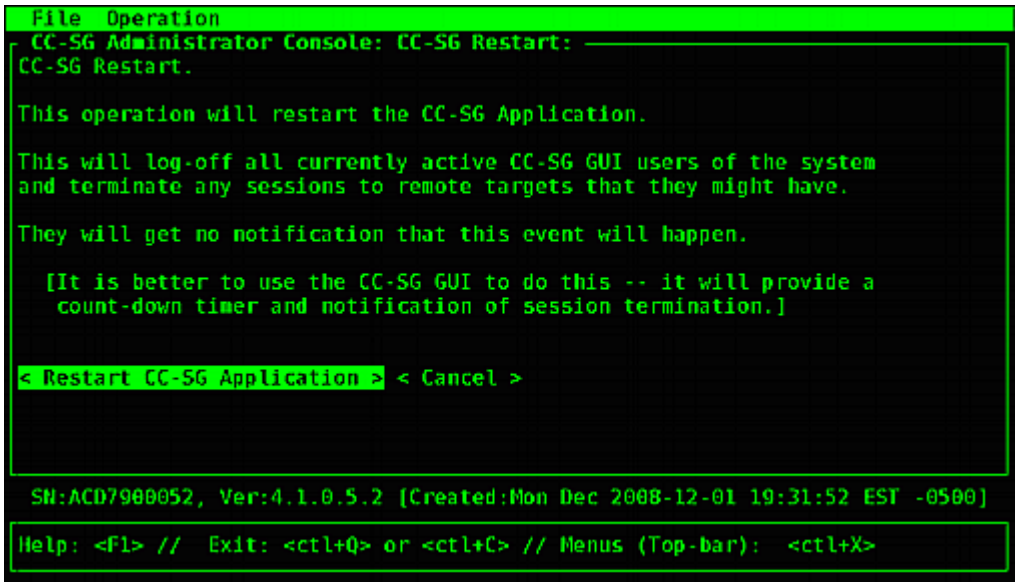
Wenn Sie CC-SG neu starten, werden alle aktuellen CC-SG-Benutzer abgemeldet und die Sitzungen mit Remotezielservern beendet.

Wichtig: Es wird DRINGEND empfohlen, CC-SG auf dem Administrations-Client neu zu starten, wenn es nicht absolut notwendig ist, den Neustart in der Diagnosekonsole auszuführen. Weitere Informationen finden Sie unter *CC-SG neu starten* (auf Seite 272). Beim Neustarten von CC-SG in der Diagnosekonsole werden die Benutzer der grafischen Benutzeroberfläche über den Neustart NICHT informiert.

So starten Sie CC-SG mit der Diagnosekonsole neu:

1. Wählen Sie "Operation > Admin > CC-SG Restart".

2. Klicken Sie auf "Restart CC-SG Application", oder drücken Sie die Eingabetaste. Bestätigen Sie den Neustart im nächsten Bildschirm.



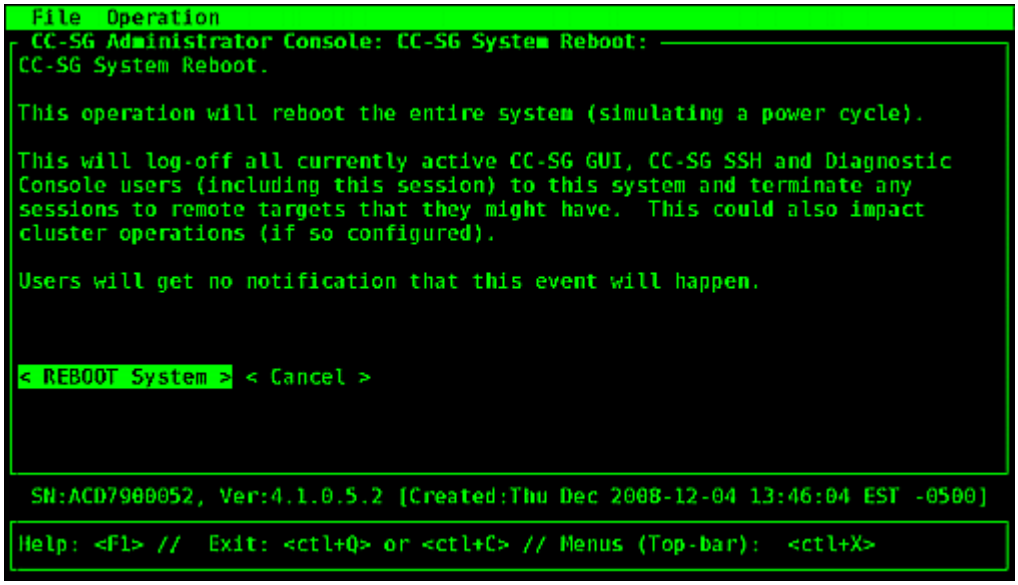
CC-SG mit der Diagnosekonsole neu hochfahren

Mit dieser Option wird das gesamte CC-SG neu hochgefahren. Dies entspricht dem Aus- und erneutem Einschalten. Benutzer erhalten keine Benachrichtigung. Benutzer von CC-SG, SSH und der Diagnosekonsole (einschließlich dieser Sitzung) werden abgemeldet. Alle Verbindungen zu Remotezielservern werden getrennt.

So fahren Sie CC-SG neu hoch:

1. Wählen Sie "Operation > Admin > CC-SG System Reboot".

2. Klicken Sie auf "REBOOT System", oder drücken Sie die Eingabetaste, um CC-SG neu hochzufahren. Bestätigen Sie das Hochfahren im nächsten Bildschirm.



CC-SG-System über die Diagnosekonsole ausschalten

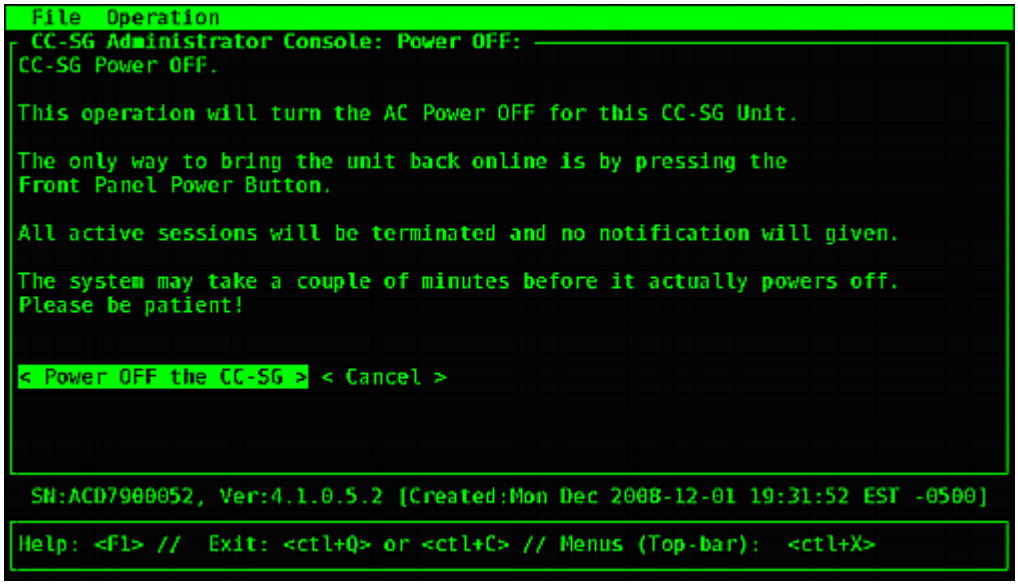
Mit dieser Option schalten Sie die CC-SG-Einheit aus. Angemeldete Benutzer erhalten keine Benachrichtigung. Benutzer von CC-SG, SSH und der Diagnosekonsole (einschließlich dieser Sitzung) werden abgemeldet. Alle Verbindungen zu Remotezielservern werden getrennt.

Sie können die CC-SG-Einheit nur wieder einschalten, indem Sie die Power-Taste vorne am Gerät betätigen.

So schalten Sie CC-SG aus:

1. Wählen Sie "Operation > Admin > CC-SG System Power OFF".

2. Klicken Sie entweder auf "Power OFF the CC-SG" oder drücken Sie die Eingabetaste, um den Strom an der CC-SG-Einheit abzuschalten. Bestätigen Sie das Ausschalten im nächsten Bildschirm.



Kennwort des CC-Superusers mit der Diagnosekonsole zurücksetzen

Mit dieser Option setzen Sie das Kennwort für das CC-Superuser-Konto auf den werkseitigen Standardwert zurück.

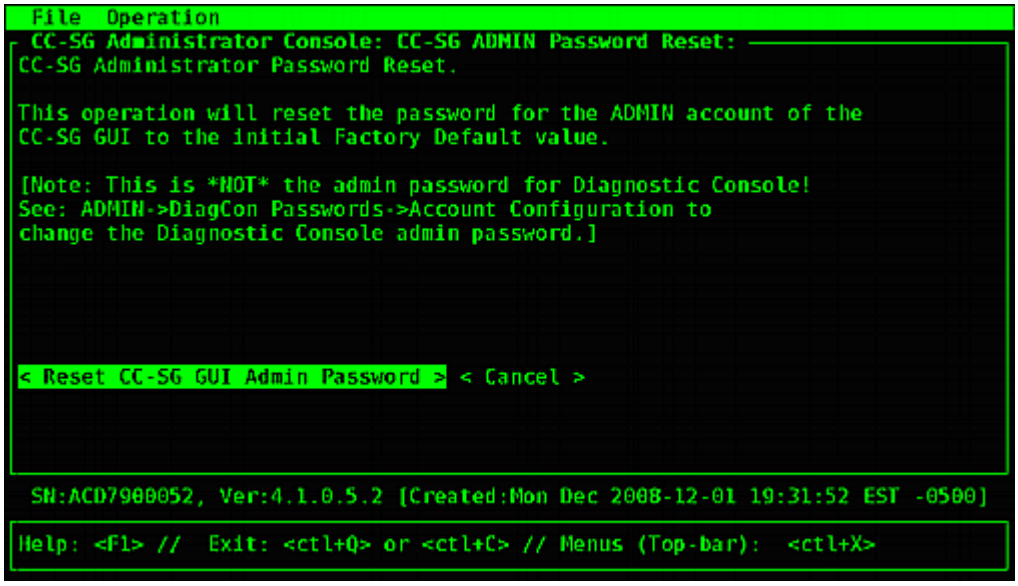
Werkseitiges Standardkennwort: raritan

Hinweis: Dies ist nicht das Kennwort für den Benutzer admin der Diagnosekonsole. Weitere Informationen finden Sie unter **Kennworteinstellungen der Diagnosekonsole** *(auf Seite 381).*

▶ So setzen Sie das admin Kennwort der grafischen Benutzeroberfläche von CC-SG zurück:

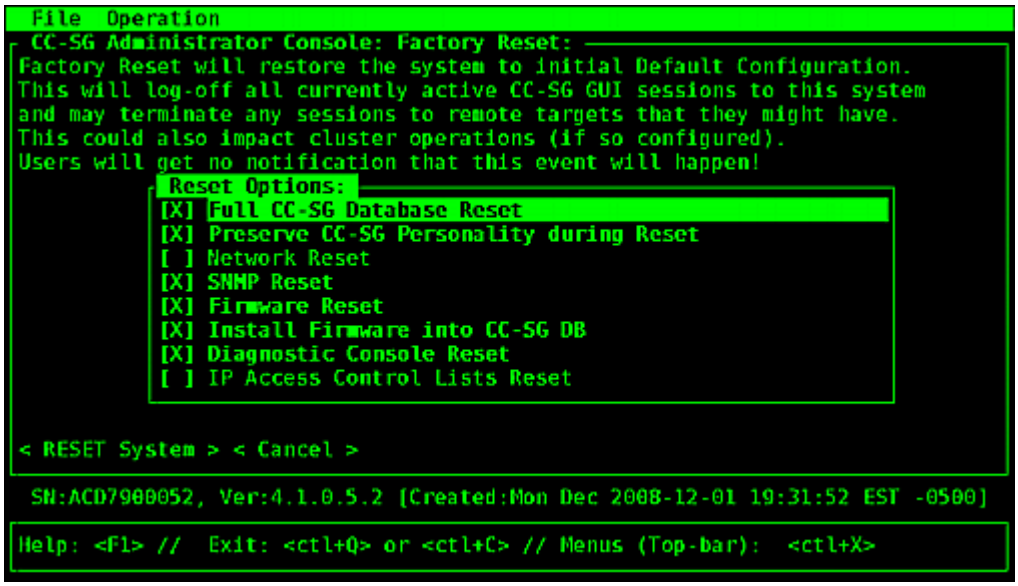
1. Wählen Sie Operation > Admin > CC-SG ADMIN Password Reset.

2. Klicken Sie auf "Reset CC-SG GUI Admin Password", oder drücken Sie die Eingabetaste, um das admin Kennwort auf die werkseitige Standardeinstellung zurückzusetzen. Bestätigen Sie das Zurücksetzen im nächsten Bildschirm.



Werksseitig eingestellte Konfiguration von CC-SG wiederherstellen

Durch diese Option wird das gesamte CC-SG-System oder Teile davon auf die werkseitig eingestellten Standardwerte zurückgesetzt. Alle aktiven CC-SG-Benutzer werden ohne Benachrichtigung abgemeldet, und die SNMP-Verarbeitung wird unterbrochen.



Es wird empfohlen, die ausgewählten Standardoptionen zu verwenden.

Option	Beschreibung
Full CC-SG Database Reset	Diese Option entfernt die vorhandene CC-SG-Datenbank und erstellt eine neue Version mit den werkseitigen Standardwerten. Netzwerkeinstellungen, SNMP-Einstellungen, Firmware und Diagnosekonsole-Einstellungen sind nicht Teil der CC-SG-Datenbank. Die IP-ACL-Einstellungen werden mit einer vollständigen Datenbankzurücksetzung zurückgesetzt, unabhängig davon, ob Sie die Option "IP-ACL-Tabellen" auswählen oder nicht. Die Konfiguration der Netzwerkumgebung wird beim Zurücksetzen gelöscht, d. h. die CC-SG-Einheit "weiß" nicht mehr, ob es ein Mitglied der Netzwerkumgebung war oder nicht.
Preserve CC-SG Personality during Reset	Diese Option wird aktiviert, wenn Sie "Full CC-SG Database Reset" auswählen. Bei der Neuerstellung der CC-SG-Datenbank werden einige zuvor konfigurierte Optionen gespeichert. ▪ Sichere Kommunikation zwischen PC-Clients und CC-SG ▪ Erzwingt sichere Kennwörter ▪ Direkte und Proxy-Verbindungen zu Out-of-Band-Knoten ▪ Leerlaufzeitgeber-Einstellung
Network Reset	Diese Option setzt die Netzwerkeinstellungen auf die werkseitigen Standardwerte zurück. ▪ Hostname: CommandCenter ▪ Domänenname: localdomain ▪ Modus: IP-Ausfallsicherung ▪ Konfiguration: Statisch ▪ IP-Address (IP-Adresse): 192.168.0.192 ▪ Netzmaske: 255.255.255.0 ▪ Gateway: keiner ▪ Primärer DNS-Server: keiner ▪ Sekundärer DNS-Server: keiner ▪ Adaptergeschwindigkeit: Automatisch
SNMP Reset	Diese Option setzt die SNMP-Einstellungen auf die werkseitigen Standardwerte zurück. ▪ Port: 161 ▪ Community mit Lesezugriff: public ▪ Community mit Lese/Schreibzugriff: private ▪ Systemkontakt, -name, -standort: keiner

Option	Beschreibung
	▪ SNMP-Trap-Konfiguration ▪ SNMP-Trap-Ziele
Firmware Reset	Diese Option setzt alle Geräte-Firmeware-Dateien auf die werkseitigen Standardwerte zurück. Diese Option ändert die CC-SG-Datenbank nicht.
Install Firmware into CC-SG DB	Diese Option lädt die Firmware-Dateien für die aktuelle CC-SG-Version in die CC-SG-Datenbank.
Diagnostic Console Reset	Diese Option stellt die Einstellungen für die Diagnosekonsolen mit den werkseitigen Standardwerten wieder her.
IP Access Control Lists Reset	Diese Option entfernt alle Einträge aus der IP-ACL-Tabelle. Die IP-ACL-Einstellungen werden mit einer vollständigen Datenbankzurücksetzung zurückgesetzt, unabhängig davon, ob Sie die Option "IP Access Control Lists reset" auswählen oder nicht. Weitere Informationen finden Sie unter ***Zugriffssteuerungsliste*** (auf Seite 327).

So setzen Sie CC-SG auf die werkseitige Konfiguration zurück:

1. Wählen Sie "Operation > Admin > Factory Reset".
2. Wählen Sie die Rücksetzungsoptionen.
3. Klicken Sie auf "Reset System".
4. Auf dem Bildschirm wird eine Warnung und eine Fortschrittleiste angezeigt. Die Fortschrittleiste gibt den aktuellen Status des Zurücksetzens an. Sie können CC-SG erst wieder verwenden, wenn das Zurücksetzen abgeschlossen ist.

Während des Zurücksetzens darf CC-SG NICHT ausgeschaltet, aus- und wiedereingeschaltet oder unterbrochen werden. Andernfalls kann es beim CC-SG zu Datenverlust kommen.

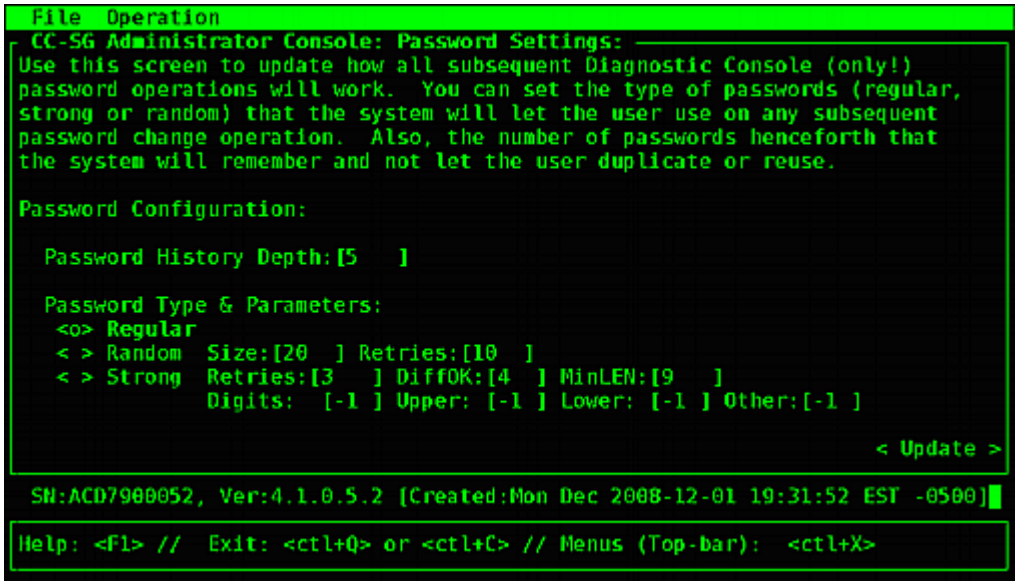
Kennworteinstellungen der Diagnosekonsole

Mit dieser Option können Sie die Sicherheitsstärke von Kennwörtern (status und admin) sowie Kennwortattribute konfigurieren. Dazu gehören die Höchstanzahl an Tagen, die verstreichen müssen, bevor das Kennwort geändert werden muss. Führen Sie diese Aufgaben über das Menü "Account Configuration" durch. Die Optionen dieser Menüs beziehen sich nur auf Konten (status und admin) und Kennwörter der Diagnosekonsole. Sie haben keine Auswirkungen auf normale CC-SG-Konten oder -Kennwörter der Benutzeroberfläche.

So konfigurieren Sie Kennwörter für die Diagnosekonsole:

1. Wählen Sie "Operation > Admin > DiagCon Passwords > Password Configuration".

2. Geben Sie in das Feld Länge der Kennwortchronik die Anzahl an Kennwörtern ein, die gespeichert werden sollen. Die Standardeinstellung ist fünf.



3. Wählen Sie Regular, Random oder Strong für die Kennwörter für admin und status (falls aktiviert) aus.

Kennworteinstellung	Beschreibung
Regular	Dies ist der Standardwert. Kennwörter müssen länger als vier Zeichen mit wenigen Einschränkungen sein. Dies ist die standardmäßige Kennwortkonfiguration des Systems.
Random	Bietet zufällig erzeugte Kennwörter. Konfigurieren Sie die maximale Kennwortgröße size in Bits (Mindestwert 14, Höchstwert 70 und Standardwert 20) und die Anzahl der Wiederholungen retries (Standardwert 10), d. h. wie oft Sie gefragt werden, ob Sie das neue Kennwort übernehmen möchten. Sie können entweder annehmen (indem Sie das neue Kennwort zweimal eingeben) oder das zufällige Kennwort ablehnen. Sie können kein eigenes Kennwort auswählen.
Strong	Erzwingt sichere Kennwörter. Retries ist die Anzahl an Versuchen, die Sie haben, bis eine Fehlermeldung ausgegeben wird. DiffOK ist die Anzahl der Zeichen, die in dem neuen Kennwort im Vergleich zum alten Kennwort gleich sein darf. MinLEN ist die Mindestzeichenlänge, die für das Kennwort erforderlich ist. Legen Sie die Werte für Digits (Zahlen), Upper (Großbuchstaben), Lower (Kleinbuchstaben) und Other (Sonderzeichen) fest, die für das Kennwort erforderlich sind. Positive Zahlen geben die Höchstanzahl von „credit“ dieser

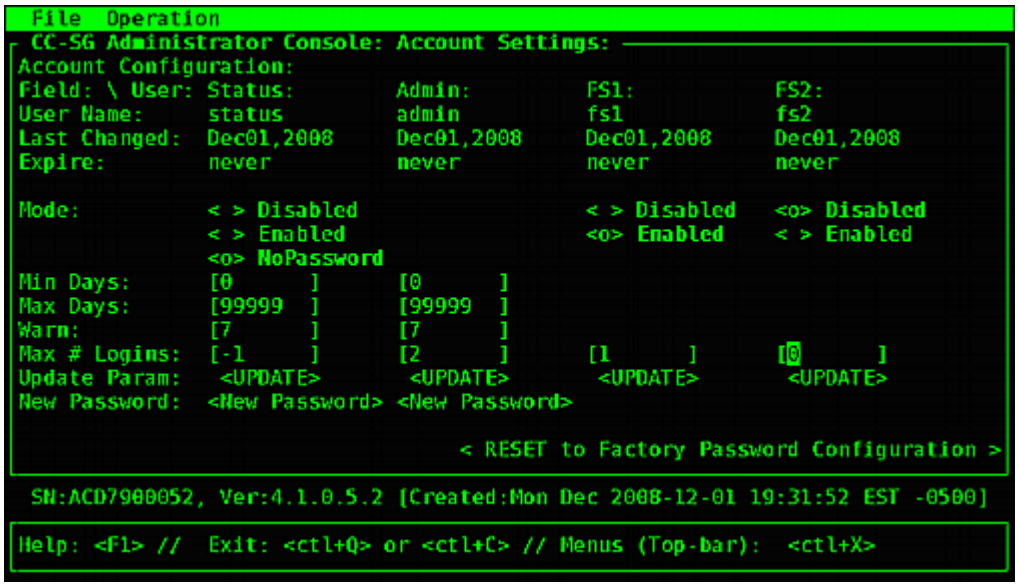
Kennworteinstellung	Beschreibung
	Zeichenklasse an, der für die „simplicity“-Zählung gesammelt werden kann. Negative Zahlen geben an, dass das Kennwort mindestens so viele Zeichen der angegebenen Klasse enthalten muss. Der Wert -1 bedeutet also, dass jedes Kennwort mindestens eine Zahl enthalten muss.

Konfiguration des Diagnosekonsolen-Kontos

Standardmäßig erfordert das Konto status kein Kennwort, Sie können hier jedoch ein Kennwort konfigurieren. Andere Aspekte des admin-Kennworts können konfiguriert werden, und die Field Support-Konten können aktiviert oder deaktiviert werden.

So konfigurieren Sie Konten:

1. Wählen Sie "Operation > Admin > DiagCon Passwords > Account Configuration".
2. Im angezeigten Bildschirm können Sie die Einstellungen für jedes Konto anzeigen: Status, Admin, FS1 und FS2.



Dieses Fenster ist in drei Hauptbereiche eingeteilt:

- Oben werden die Informationen mit Leseberechtigung zu den Konten im System angezeigt.

- Im mittleren Bereich werden die verschiedenen Parameter angezeigt, die sich auf jede ID beziehen und dafür relevant sind. Außerdem wird eine Reihe Schaltflächen bereitgestellt, damit die Parameter aktualisiert oder neue Kennwörter für die Konten bereitgestellt werden können.
- Im unteren Bereich wird die Kennwortkonfiguration auf den Auslieferungszustand zurückgesetzt.

3. Wenn ein Kennwort für das Status-Konto erforderlich sein soll, wählen Sie darunter die Option Enabled aus.
4. Für die Konten Admin und Status können Sie Folgendes konfigurieren:

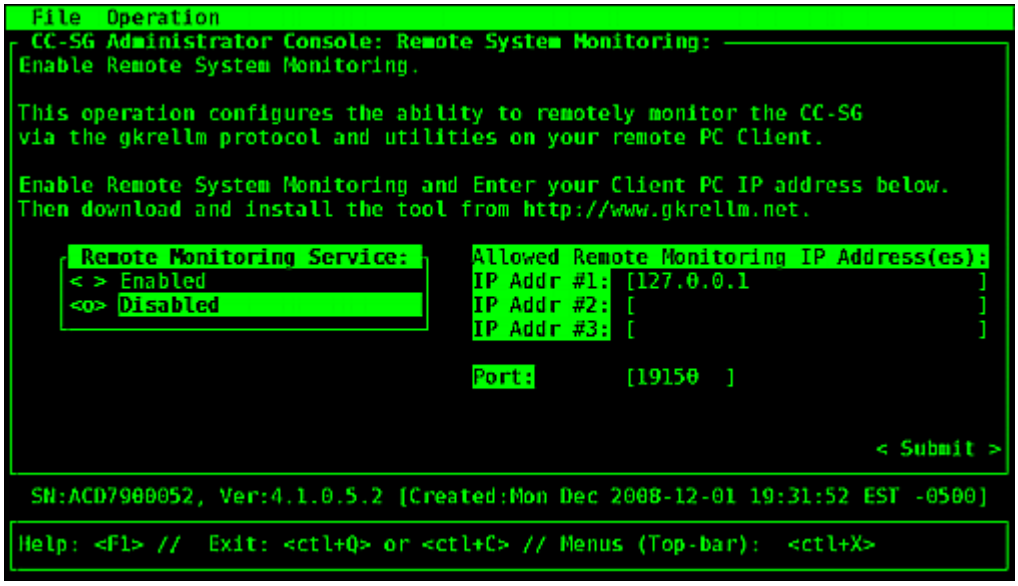
Einstellung	Beschreibung
User \ User Name	(Lesezugriff) Der aktuelle Benutzername oder die Benutzer-ID für dieses Konto.
Last Changed	(Lesezugriff) Das Datum, an dem das Kennwort für dieses Konto zuletzt geändert wurde.
Expire	(Lesezugriff) Dies ist das Datum, an dem das Kennwort für dieses Konto geändert werden muss.
Mode	Eine konfigurierbare Option, wenn das Konto deaktiviert (Anmeldung nicht zulässig) oder aktiviert (Token zur Authentifizierung erforderlich) oder der Zugriff erlaubt und kein Kennwort erforderlich ist. (Sperren Sie nicht beide Admin- und FS1-Konten gleichzeitig, da Sie sonst die Diagnosekonsole nicht verwenden können.)
Min Days	Die Mindestanzahl an Tagen nach einer Kennwortänderung, nach denen das Kennwort erneut geändert werden kann. Der Standardwert ist 0.
Max Days	Die Höchstanzahl an Tagen, die das Kennwort gültig ist. Der Standardwert ist 99999.
Warning	Die Anzahl an Tagen, die Warnhinweise ausgegeben werden, bevor das Kennwort ungültig wird.
Max # of Logins	Die Höchstanzahl an gleichzeitigen Anmeldungen, die für das Konto zulässig ist. Negative Zahlen bedeuten keine Einschränkungen (-1 ist der Standardwert für die Anmeldung mit status). 0 bedeutet, dass sich niemand anmelden kann. Eine positive Zahl legt die Anzahl an Benutzern fest, die gleichzeitig angemeldet sein können (2 ist der Standardwert für die Anmeldung mit "admin").
UPDATE	Vorgenommene Änderungen für diese ID werden gespeichert.
New Password	Geben Sie ein neues Kennwort für das Konto ein.

Überwachung des Remotesystems konfigurieren

Sie können von der Funktion für die Überwachung des Remotesystems das Tool GKrellM verwenden lassen. Das Tool GKrellM bietet eine grafische Ansicht der Ressourcennutzung der CC-SG-Einheit. Das Tool ähnelt der Registerkarte "Systemleistung" des Windows Task Managers.

1: Aktivieren Sie Überwachung des Remotesystems für das CC-SG-Gerät:

1. Wählen Sie "Operation > Utilities > Remote System Monitoring".



2. Aktivieren Sie "Enabled" im Feld "Remote Monitoring Service".
3. Geben Sie im Feld "Allowed Remote Monitoring IP Addresses" die IP-Adresse des Client-PCs ein, den das CC-SG-Gerät überwachen soll. Sie können bis zu drei IP-Adressen eingeben.
4. Der Standard-Port für das Tool GKrellM ist 19150. Sie können den Port ändern.
5. Wählen Sie "Submit" (Übertragen).

2: Laden Sie die Client-Software für die Überwachung des Remotesystems herunter:

1. Navigieren Sie zu www.gkrellm.net.
2. Laden Sie das Paket für Ihren Client-PC herunter und installieren Sie es.

3: Konfigurieren Sie den Client für die Überwachung des Remotesystems für CC-SG:

Folgen Sie den Anweisungen in der Liesmich-Datei, um das CC-SG-Gerät als zu überwachendes Ziel festzulegen.

Windows-Benutzer müssen die Befehlszeile verwenden, um das Gkrellm-Installationsverzeichnis zu suchen, und dann die in der Liesmich-Datei angegebenen Befehle ausführen.

Berichte zu Historical Data Trending (Trendermittlung für Datenhistorie) anzeigen

Die Historical Data Trending (Trendermittlung für die Datenhistorie) sammelt Informationen zu CPU-Auslastung, Speicherauslastung, Java-Heap-Kapazität und Netzwerkverkehr. Diese Informationen werden in einem Bericht zusammengefasst, den Sie aus CC-SG als Webseite anzeigen können. Der Bericht enthält den Status von CC-SG und Links zu historischen Daten.

Von den Trendermittlungsberichten für Datenhistorie werden keine Daten mehr ermittelt, wenn die Systemzeit und das Systemdatum von CC-SG auf einen früheren Zeitpunkt gesetzt werden. Die Datenermittlung wird wieder aufgenommen, wenn Datum und Uhrzeit den ursprünglichen Zeitpunkt erreichen. Wenn Datum und Uhrzeit auf einen späteren Zeitpunkt eingestellt werden, weisen die Berichte bei den Daten eine entsprechende Lücke auf.

1: Anzeige von Historical Data Trending (Trendermittlung für Datenhistorie) aktivieren:

1. Wählen Sie "Operation > Diagnostic Console Config".
2. Wählen Sie in der Liste "Ports" die Option "Web".
3. Aktivieren Sie in der Liste "Status" das Kontrollkästchen "Status" neben "Web".
4. Klicken Sie auf Speichern.

2: Berichte zu Historical Data Trending (Trendermittlung für die Datenhistorie) anzeigen:

1. Verwenden Sie einen unterstützten Internetbrowser, und geben Sie folgenden URL ein: `http(s)://<IP-Adresse>/status/`, wobei `<IP-Adresse>` für die IP-Adresse von CC-SG steht. Der Schrägstrich (/) nach "/status" ist obligatorisch. Beispiel: `https://10.20.3.30/status/`.
2. Es wird eine Statusseite geöffnet. Diese Seite enthält dieselben Informationen wie die Statuskonsole. Siehe ***Statuskonsole*** (auf Seite 354).

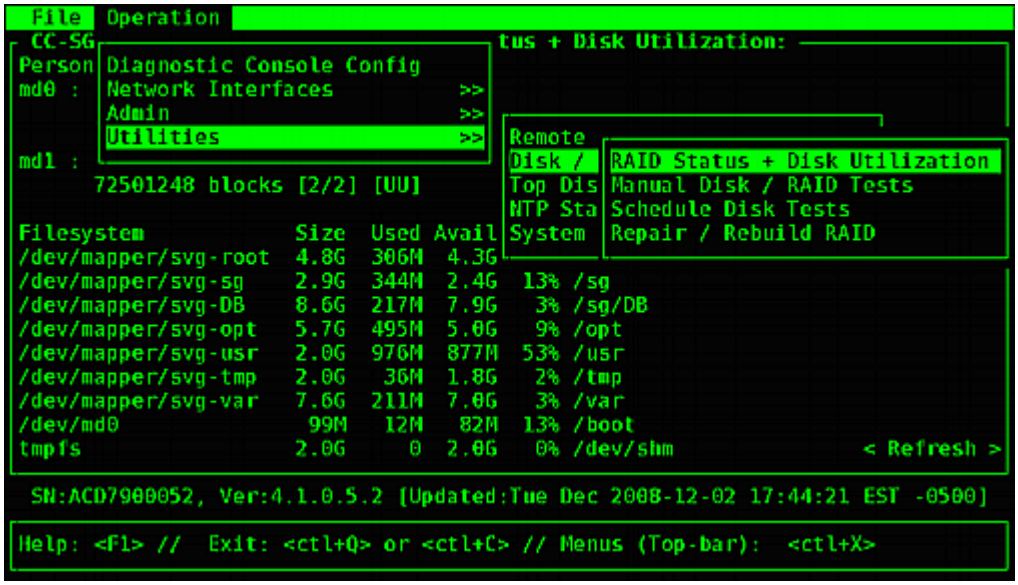
- Klicken Sie auf den Link "Historical CC-SG Monitors", um Informationen zu CPU-Auslastung, Speicherauslastung, Java-Heap-Kapazität und Netzwerkverkehr anzuzeigen. Klicken Sie auf jedes Diagramm, um Details auf einer neuen Seite anzuzeigen.

RAID-Status und Laufwerksauslastung anzeigen

Diese Option zeigt den Status der CC-SG-Festplatten an, wie Festplattengröße, ob sie aktiv und betriebsbereit sind, Status von RAID-1 sowie der von verschiedenen Dateisystemen verwendete Festplattenspeicher.

So zeigen Sie den CC-SG-Festplattenstatus an:

1. Wählen Sie "Operation (Vorgang) > Utilities (Werkzeuge) > Disk/RAID Utilities (Laufwerk/RAID-Werkzeuge) > RAID Status (RAID-Status) + Disk Utilization (Laufwerkauslastung)".



2. Klicken Sie auf "Aktualisieren", oder drücken Sie die Eingabetaste, um das Fenster zu aktualisieren. Es ist besonders hilfreich, die Anzeige beim Aktualisieren oder Installieren zu aktualisieren, um den Fortschritt der RAID-Festplatten anzuzeigen, wenn sie neu erstellt und synchronisiert werden.

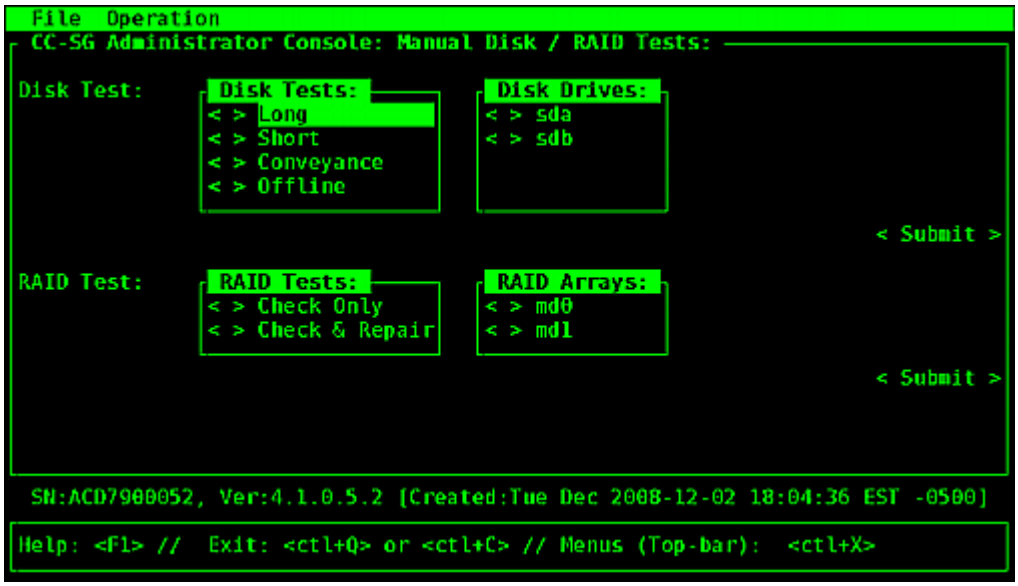
Hinweis: Die Festplattenlaufwerke werden vollständig synchronisiert, und der vollständige RAID-1-Schutz steht zur Verfügung, wenn Sie ein Fenster wie oben gezeigt sehen. Beachten Sie, dass der Status der Arrays "md0" und "md1" den Wert "[UU]" aufweist.

Laufwerk- oder RAID-Tests ausführen

Sie können SMART-Laufwerktests oder RAID-Tests manuell prüfen und Reparaturen ausführen.

So führen Sie einen Laufwerktest oder einen RAID-Test sowie eine Reparatur aus:

1. Wählen Sie "Operation (Vorgang) > Utilities (Werkzeuge) > Disk/RAID Utilities (Laufwerk/RAID-Werkzeuge) > Manual Disk/RAID Tests" (Manuelle Laufwerk-/RAID-Tests).



2. So führen Sie einen SMART-Laufwerktest aus:
   a. Wählen Sie im Bereich "Disk Test" (Laufwerktest) den Testtyp sowie das zu testende Laufwerk aus.
   b. Wählen Sie "Submit" (Übertragen).
   c. Der Test wird geplant, und der Bildschirm mit den SMART-Informationen wird angezeigt.
   d. Wenn die erforderliche Zeit wie im Bildschirm angezeigt abgelaufen ist, werden die Ergebnisse im Bildschirm "Repair/Rebuild RAID" (RAID reparieren/wiederherstellen) angezeigt. Siehe ***Repair (Reparieren) oder Rebuild (Wiederherstellen) von RAID-Laufwerken*** (auf Seite 392).
3. So führen Sie einen RAID-Test und eine Reparatur aus:
   a. Wählen Sie im Bereich "RAID Test" (RAID-Test) den Testtyp sowie den zu testenden RAID-Array aus. Der md0-Array ist eine kleine Startpartition, während md1-Array den Rest des Systems abdeckt.

b. Wählen Sie "Submit" (Übertragen).

c. Sie können den Testfortschritt im Bildschirm "RAID Status+Disk Utilization" (RAID-Status+Laufwerkauslastung) verfolgen. Siehe ***RAID-Status und Laufwerksauslastung anzeigen*** (auf Seite 387). **Optional.**

d. Nachdem der Test abgeschlossen ist, werden die Ergebnisse im Bildschirm "Repair/Rebuild RAID" (RAID reparieren/wiederherstellen) angezeigt. Siehe ***Repair (Reparieren) oder Rebuild (Wiederherstellen) von RAID-Laufwerken*** (auf Seite 392). Wenn in der Spalte "Mis-Match" (Nichtübereinstimmung) für den angegebenen Array ein Wert ungleich Null angezeigt wird, kann dies auf ein Problem hinweisen. Wenden Sie sich in diesem Fall an den technischen Support von Raritan.

Laufwerktests planen

Sie können die Ausführung SMART-basierter Tests für die Laufwerke in regelmäßigen Abständen planen. Die auf dem Laufwerk installierte Firmware führt diese Tests aus. Die Testergebnisse werden im Bildschirm "Repair/Rebuild" (Reparieren/Wiederherstellen) angezeigt. Siehe ***Repair (Reparieren) oder Rebuild (Wiederherstellen) von RAID-Laufwerken*** (auf Seite 392).

SMART-Tests können ausgeführt werden, während CC-SG betriebsbereit ist und verwendet wird. Sie wirken sich nur minimal auf die Leistung des CC-SG aus, jedoch können CC-SG-Aktivitäten die Fertigstellung der SMART-Tests erheblich verzögern. Daher ist es sinnvoll, die Tests nicht zu häufig zu planen.

Halten Sie beim Planen der SMART-Tests folgende Richtlinien ein:

- Sie können jeweils nur einen Test ausführen.
- Es kann kein anderer Test geplant werden, wenn ein Laufwerk gerade getestet wird.
- Wenn zwei Tests zur selben Zeit geplant sind, wird der längere Test ausgeführt.
- Der Test wird "innerhalb" der angegebenen Stunde ausgeführt, jedoch nicht unbedingt am Anfang der Stunde.
- Planen Sie SMART-Tests nicht für Zeiträume, in denen eine höhere Laufwerksaktivität stattfindet, wie z. B. bei hoher CC-SG-Auslastung oder bei Vakuumvorgängen, die täglich um Mitternacht und 12:00 Uhr Mittags stattfinden.

Hinweis: Standardmäßig verfügt CC-SG über einen geplanten Kurztest, der täglich um 2:00 Uhr Nachts ausgeführt wird, sowie einen geplanten Langtest, der jeden Sonntag um 3:00 Uhr Nachts ausgeführt wird. Diese geplanten Tests werden auf beiden Laufwerken ausgeführt.

So ändern Sie die Planung der Laufwerktests:

1. Wählen Sie "Operation (Vorgang) > Utilities (Werkzeuge) > Disk/RAID Utilities (Laufwerk/RAID-Werkzeuge) > Schedule Disk Tests (Laufwerktests planen)".

```
 File  Operation
 CC-SG Administrator Console: Schedule Disk Tests:

  SMART Test    | Month | Day of Month | Day of Week | Hour
   Disk sda:    | 1->12 |     1->31    |     1->7    | 0->23
 ____________________________________________________________
 [X] Long       [    ]      [    ]       [7   ]     [03  ]
 [X] Short      [    ]      [    ]       [    ]     [02  ]
 [ ] Conveyance [    ]      [    ]       [    ]     [    ]
 [ ] Offline    [    ]      [    ]       [    ]     [    ]

   Disk: sdb:
 ____________________________________________________________
 [X] Long       [    ]      [    ]       [7   ]     [03  ]
 [X] Short      [    ]      [    ]       [    ]     [02  ]
 [ ] Conveyance [    ]      [    ]       [    ]     [    ]
 [ ] Offline    [    ]      [    ]       [    ]     [    ]

                                                    < Submit >
 SN:ACD7900052, Ver:4.1.0.5.2 [Created:Tue Dec 2008-12-02 18:04:36 EST -0500]

Help: <F1> //  Exit: <ctl+Q> or <ctl+C> // Menus (Top-bar):  <ctl+X>
```

2. Klicken Sie mit der Maus, oder verwenden Sie die Pfeiltaste zum Navigieren, und drücken Sie die Leertaste, um einen Testtyp auszuwählen und mit einem X zu kennzeichnen. Die unterschiedlichen Testtypen benötigen unterschiedlich viel Zeit.
   - Ein Kurztest dauert ca. zwei Minuten, wenn das System nur wenig ausgelastet ist.
   - Ein Übertagungstest dauert ca. fünf Minuten.
   - Ein Langtest dauert ca. 50 Minuten.
   - Ein Offline-Test dauert maximal 50 Minuten.
3. Geben Sie das Datum und die Uhrzeit für die Ausführung dieses Tests an. Geben Sie jeweils eine Zahl in die Felder "Month" (Monat), "Day of Month" (Tag), "Day of the Week" (Wochentag) and "Hour" (Stunde) ein.
   - Für das Feld "Day of the Week" (Wochentag) werden die Zahlen 1 für Montag bis 7 für Sonntag verwendet.
   - Die Stunden werden im 24-Stundenformat angegeben.

   Hinweis: Ein leeres Feld verwendet alle Werte.

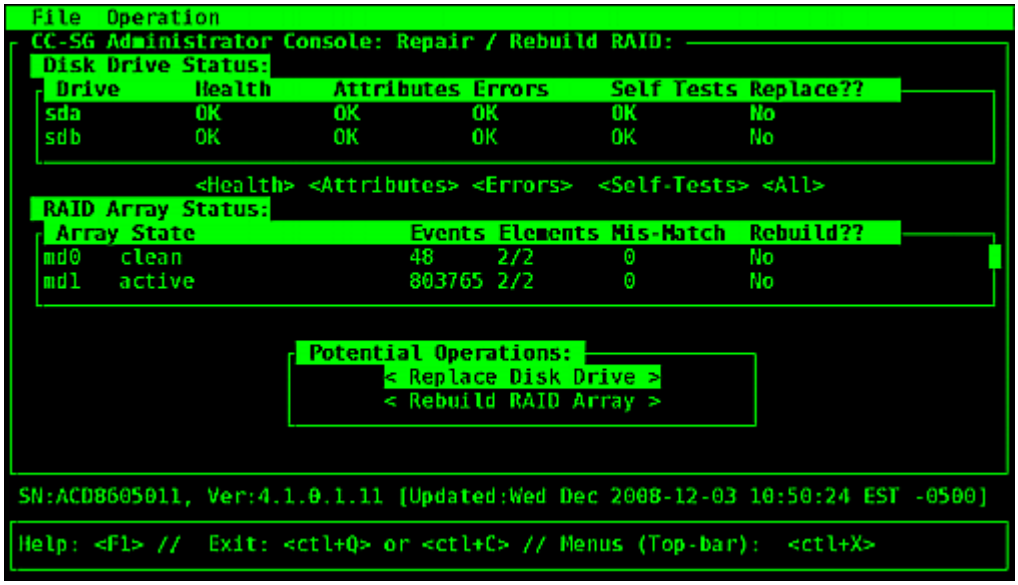
4. Wählen Sie "Submit" (Übertragen).

Repair (Reparieren) oder Rebuild (Wiederherstellen) von RAID-Laufwerken

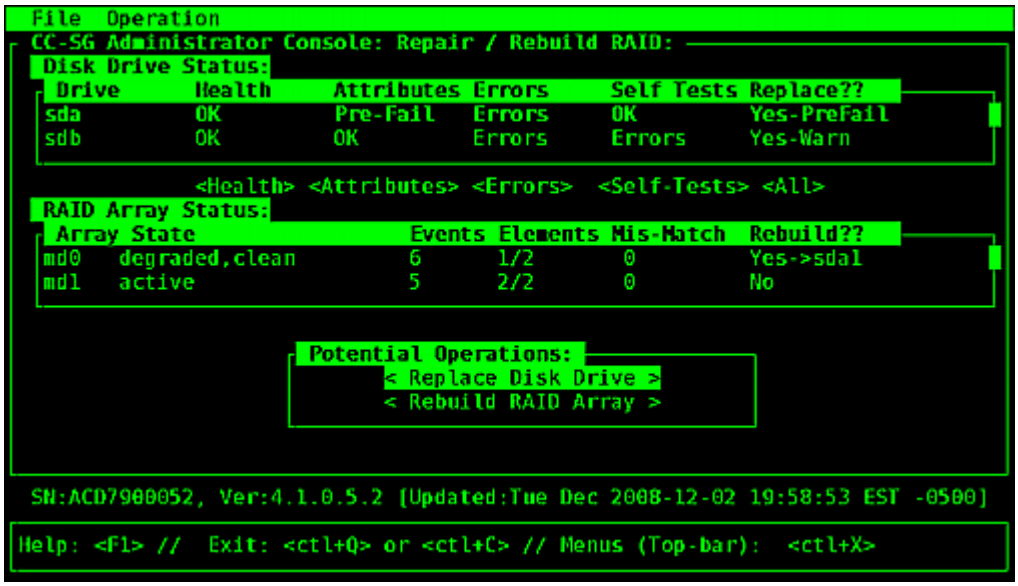
Diese Option zeigt die detaillierten Statusinformationen für Laufwerke und RAID-Arrays an und gibt an, ob Sie ein Laufwerk ersetzen oder ein RAID-1-Mirror-Array wiederherstellen sollen. Bevor Sie ein Laufwerk ersetzen oder während des Betriebs austauschen, müssen Sie ein Ersatzgerät von Raritan erwerben.

So reparieren Sie die RAID-Festplatte oder stellen sie wieder her:

1. Wählen Sie "Operation (Vorgang) > Utilities (Werkzeuge) > Disk/RAID Utilities (Laufwerk/RAID-Werkzeuge) > Repair/Rebuild RAID (RAID repaieren/wiederherstellen)".
2. Wenn für ein Element in der Spalte "Replace??" (Ersetzen??)oder "Rebuild??" (Wiederherstellen??) der Hinweis "No" (Nein) nicht angezeigt wird. kontaktieren Sie den technischen Support von Raritan.
   - Ein gutes System:



- Ein zusammengestelltes System mit mehreren Problemen:



Das System aktualisiert die angezeigten Informationen, wenn Sie mithilfe der Tab-Taste oder der Maus zwischen den Feldern "Disk Drive Status" (Laufwerkstatus), "RAID Array Status" (RAID-Array-Status) und "Potential Operations" (Potentieller Vorgang) wechseln.

3. Sie können im Bereich "Disk Drive Status" (Laufwerkstatus) jede Schaltfläche unter der Tabelle auswählen, um detaillierte SMART-Informationen anzuzeigen. **Optional.**
4. Wählen Sie entweder "Replace Disk Drive" (Laufwerk ersetzen) oder "Rebuild RAID Array" (RAID-Array wiederherstellen), und folgen Sie den Anweisungen auf dem Bildschirm, bis der Vorgang abgeschlossen ist.

Top Display mit der Diagnosekonsole anzeigen

Mit Top Display können Sie die Prozessliste und die Attribute, die zurzeit ausgeführt werden, sowie den allgemeinen Systemzustand anzeigen.

So zeigen Sie die Prozesse an, die unter CC-SG ausgeführt werden:

1. Wählen Sie "Operation (Vorgang) > Utilities (Werkzeuge) > Top Display (Gesamtübersicht anzeigen)".

2. Zeigen Sie die Gesamtanzahl der Prozesse an, die ausgeführt werden, ruhen oder gestoppt wurden.

```
top - 20:46:55 up 1 day,  9:25,  8 users,  load average: 0.27, 0.32, 0.28
Tasks: 149 total,   1 running, 148 sleeping,   0 stopped,   0 zombie
Cpu(s):  0.2%us,  0.3%sy,  0.0%ni, 99.5%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Mem:   4152196k total,  1646716k used,  2505480k free,   608628k buffers
Swap:  2031608k total,        0k used,  2031608k free,   565668k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
19043 sg        25   0 1343m 272m  10m S    0  6.7   2:02.46 java
    1 root      15   0  2060  580  504 S    0  0.0   0:00.91 init
    2 root      RT  -5     0    0    0 S    0  0.0   0:00.64 migration/0
    3 root      34  19     0    0    0 S    0  0.0   0:00.22 ksoftirqd/0
    4 root      RT  -5     0    0    0 S    0  0.0   0:00.00 watchdog/0
    5 root      RT  -5     0    0    0 S    0  0.0   0:49.48 migration/1
    6 root      34  19     0    0    0 S    0  0.0   0:00.27 ksoftirqd/1
    7 root      RT  -5     0    0    0 S    0  0.0   0:00.00 watchdog/1
    8 root      10  -5     0    0    0 S    0  0.0   0:00.84 events/0
    9 root      10  -5     0    0    0 S    0  0.0   0:00.21 events/1
   10 root      10  -5     0    0    0 S    0  0.0   0:03.04 khelper
   11 root      10  -5     0    0    0 S    0  0.0   0:00.00 kthread
   15 root      10  -5     0    0    0 S    0  0.0   0:00.10 kblockd/0
   16 root      10  -5     0    0    0 S    0  0.0   0:00.00 kblockd/1
   17 root      15  -5     0    0    0 S    0  0.0   0:00.00 kacpid
  170 root      15  -5     0    0    0 S    0  0.0   0:00.00 cqueue/0
  171 root      15  -5     0    0    0 S    0  0.0   0:00.00 cqueue/1
```

3. Geben Sie `h` ein, um eine Hilfeseite für den Befehl top (Gesamtübersicht) anzuzeigen. Die Hilfetaste F1 funktioniert in diesem Fall nicht.

NTP-Status anzeigen

Sie können den Status des NTP-Zeitdaemons anzeigen, falls dieser konfiguriert wurde und unter CC-SG ausgeführt wird. Der NTP-Daemon kann nur über die grafische Benutzeroberfläche des CC-SG-Administrations-Client konfiguriert werden.

So zeigen Sie den Status des NTP-Daemons in CC-SG an:

1. Wählen Sie "Operation (Vorgang) > Utilities (Werkzeuge) > NTP Status Display (NTP-Statusanzeige)".

- NTP ist nicht aktiviert oder ordnungsgemäß konfiguriert:

```
 File  Operation
 CC-SG Administrator Console: NTP Status:

NTP Daemon does not appear to be running

                                                                  < Refresh >
 SN:ACD7900052, Ver:4.1.0.5.2 [Updated:Tue Dec 2008-12-02 20:47:35 EST -0500]
Help: <F1> //  Exit: <ctl+Q> or <ctl+C> // Menus (Top-bar):  <ctl+X>
```

- NTP ist ordnungsgemäß konfiguriert und wird ausgeführt:

```
 File  Operation
 CC-SG Administrator Console: NTP Status:
NTP Daemon PID=16991
synchronised to NTP server (192.168.51.11) at stratum 6
   time correct to within 26 ms
   polling server every 64 s

-----------

client    127.127.1.0
client    192.168.51.11
     remote           local      st poll reach  delay   offset    disp
=============================================================================
=127.127.1.0     127.0.0.1       10   64  377 0.00000  0.000000 0.03058
*192.168.51.11   192.168.51.26    5   64  377 0.00043 -0.013413 0.08279


                                                                  < Refresh >
 SN:ACD7900052, Ver:4.1.0.5.2 [Updated:Tue Dec 2008-12-02 23:18:06 EST -0500]
Help: <F1> //  Exit: <ctl+Q> or <ctl+C> // Menus (Top-bar):  <ctl+X>
```

Systemschnappschuss aufnehmen

Wenn CC-SG nicht ordnungsgemäß funktioniert, ist es sehr hilfreich, die in CC-SG gespeicherten Informationen aufzunehmen, wie z. B. Systemprotokolle, Konfigurationen oder Datenbank, und zur Analyse und Problembehandlung an den technischen Support von Raritan zu senden.

1: Nehmen Sie einen Schnappschuss des CC-SG auf:

1. Wählen Sie "Operation (Vorgang) > Utilities (Werkzeuge) > System Snapshot (Systemschnappschuss)".
2. Klicken Sie auf "Ja", oder wählen Sie dies aus. Das Menü "System Snapshot" (Systemschnappschuss) wird geöffnet.
3. Vergewissern Sie sich, dass jeder im Bildschirm angezeigte verwendete Wert unter 60 % liegt und dass für den Schnappschuss ausreichend Speicherkapazität vorhanden ist. Andernfalls brechen Sie den Vorgang ab und führen eine Bereinigung aus, oder Sie bitten den technischen Support von Raritan um Hilfe.
4. Die Optionen für den Systemschnappschuss sind in zwei Bereiche unterteilt:
   - "Snapshot Configuration" (Schnappschusskonfiguration) zeigt eine Liste der CC-SG-Daten an, von denen Sie einen Schnappschuss erstellen können.
   - "Snapshot Operations" (Schnappschussvorgänge) zeigt eine Liste der Vorgänge an, die beim Aktivieren des Schnappschussvorgangs ausgeführt werden können.
5. Normalerweise ist es nicht erforderlich, die Standardoptionen für den Schnappschuss zu ändern, es sei denn Sie werden vom technischen Support von Raritan dazu aufgefordert. Wenn Sie dazu aufgefordert werden, klicken Sie mit der Maus oder verwenden die Pfeiltasten **zum Navigieren und drücken die Leertaste, um die gewünschten Schnappschussoptionen auszuwählen und mit einem X zu kennzeichnen.**
6. Klicken Sie auf "Submit" (Übertragen), oder wählen Sie dies aus, um mit dem Schnappschuss fortzufahren.
7. Während des Schnappschusses wird auf dem Bildschirm eine schnell laufende Liste von Elementen angezeigt. Es ist normal, dass CC-SG manchmal kurz anhält.
8. Nachdem der Schnappschuss erstellt wurde, zeigt CC-SG die Informationen für den Schnappschuss an, einschließlich:
   - Speicherort und Dateiname der CC-SG-Schnappschussdatei
   - Größe
   - MD5-Prüfsumme

Die Schnappschussinformationen dienen nur zur Referenz. Es ist nicht erforderlich, sie zu notieren.

9. Drücken Sie die Eingabetaste, um zum Menü "System Snapshot" (Systemschnappschuss) zurückzukehren.

2: Rufen Sie die CC-SG-Schnappschussdatei ab:

1. Verwenden Sie einen unterstützten Internetbrowser, und geben Sie folgenden URL ein: `http(s)://<IP-Adresse>/upload/`, wobei `<IP-Adresse>` für die IP-Adresse von CC-SG steht. Der Schrägstrich (/) nach `/upload` ist obligatorisch. Beispiel: `https://10.20.3.30/upload/`.
2. Das Dialogfeld "Enter Network Password" (Netzwerkkennwort eingeben) wird angezeigt. Geben Sie den Benutzernamen und das Kennwort des Diagnosekonsole-Administrationskontos ein, und klicken Sie auf OK, um sich anzumelden.
3. Alle verfügbaren Schnappschussdateien, die je in CC-SG aufgenommen wurden, werden angezeigt.

   Hinweis: CC-SG behält die Schnappschussdateien nur 10 Tage. Sie müssen die Dateien daher rechtzeitig abrufen.

4. Klicken Sie auf die Schnappschussdatei mit dem entsprechenden Dateinamen oder auf die Datei mit dem Namen "snapshot", weil dies die neueste Schnappschussdatei ist. Die Dateien sind bereits komprimiert, verschlüsselt und signiert. Sie müssen sie nur noch im Binärmodus übertragen.
5. Wenn Sie eine Datei mit IE speichern, speichern Sie sie als Raw-Datei, indem Sie in der Dropdown-Liste "Dateityp" des Dialogfelds "Speichern unter" die Option "Alle Dateien" auswählen.

Videoauflösung für Diagnosekonsole ändern

Raritan empfiehlt, dass Sie die Videoauflösung der Diagnosekonsole für den Monitor anpassen, um das Menü ordnungsgemäß anzuzeigen.

So passen Sie die Videoauflösung an:

1. Starten Sie CC-SG neu. Siehe ***CC-SG mit der Diagnosekonsole neu starten*** (siehe "***CC-SG mit der Diagnosekonsole neu hochfahren***" auf Seite 376).
2. Wenn die folgende Meldung angezeigt wird, drücken Sie innerhalb von fünf Sekunden eine beliebige Taste, um das Menü "GRUB" aufzurufen, wie z. B. Esc oder eine Pfeiltaste.

   ```
   Press any key to enter the menu (Drücken Sie eine
   beliebige Taste, um das Menü aufzurufen)
   ```

   ```
   Booting CentOS (x.x.x) in x seconds.... (Boote CentOS
   (x.x.x) in x Sekunden....)
   ```

3. Markieren Sie die Option "1024x768/24-bit" mithilfe der Pfeiltasten nach oben oder unten, und drücken Sie die Eingabetaste.

Kapitel 17 Integration von Power IQ

Wenn Sie sowohl CC-SG als auch Power IQ verwenden, gibt es mehrere Möglichkeiten, beide zusammen zu nutzen.

1. Steuern Sie die Stromversorgung von Power IQ-IT-Geräten über CC-SG.

   Wenn Sie beispielsweise die Stromversorgung eines Power IQ-IT-Geräts steuern möchten, das auch als CC-SG-Knoten fungiert, können Sie eine Power IQ Proxy-Schnittstelle verwenden, um Befehle zur Stromversorgungssteuerung in CC-SG zu geben.

2. Verwenden Sie CSV-Dateiimporte und -exporte, um Daten auf diesen beiden Systemen gemeinsam zu nutzen.

   Wenn Sie beispielsweise eine CC-SG-Einheit mit vielen Dominion PX-Geräten im IP-Netzwerk verwenden, können Sie eine CSV-Datei aus CC-SG exportieren, in der alle Knotennamen enthalten sind, die Datei gemäß den Spezifikation ändern und sie anschließend in Power IQ importieren. Siehe ***Dominion PX-Daten zur Verwendung in Power IQ*** (siehe "***Dominion PX-Daten zur Verwendung in Power IQ exportieren***" auf Seite 408).

   Oder, wenn Sie Power IQ mit vielen Dominion PX-Geräten verwenden und Sie die aktuellen IT-Gerätenamen als Knoten in CC-SG übernehmen möchten, können Sie eine Datei aus Power IQ exportieren, die Datei gemäß den Spezifikation ändern und sie anschließend in CC-SG importieren. Siehe ***Powerstrips aus Power IQ importieren*** (auf Seite 406).

3. Synchronisieren Sie Power IQ mit der CC-SG-Einheit, um automatisch IT-Geräte in CC-SG zu importieren, die in Power IQ konfiguriert wurden. Siehe ***Konfigurieren der Synchronisierung von Power IQ und CC-SG*** (auf Seite 403).

In diesem Kapitel

Stromversorgungssteuerung von Power IQ-IT-Geräten 399
Konfigurieren der Synchronisierung von Power IQ und CC-SG 403
Dominion PX-Daten von Power IQ importieren und exportieren 406

Stromversorgungssteuerung von Power IQ-IT-Geräten

Sie können CC-SG verwenden, um die Stromversorgung eines Power IQ-IT-Geräts, das Sie als Knoten zu CC-SG hinzugefügt haben, zu steuern.

Hiermit können Sie die Stromversorgung von Knoten steuern, die mit nicht durch CC-SG verwalteten PDUs verbunden sind.

Power IQ-Dienste konfigurieren

Sie müssen den Power IQ-Dienst konfigurieren, bevor Sie Power IQ-Proxy-Schnittstellen zu Knoten hinzufügen können, oder Power IQ mit CC-SG synchronisieren, um IT-Geräte zu CC-SG als Knoten hinzuzufügen. Rufen Sie dazu in CC-SG das Menü "Access" (Zugriff) auf.

Sie müssen über Rechte für CC-Setup und -Steuerung verfügen, um die Power IQ-Dienste konfigurieren zu können.

So konfigurieren Sie Power IQ-Dienste:

1. Stellen Sie sicher, dass die Web-API in Power IQ aktiviert ist. Klicken Sie auf der Registerkarte "Einstellungen" im Abschnitt "Security and Encryption" (Sicherheit und Verschlüsselung) auf "Web-API".

   Aktivieren Sie das Kontrollkästchen "Enable Web API" (Web-API aktivieren), und klicken Sie auf "Speichern".

2. Stellen Sie sicher, dass die Stromversorgung in Power IQ aktiviert ist. Klicken Sie auf der Registerkarte "Einstellungen" im Abschnitt "Appliance Administration" (Appliance-Administration) auf "Stromversorgungssteuerung". Aktivieren Sie das Kontrollkästchen "Enable Power Control" (Stromversorgungssteuerung aktivieren), und klicken Sie auf "Speichern".

3. Wählen Sie im CC-SG-Administrations-Client "Access > Power IQ Services > Add Power IQ Services" (Zugriff > Power IQ-Dienste > "Power IQ-Dienste hinzufügen) aus. Das Dialogfeld "New Power IQ Services Configuration" (Neue Power IQ-Dienste-Konfiguration) wird geöffnet.

4. Geben Sie einen Namen für das Gerät in das Feld "Power IQ Device Name" (Power IQ-Gerätename) ein. Der Name muss für das Power IQ-Gerät, das den Dienst zur Verfügung stellt, eindeutig sein. CC-SG akzeptiert keine doppelten Namen. Weitere Informationen zu den Regeln, die von CC-SG für die Länge von Namen verwendet werden, finden Sie unter ***Benennungskonventionen*** (siehe "***Benennungsregeln***" auf Seite 457).

5. Geben Sie die IP-Adresse oder den Hostnamen des Geräts im Feld "IP-Adresse/Hostname" ein. Die Regeln zur Vergabe von Hostnamen werden unter ***Terminologie/Abkürzungen*** (auf Seite 2) beschrieben.

6. Geben Sie im Feld "Heartbeat-Timeout (Sek.)" die Zeit (in Sekunden, von 30 bis 50.000) ein, die verstreichen soll, bevor zwischen dem neuen Gerät und CC-SG ein Zeitüberschreitungsfehler auftritt.

7. Geben Sie Authentifizierungsinformationen ein:

- Um ein Dienstkonto zur Authentifizierung zu verwenden, markieren Sie das Kontrollkästchen "Dienstkontoinformationen verwenden". Wählen Sie das gewünschte Dienstkonto im Menü "Dienstkontoname".

Oder

- Geben Sie einen Benutzernamen und ein Kennwort für die Authentifizierung ein.

8. Geben Sie eine kurze Beschreibung für das Gerät in das Feld "Beschreibung" ein. **Optional.**
9. Klicken Sie auf "Verbindung testen". Siehe ***Fehlerbehebung bei Verbindungen zu Power IQ*** (auf Seite 401), um Informationen zu Fehlermeldungen zu erhalten. Wenn Sie die Synchronisierung verwenden, siehe ***Konfigurieren der Synchronisierung von Power IQ und CC-SG*** (auf Seite 403).

Fehlerbehebung bei Verbindungen zu Power IQ

Prüfen Sie diese möglichen Fehlermeldungen und Lösungen, um Fehler bei der Verbindung mit Power IQ zu beheben.

Stellen Sie die Ursache fest, und bearbeiten Sie dann die Konfiguration, um sie zu korrigieren. Siehe ***Power IQ-Dienste konfigurieren*** (auf Seite 400).

Meldung	Auflösung
Kommunikation mit Verwaltungsgerät <Name> auf <IP> nicht möglich.	Dieser Fehler kann auf verschiedene Zustände hinweisen. ▪ Die Verbindung wurde remote abgelehnt. Auf der Remote-Adresse oder dem Port lauscht kein Prozess. ▪ Überprüfen Sie die Firewalls. Der Remote-Host kann aufgrund einer dazwischenliegenden Firewall nicht erreicht werden, oder ein dazwischenliegender Router ist ausgefallen. ▪ Unbekannter Host. Die IP-Adresse konnte anhand des eingegebenen Hostnamens nicht aufgelöst werden.
Authentifizierung fehlgeschlagen.	Benutzername und Kennwort sind falsch.
Kommunikation mit Verwaltungsgerät <Name> auf <IP> nicht möglich,	Die Web-API ist in Power IQ nicht aktiviert. Melden Sie sich bei Power IQ an, wählen Sie "Einstellungen >

Meldung	Auflösung
stellen Sie sicher, dass dessen Web-API aktiviert ist.	Web-API" und dann "Enable Web API" (Web-API aktivieren), und klicken Sie dann auf "Speichern".

Stromversorgungssteuerung von Power IQ-IT-Geräten konfigurieren

Wenn Sei den Power IQ-Dienst konfiguriert haben, können Sie auch konfigurieren, dass CC-SG die von Ihnen benötigten Knoten und Schnittstellen hinzufügt.

1. Fügen Sie das IT-Gerät hinzu, dessen Stromversorgung Sie steuern möchten. Siehe ***Knoten hinzufügen*** (auf Seite 130).
2. Fügen Sie eine Power IQ Proxy-Schnittstelle zur Stromversorgungssteuerung zum Knoten hinzu. Siehe ***Schnittstellen hinzufügen*** (auf Seite 148) und ***Schnittstellen für Power IQ Proxy-Stromversorgungsverbindungen*** (auf Seite 156).

Konfigurieren der Synchronisierung von Power IQ und CC-SG

CC-SG führt eine Synchronisierung mit Power IQ durch, um die in Power IQ konfigurierten IT-Geräte in CC-SG als Knoten hinzuzufügen. Bei der Synchronisierung erstellt CC-SG einen Knoten mit einer Power IQ-Proxy-Schnittstelle für jedes neue identifizierte IT-Gerät. Wenn CC-SG einen doppelten Knoten erkennt, bestimmt die von Ihnen gewählte Synchronisierungsrichtlinie, ob die Knoten konsolidiert, umbenannt oder abgelehnt werden.

Sie können jederzeit eine manuelle Synchronisierung durchführen oder eine Aufgabe einrichten, die periodisch wiederkehrend als Aufgabe ausgeführt wird. Weitere Informationen finden Sie unter ***Aufgabenmanager*** (auf Seite 330).

Sie können auch alle IT-Geräte von Power IQ abrufen oder einen Filter einrichten, sodass CC-SG nur die IT-Geräte synchronisiert, welche der Filter zulässt.

Schritt 1 – Hinzufügen einer Verbindung zu Power IQ für eine Synchronisierung mit CC-SG:

- Siehe ***Power IQ-Dienste konfigurieren*** (auf Seite 400).

Schritt 2 – Erstellen eines Filters (optional):

Filter sind optional. Wenn Sie keinen Filter erstellen, werden alle in Power IQ konfigurierten IT-Geräte entsprechend der Synchronisierungsrichtlinie zu CC-SG hinzugefügt. Filter gelten nur für die ausgewählte Power IQ-Instanz.

1. Wählen Sie "Access (Zugriff) > Power IQ Services (Power IQ-Dienste)" und dann den Namen des zu synchronisierenden Power IQ.
2. Wählen Sie im Abschnitt "Synchronisierung" einen Feldnamen aus der Liste "Feld". Die aufgeführten Feldnamen beziehen sich auf Felder in Power IQ.
3. Wählen Sie einen Suchoperator aus der Liste "Operator".
   - LIKE gibt IT-Geräte aus, bei denen der Wert im angegebenen Feld den genannten Text enthält. Der Wert "win" ist beispielsweise in "windows", "windows2k" und "win7" enthalten.
   - EQUAL gibt nur IT-Geräte aus, die genau den Wert im angegebenen Feld enthalten.
4. Geben Sie den im angegebenen Feld zu suchenden Wert ein, und verwenden Sie dabei den genannten Operator.
5. Klicken Sie zum Speichern auf OK, oder lassen Sie dieses Dialogfeld geöffnet und fahren Sie mit Schritt 3 fort.

Schritt 3 – Erstellen einer Synchronisierungsrichtlinie:

Hinweis: Die Synchronisierungsrichtlinie gilt für ALLE Power IQ-Instanzen, die in CC-SG konfiguriert sind. Siehe **Power IQ-Synchronisierungsrichtlinien** *(auf Seite 405), um Informationen zu jeder Richtlinie und anderen Synchronisierungsergebnissen zu erhalten.*

1. Wählen Sie im Abschnitt "Synchronisierung" die Option für die gewünschte Synchronisierungsrichtlinie:
   - Consolidate Nodes (Knoten konsolidieren)
   - Rename Duplicate Nodes (Doppelte Knoten umbenennen)
   - Reject Duplicate Nodes (Doppelte Knoten ablehnen)
2. Klicken Sie zum Speichern auf OK. Siehe ***Synchronisierung von Power IQ und CC-SG*** (auf Seite 404), um Informationen zur manuellen Synchronisierung und zur Synchronisierung nach Aufgabe zu erhalten.

Synchronisierung von Power IQ und CC-SG

Wenn Sie die Synchronisierungseinstellungen konfiguriert haben, können Sie jederzeit eine manuelle Synchronisierung durchführen. Alternativ können Sie eine Aufgabe erstellen, um periodisch wiederkehrend eine Synchronisierung durchzuführen.

Sie müssen über eine Berechtigung für Geräte-, Port- und Knotenverwaltung verfügen, um eine Synchronisierung durchführen zu können.

Siehe ***Konfigurieren der Synchronisierung von Power IQ und CC-SG*** (auf Seite 403) und ***Power IQ-Synchronisierungsrichtlinien*** (auf Seite 405), um weitere Informationen zur Konfiguration der Synchronisierungseinstellungen zu erhalten.

So synchronisieren Sie sofort Power IQ und CC-SG:

Wenn Sie auf "Jetzt synchronisieren" klicken, wird nur die ausgewählte Power IQ-Instanz synchronisiert. Wenn Sie alle Power IQ-Instanzen mit einem Zeitplan synchronisieren möchten, können Sie eine Aufgabe erstellen. Siehe nächste Vorgehensweise.

1. Wählen Sie "Access (Zugriff) > Power IQ Services (Power IQ-Dienste)" und dann die zu synchronisierende Power IQ-Instanz.
2. Überprüfen Sie, dass Filter und Richtlinie korrekt sind, und klicken Sie dann auf "Jetzt synchronisieren".
3. Das Dialogfeld "Synchronization Status Message" (Synchronisierungsstatusmeldung) wird angezeigt. Überprüfen Sie die Meldungen auf Ergebnisse Ihrer Synchronisierung.

So synchronisieren Sie Power IQ und CC-SG als Aufgabe:

1. Erstellen Sie die Aufgabe "Power IQ-Synchronisierung". Siehe ***Aufgaben planen*** (auf Seite 332).

Power IQ-Synchronisierungsrichtlinien

Wenn CC-SG einen doppelten Knoten erkennt, bestimmt die von Ihnen gewählte Synchronisierungsrichtlinie, ob die Knoten konsolidiert, umbenannt oder abgelehnt werden.

Siehe ***Konfigurieren der Synchronisierung von Power IQ und CC-SG*** (auf Seite 403) zum Festlegen der Synchronisierungsrichtlinie.

Synchronisierungsrichtlinien:

- Consolidate Nodes (Knoten konsolidieren):

  Wenn ein IT-Gerät (wie vom externen Schlüssel festgelegt) von mehr als einer Power IQ abgerufen wird, verfügt der Knoten über eine Power IQ-Proxy-Schnittstelle für jede Power IQ. CC-SG lässt doppelte Schnittstellennamen für einen einzigen Knoten zu.

- Rename Duplicate Nodes (Doppelte Knoten umbenennen):

  Wenn ein IT-Gerät (wie vom externen Schlüssel festgelegt) von mehr als einer Power IQ abgerufen wird, wird für jede ein Knoten mit einer einzigen Power IQ-Proxy-Schnittstelle erstellt. CC-SG benennt die Knoten um, um sie eindeutig zu machen, indem er eine Zahl in Klammern hinzufügt. Beispiel: `Knoten`, `Knoten(2)`, `Knoten(3)`

- Reject Duplicate Nodes (Doppelte Knoten ablehnen):

  Wenn ein IT-Gerät (wie vom externen Schlüssel festgelegt) von mehr als einer Power IQ abgerufen wird, wird für die erste Instanz ein Knoten und eine Power IQ-Proxy-Schnittstelle erstellt; nachfolgende Instanzen werden abgelehnt und als Fehler protokolliert. Das ist der Standard.

Andere Synchronisierungsergebnisse:

Wenn ein IT-Gerät bei der Synchronisierung nicht mehr besteht (wie vom externen Schlüssel festgelegt) und mit dem Knoten nur eine einzige Schnittstelle vom Typ Power IQ-Proxy-Schnittstelle verknüpft ist, wird der Knoten aus CC-SG gelöscht.

Wenn der Knoten noch über andere Schnittstellen neben der einzigen mit ihm verknüpften Power IQ-Proxy-Schnittstelle verfügt, wird nur diese Power IQ-Proxy-Schnittstelle aus CC-SG gelöscht.

Wenn eine Power IQ-Instanz aus CC-SG gelöscht wird, sind die Ergebnisse dieselben.

Dominion PX-Daten von Power IQ importieren und exportieren

Sie benötigen die Berechtigungen für CC-Setup und -Steuerung, Geräte-, Port- und Knotenverwaltung, um Dominion PX-Daten von Power IQ importieren bzw. exportieren zu können.

Powerstrips aus Power IQ importieren

Sie können Dominion PX-Geräte und deren Ausgangsnamen aus Power IQ importieren. Wenn die Dominion PX-Geräte bereits von CC-SG verwaltet werden, müssen Sie sie zunächst löschen. Durch den Import werden die Dominion PX-Geräte hinzugefügt und die in der CSV-Datei angegebenen Ausgänge konfiguriert und benannt.

Geräte und Ausgänge in der CSV-Datei, die keine Dominion PX-Geräte oder -Ausgänge sind, werden beim Importieren ignoriert.

Sie können den Power IQ-Dienst verwenden, um Knoten für Power IQ-IT-Geräte zu erstellen, die mit Dominion PX-Geräten und Powerstrips anderer Anbieter verbunden sind, und die nicht aus Power IQ importiert werden können. Siehe ***Stromversorgungssteuerung von Power IQ-IT-Geräten*** (auf Seite 399).

Schritt 1: CSV-Datei aus Power IQ exportieren

1. Melden Sie sich bei Power IQ an und navigieren Sie zum Dashboard.
2. Klicken Sie auf "Outlet Naming" (Ausgangsbenennung).
3. Klicken Sie neben dem Import auf den Link zum Exportieren einer CSV-Datei mit den aktuellen Ausgangsnamen.
4. Öffnen oder speichern Sie die Datei. Die Datei enthält alle Ausgänge in Power IQ.

Schritt 2: CSV-Datei bearbeiten

1. Bearbeiten Sie die exportierte CSV-Datei.
2. Löschen Sie die Spalte mit dem PX-Namen. Sie werden später eine Zeile mit einem Befehl zum Hinzufügen aller PX-Geräte erstellen.
3. Fügen Sie zwei Spalten am Anfang aller Zeilen ein.
   a. Geben Sie in Spalte 1 den Befehl `ADD` (Hinzufügen) ein.
   b. Geben Sie in Spalte 2 das Tag `OUTLETS` (Ausgänge) ein.
4. Fügen Sie eine Zeile für jedes hinzuzufügende PX-Gerät ein.

Spaltennummer	Tag oder Wert	Details
1	`ADD (Hinzufügen)`	Die erste Spalte für alle Tags ist der Befehl `ADD` (Hinzufügen).
2	`PX-DEVICE (PX-Gerät)`	Geben Sie das Tag wie beschrieben ein. Bei Tags wird die Groß- und Kleinschreibung nicht berücksichtigt.
3	IP-Adresse oder Hostname des PX-Geräts	Erforderliches Feld.
4	Benutzername	Erforderliches Feld.
5	Kennwort	Erforderliches Feld.
6	Alle Ausgänge konfigurieren	`TRUE` (Wahr) oder `FALSE` (Falsch) Der Standardwert ist `FALSE` (Falsch).
7	Beschreibung	Optional.

Schritt 3: Bearbeitete CSV-Datei in CC-SG importieren

1. Wählen Sie im CC-SG-Administrations-Client "Administration > Importieren > Import Powerstrips" (Powerstrips importieren).
2. Klicken Sie auf "Durchsuchen" und wählen Sie die zu importierende CSV-Datei aus. Klicken Sie auf "Öffnen".
3. Klicken Sie auf Überprüfen. Die Dateiinhalte werden im Bereich "Analysebericht" angezeigt.
   - Wenn die Datei ungültig ist, wird eine Fehlermeldung angezeigt. Klicken Sie auf "OK". Im Bereich "Probleme" auf der Seite wird eine Beschreibung der Dateiprobleme aufgeführt. Klicken Sie auf "In Datei speichern", um die Liste der Probleme zu speichern. Korrigieren Sie die CSV-Datei und versuchen Sie sie anschließend erneut zu validieren. Siehe ***Problembehebung bei CSV-Dateien*** (auf Seite 436).
4. Klicken Sie auf "Importieren".
5. Die Ergebnisse des Imports werden im Bereich "Aktionen" angezeigt. Erfolgreich importierte Elemente werden grün dargestellt. Nicht erfolgreich importierte Elemente werden rot dargestellt. Elemente, die aufgrund eines bereits vorhandenen oder bereits importierten Duplikats nicht erfolgreich importiert wurden, werden ebenso rot dargestellt.
6. Um weitere Details zu den Importergebnissen anzuzeigen, rufen Sie den Überwachungslistenbericht auf. Siehe ***Einträge in der Überwachungsliste für Importe*** (auf Seite 435).

Dominion PX-Daten zur Verwendung in Power IQ exportieren

Sie können Daten von Dominion PX-Geräten, die in CC-SG konfiguriert wurden, als CSV-Datei exportieren. Die exportierten Daten können als Teil einer CSV-Datei verwendet werden, um Daten in Power IQ zu importieren. Zu den Daten zählen Dominion PX-Geräte, Ausgangsnamen und IT-Gerätenamen.

Nur Dominion PX-Geräte, die an das IP-Netzwerk angeschlossen sind, können exportiert werden. Damit werden Dominion PX-Powerstrips ausgeschlossen, die nur als verwaltete Powerstrips bereitgestellt und nicht im IP-Netzwerk als Geräte verfügbar sind.

Hinweis: Exportierte Power IQ-Daten können nur in Power IQ importiert werden, nachdem die Datei wie beschrieben bearbeitet wurde. Die Datei kann nicht in CC-SG importiert werden.

Schritt 1: CSV-Datei aus CC-SG exportieren:

1. Klicken Sie auf "Administration > Exportieren > Power IQ-Daten exportieren".
2. Klicken Sie auf "In Datei exportieren".
3. Geben Sie einen Namen für die Datei ein, und wählen Sie den Speicherort aus.
4. Klicken Sie auf Speichern.

Schritt 2: CSV-Datei bearbeiten und in Power IQ importieren:

Die Exportdatei enthält drei Abschnitte. Lesen Sie die Kommentare in der CSV-Datei, um Anweisungen zur Verwendung der einzelnen Abschnitte als Teil einer Multi-Tab-CSV-Importdatei für Power IQ zu erhalten.

Weitere Informationen erhalten Sie im *Power IQ User Guide* und *CSV Import Template* auf der Support-Seite "Firmware and Documentation" (Firmware und Dokumentation) auf der Website von Raritan.

Anhang A Technische Daten für V1 und E1

In diesem Kapitel

V1-Modell.....409
E1-Modell.....410

V1-Modell

V1 – Allgemeine technische Daten	
Formfaktor	1U
Abmessungen (T x B x H)	615 mm x 485 mm x 44 mm
Gewicht	10,80 kg
Stromversorgung	Ein Netzteil (1 x 300 Watt)
Betriebstemperatur	10° - 35° (50°- 95°)
Mittlerer Reparaturabstand (Mean Time Between Failure, MTBF)	36.354 Stunden
KVM-Administrationsport	(DB15 + PS2 oder USB Tastatur/Maus)
Serieller Administrationsport	DB9
Konsolenport	(2) USB 2.0 Ports

V1 – Umgebungsanforderungen	
Betrieb	
Luftfeuchtigkeit	8% bis 90% relative Luftfeuchtigkeit
Höhe über NN	Kann problemlos in Höhen von 0 bis 3.048 m betrieben und bis zu 12.192 m gelagert werden.
Erschütterung	5-55-5 Hz, 0,38 mm, 1 Minute/Zyklus; 30 Minuten für jede Achse (x,y,z)
Stoß	Nicht zutreffend
Lagerung	
Temperatur	-40° - +60° (-40°-140°)

Betrieb	
Luftfeuchtigkeit	5% bis 95% relative Luftfeuchtigkeit
Höhe über NN	Kann problemlos in Höhen von 0 bis 3.048 m betrieben und bis zu 12.192 m gelagert werden.
Erschütterung	5-55-5 Hz, 0,38 mm, 1 Minute/Zyklus; 30 Minuten für jede Achse (x,y,z)
Stoß	Nicht zutreffend

E1-Modell

E1 – Allgemeine technische Daten	
Formfaktor	2U
Abmessungen (T x B x H)	687 mm x 475 mm x 88 mm
Gewicht	20 kg
Stromversorgung	SP502-2S während des Betriebs austauschbare Netzteile 500 W 2U
Betriebstemperatur	0 bis 50° C
Mittlerer Reparaturabstand (Mean Time Between Failure, MTBF)	53.564 Stunden
KVM-Administrationsport	PS/2-Tastatur- und -Mausports, 1 VGA-Port
Serieller Administrationsport	Serieller Fast UART 16550 Port
Konsolenport	(2) USB 2.0 Ports

E1 – Umgebungsanforderungen	
Betrieb	
Luftfeuchtigkeit	5-90 %, nicht-kondensierend
Höhe über NN	Meeresspiegel bis 213.360,00 cm
Erschütterung	10 Hz bis 500 Hz Durchlauf bei 0,5 g konstanter Beschleunigung über eine Stunde auf jeder der senkrechten Achsen x, y und z
Stoß	5 g für 11 ms mit ½ Sinuskurve für jede senkrechte Achse x, y und z

Betrieb **Lagerung**	
Temperatur	-40° bis 70° C
Luftfeuchtigkeit	5-90 %, nicht-kondensierend
Höhe über NN	Meeresspiegel bis 12.192 m
Erschütterung	10 Hz bis 300 Hz Durchlauf bei 2 g konstanter Beschleunigung über eine Stunde auf jeder der senkrechten Achsen x, y und z
Stoß	30 g für 11 ms mit ½ Sinuskurve für jede senkrechte Achse x, y und z

Anhang B CC-SG und Netzwerkkonfiguration

Dieser Anhang enthält die Netzwerkanforderungen (inkl. Adressen, Protokolle und Ports) für eine typische CC-SG-Implementierung. Sie finden Informationen, wie Sie Ihr Netzwerk für beide externen Zugriffe und zur Einhaltung der internen Sicherheits- und Routingrichtlinien konfigurieren können. Details werden für TCP/IP-Netzwerkadministratoren bereitgestellt. Die Rolle und der Verantwortungsbereich des TCP/IP-Administrators kann über den eines CC-SG-Administrators hinausgehen. Dieser Anhang hilft dem Administrator, CC-SG und die Komponenten in den Sicherheitszugriff und die Routingrichtlinien einer Site zu integrieren.

Die Tabellen enthalten die Protokolle und Ports, die von CC-SG und den verknüpften Komponenten benötigt werden.

In diesem Kapitel

Erforderliche geöffnete Ports für CC-SG-Netzwerke: Übersicht 412
CC-SG-Kommunikationskanäle 414

Erforderliche geöffnete Ports für CC-SG-Netzwerke: Übersicht

Die folgenden Ports müssen geöffnet sein:

Portnummer	Protokoll	Zweck	Details
80	TCP	HTTP-Zugriff auf CC-SG	Unverschlüsselt.
443	TCP	HTTP-(SSL-)Zugriff auf CC-SG und Knotenzugriff auf mit Dominion KXII verbundene Knoten im Direktmodus	SSL-/AES-128-/AES-256-Verschlüsselung.
8080	TCP	CC-SG-an-PC-Client	SSL-/AES-128-/AES-256-Verschlüsselung, falls konfiguriert.
2400	TCP	Knotenzugriff (Proxy-Modus)	Dieser Port muss pro Raritan-Gerät geöffnet werden, auf das extern zugegriffen wird. Die anderen Ports in der Tabelle müssen nur für den Zugriff auf CC-SG geöffnet werden. Nur verschlüsselt für Dominion KX II-Geräte, Version 2.1.10 oder höher, wenn die Verschlüsselung

Portnummer	Protokoll	Zweck	Details
			im Gerät festgelegt wird.
5000	TCP	Knotenzugriff (Direktmodus)	Dieser Port muss pro Raritan-Gerät geöffnet werden, auf das extern zugegriffen wird. Die anderen Ports in der Tabelle müssen nur für den Zugriff auf CC-SG geöffnet werden. AES-128-/AES-256-Verschlüsselung, falls konfiguriert.
80 und 443 für Steuerungssystemknoten 80, 443, 902 und 903 für Knoten des virtuellen Hosts und virtuellen Geräts	TCP	Virtueller Knotenzugriff	Nicht zutreffend
51000	TCP	SX-Zielzugriff (Direktmodus)	AES-128-/AES-256-Verschlüsselung, falls konfiguriert.

Mögliche Ausnahmen für die erforderlichen offenen Ports:

Port 80 kann geschlossen werden, falls der Zugriff auf CC-SG vollständig über HTTPS-Adressen erfolgt.

Ports 5000 und 51000 können geschlossen werden, wenn der CC-SG-Proxymodus für Verbindungen von der Firewall verwendet wird.

CC-SG-Kommunikationskanäle

Jeder Kommunikationskanal ist dokumentiert. Die Tabelle enthält für jeden Kommunikationskanal Folgendes:

- Die symbolischen IP-Adressen, die von den Kommunikationsteilnehmern verwendet werden. Diese Adressen müssen für jeden Kommunikationspfad zwischen den Einheiten erlaubt sein.
- Die Richtung, in die die Kommunikation hergestellt wird. Dies kann für Ihre besonderen Site-Richtlinien wichtig sein. Für eine bestimmte CC-SG-Rolle muss der Pfad zwischen den kommunizierenden Parteien verfügbar sein. Dies gilt auch für alternative Routenpfade, die ggf. bei einem Netzwerkausfall verwendet werden.
- Die Portnummer und das Protokoll, die von CC-SG verwendet werden.
- Zeigt an, ob der Port konfigurierbar ist, d. h. der Administrations-Client oder die Diagnosekonsole stellen ein Feld bereit, in dem Sie einen anderen Wert für die Portnummer als den Standardwert angeben können. Dies kann aufgrund von Konflikten mit anderen Anwendungen im Netzwerk oder aus Sicherheitsgründen nötig sein.
- Details zur Kommunikationsmethode, die Nachricht, die über den Kommunikationskanal weitergegeben wird oder die Verschlüsselung.

CC-SG und Raritan-Geräte

Eine Hauptrolle von CC-SG ist die Verwaltung und Steuerung von Raritan-Geräten (z. B. Dominion KX II). Normalerweise kommuniziert CC-SG mit diesen Geräten über ein TCP/IP-Netzwerk (lokal, WAN oder VPN), und die Protokolle TCP und UDP werden wie folgt verwendet:

Kommunikationsrichtung	Portnummer	Protokoll	Konfigurierbar?	Details
CC-SG zu Lokaler Broadcast	5000	UDP	ja	Heartbeat
CC-SG zu Remote LAN IP	5000	UDP	ja	Heartbeat
CC-SG zu Raritan-Gerät	5000	TCP	ja	RDM-Protokoll RC4-/AES-128-/AES-256-Verschlüsselung
Raritan-Geräte zu CC-SG	5001	UDP	nein	Heartbeat
CC-SG-an-Dominion PX	623 443	UDP	nein nein	
CC-SG zu Dominion KXII im	443	TCP	nein	

Kommunikationsrichtung	Portnummer	Protokoll	Konfigurierbar?	Details
Direktmodus				

CC-SG Clustering

Wenn die optionale CC-SG Clustering-Funktion verwendet wird, müssen die folgenden Ports für die miteinander verbundenen Subnetzwerke verfügbar sein. Wird die optionale Clustering-Funktion nicht verwendet, müssen diese Ports nicht geöffnet sein.

Jede CC-SG im Cluster kann ein anderes LAN aufweisen. Die Verbindung zwischen den Einheiten sollte jedoch sehr zuverlässig und nicht anfällig für Zeiten mit hoher Belastung sein.

Viele TCP/IP-Verbindungen in einem CC-SG-Cluster werden in der Hierarchie primärer Knoten – Sicherungsknoten verwaltet und initiiert. Diese Verbindungen können für längere Zeitspannen inaktiv sein, sie sind jedoch für den Betrieb des Clusters erforderlich.

Stellen Sie sicher, dass bei keiner der CC-SG-zu-CC-SG-Clusterverbindungen über VPN oder Firewalls eine Zeitüberschreitung auftritt oder die Verbindungen blockiert werden. Eine Zeitüberschreitung bei den Verbindungen führt zu Fehlern beim Cluster.

Kommunikationsrichtung	Portnummer	Protokoll	Konfigurierbar?	Details
CC-SG zu Lokaler Broadcast	10000	UDP	nein	Heartbeat
CC-SG zu Remote LAN IP	10000	UDP	nein	Heartbeat
CC-SG zu CC-SG	5432	TCP	nein	Von HA-JDBC auf Primär an Sicherungs-PostgreSQL DB-Server. Unverschlüsselt.
CC-SG zu CC-SG	8732	TCP	nein	Primär-/Sicherungsserver für Synchronisierung von Clustering-Steuerdatenaustausch. MD5-verschlüsselt.
CC-SG zu CC-SG	3232	TCP	nein	Primär-/Sicherungs-SNMP-Synchronisierungskonfiguration ändert die Weiterleitung.

Kommunikationsrichtung	Portnummer	Protokoll	Konfigurierbar?	Details
				Unverschlüsselt.

Zugriff auf Infrastrukturdienste

CC-SG kann zur Verwendung verschiedener Dienste nach Industriestandard wie DHCP, DNS und NTP konfiguriert werden. Diese Ports und Protokolle werden verwendet, um CC-SG die Kommunikation mit diesen optionalen Servern zu ermöglichen.

Kommunikationsrichtung	Portnummer	Protokoll	Konfigurierbar?	Details
DHCP-Server zu CC-SG	68	UDP	nein	IPv4 DHCP-Standard
CC-SG zu DHCP-Server	67	UDP	nein	IPv4 DHCP-Standard
NTP-Server zu CC-SG	123	UDP	nein	NTP-Standard
CC-SG zu DNS	53	UDP	nein	DNS-Standard

Verbindung von PC-Clients mit CC-SG

PC-Clients verwenden für die Verbindung zu CC-SG einen von drei Modi:

- Administrations- oder Zugriffs-Client über einen Webbrowser. CC-SG unterstützt SSL Version 2, SSL Version 3 und TLS Version 1 für Browserverbindungen. Sie können diese Verschlüsselungsmethoden in Ihrem Browser konfigurieren.
- Befehlszeilenschnittstelle (Command Line Interface, CLI) über SSH
- Diagnosekonsole

Kommunikationsrichtung	Portnummer	Protokoll	Konfigurierbar?	Details
PC-Client-an-CC-SG	443	TCP	nein	Client-Server-Kommunikation. SSL-/AES-128-/AES-256-Verschlüsselung, falls konfiguriert.
PC-Client-an-CC-SG	80	TCP	nein	Client-Server-Kommunikation. Unverschlüsselt. Wenn SSL aktiviert ist, wird Port 80 auf 443 umgeleitet.
PC-Client-an-CC-SG	8080	TCP	nein	Client-Server-Kommunikation. SSL-/AES-128-/AES-256-Vers

Kommunikationsrichtung	Portnummer	Protokoll	Konfigurierbar?	Details
				chlüsselung, falls konfiguriert. Port 8080 ist auf CC-SG geöffnet, nicht auf dem PC-Client.
PC-Client zu CLI SSH	22	TCP	ja	Client-Server-Kommunikation. SSL-/AES-128-/AES-256-Verschlüsselung, falls konfiguriert.
PC-Client zur Diagnosekonsole	23	TCP	ja	Client-Server-Kommunikation. SSL-/AES-128-/AES-256-Verschlüsselung, falls konfiguriert.

Verbindung von PC-Clients mit Knoten

Eine weitere wichtige Rolle von CC-SG ist die Verbindung von PC-Clients mit verschiedenen Knoten. Diese Knoten können serielle oder KVM-Konsolenverbindungen zu Raritan-Geräten (auch Out-of-Band-Verbindungen) darstellen. Ein anderer Modus verwendet In-Band-Zugriffsmethoden wie VNC, RDP oder SSH.

Ein weiterer Aspekt der Kommunikation zwischen dem PC-Client und dem Knoten ist, ob Folgendes zutrifft:

- Der PC-Client stellt entweder über ein Raritan-Gerät oder den In-Band-Zugriff eine direkte Verbindung zum Knoten her. Dies wird als Direktmodus bezeichnet.
- Der PC-Client stellt über CC-SG eine Verbindung zum Knoten her, der als Anwendungsfirewall dient. Dies wird als Proxymodus bezeichnet.

Kommunikationsrichtung	Portnummer	Protokoll	Konfigurierbar?	Details
Client an CC-SG über Proxy zum Knoten	2400 (auf CC-SG)	TCP	nein	Client-Server-Kommunikation. Unverschlüsselt.
Client an Raritan-Gerät an Out-of-Band-KVM-Knoten (Direktmodus)	5000 (auf Raritan-Gerät)	TCP	ja	Client-Server-Kommunikation. SSL-/AES-128-/AES-256-Verschlüsselung, falls konfiguriert.
Client an Raritan Dominion SX-Gerät an	51000 (auf	TCP	ja	Client-Server-Kommunikation.

Kommunikationsrichtung	Portnummer	Protokoll	Konfigurierbar?	Details
seriellen Out-of-Band-Knoten (Direktmodus)	Raritan-Gerät)			SSL-/AES-128-/AES-256-Verschlüsselung, falls konfiguriert.

CC-SG und Client für IPMI, iLO/RILOE, DRAC, RSA

Möglicherweise müssen Sie zusätzliche Ports öffnen, damit CC-SG Geräte anderer Anbieter wie iLO/RILOE- und iLO2/RILOE2-Server verwalten kann. Ziele eines iLO/RILOE-Geräts werden ein-/ausgeschaltet und direkt aktiviert und deaktiviert. IPMI-Server (Intelligent Platform Management Interface) können ebenfalls von CC-SG gesteuert werden. Das gleiche gilt für Dell DRAC- und RSA-Ziele.

Hinweis: Für einige In-Band-Schnittstellen müssen zusätzliche Ports geöffnet sein. Weitere Informationen finden Sie in den jeweiligen Handbüchern.

Kommunikationsrichtung	Portnummer	Protokoll	Konfigurierbar?	Details
CC-SG zu IPMI	623	TCP	nein	IPMI-Standard
CC-SG zu iLO/RILOE (verwendet HTTP-Ports)	80 oder 443	TCP	nein	Drittanbieterstandard
CC-SG zu DRAC	80 oder 443	TCP	nein	Drittanbieterstandard
CC-SG zu RSA	80 oder 443	TCP	nein	Drittanbieterstandard

CC-SG und SNMP

Mit Simple Network Management Protocol (SNMP) sendet CC-SG SNMP-Traps (Ereignisbenachrichtigungen) an einen SNMP-Manager im Netzwerk. CC-SG unterstützt außerdem SNMP-Get/Set-Anfragen mit Unternehmensverwaltungslösungen von Drittanbietern wie HP OpenView.

Kommunikationsrichtung	Portnummer	Protokoll	Konfigurierbar?	Details
SNMP Manager zu CC-SG	161	UDP	ja	SNMP-Standard

Kommunikationsrichtung	Portnummer	Protokoll	Konfigurierbar?	Details
CC-SG zu SNMP Manager	162	UDP	ja	SNMP-Standard

Interne CC-SG-Ports

CC-SG verwendet mehrere Ports für interne Funktionen und die die lokale Firewall sperrt den Zugriff auf diese Ports. Einige externe Scanner erkennen diese ggf. als "gesperrt" oder "gefiltert". Der externe Zugriff auf diese Ports ist nicht erforderlich und kann weiterhin gesperrt werden. Diese Ports werden zurzeit verwendet:

- 1088
- 1098
- 2222
- 4444
- 4445
- 8009
- 8083
- 8093

Außer diesen Ports verwendet CC-SG ggf. TCP- und UDP-Ports im Bereich 32xxx (oder höher). Der externe Zugriff auf diese Ports ist nicht erforderlich und kann gesperrt werden.

CC-SG-Zugriff über NAT-fähige Firewall

Wenn die Firewall NAT (Network Address Translation) mit PAT (Port Address Translation) verwendet, sollte der Proxymodus für alle Verbindungen, die diese Firewall verwenden, konfiguriert werden. Die Firewall muss für externe Verbindungen zu den Ports 80 (kein-SSL) oder 443 (SSL), 8080 und 2400 so konfiguriert sein, dass an CC-SG weitergeleitet wird, da der PC-Client die Sitzungen an diesen Ports startet.

Hinweis: Nicht-SSL-Verkehr sollte nicht über eine Firewall abgewickelt werden.

Verbindungen, die die Firewall verwenden, müssen so konfiguriert werden, dass sie den Proxymodus verwenden. Siehe ***Verbindungsmodi: Direkt und Proxy*** (auf Seite 297). CC-SG stellt eine Verbindung zu den verschiedenen Zielen für die PC-Client-Anforderungen her. CC-SG beendet die PC-Client- und Ziel-TCP/IP-Verbindung jedoch, die über eine Firewall geleitet wird.

RDP-Zugriff auf Knoten

Port 3389 muss für den RDP-Zugriff auf Knoten geöffnet sein.

VNC-Zugriff auf Knoten

Port 5800 oder 5900 muss für den VNC-Zugriff auf Knoten geöffnet sein.

SSH-Zugriff auf Knoten

Port 22 muss für den SSH-Zugriff auf Knoten geöffnet sein.

Port für die Überwachung des Remotesystems

Wenn die Funktion zur Überwachung des Remotesystems aktiviert ist, wird Port 19150 standardmäßig geöffnet. Siehe ***Überwachung des Remotesystems konfigurieren*** (auf Seite 385).

Anhang C Benutzergruppenberechtigungen

Diese Tabelle zeigt, welche Zugriffsrechte einem Benutzer zugewiesen sein müssen, damit er Zugriff auf einen CC-SG-Menüpunkt hat.

*Keine bedeutet, dass keine bestimmte Berechtigung erforderlich ist. Benutzer mit Zugriff auf CC-SG können diese Menüs und Befehle anzeigen und darauf zugreifen.

Menü > Untermenü	Menüelement	Erforderliche Berechtigung	Beschreibung
Secure Gateway	Dieses Menü steht allen Benutzern zur Verfügung.		
	Mein Profil	Keine*	
	Tipp des Tages	Keine*	
	Drucken	Keine*	
	Fenster drucken	Keine*	
	Abmelden	Keine*	
	Beenden	Keine*	
Benutzer	Dieses Menü und die Benutzerstrukturansicht stehen nur Benutzern mit der Berechtigung „User Management“ (Benutzerverwaltung) zur Verfügung.		
> Benutzermanager	> Benutzer hinzufügen	Benutzerverwaltung	
	(Benutzer bearbeiten)	Benutzerverwaltung	Über Benutzerprofil
	> Benutzer löschen	Benutzerverwaltung	
	> Benutzer aus Gruppe löschen	Benutzerverwaltung	
	> Benutzer abmelden	Benutzerverwaltung	
	> Massenkopieren	Benutzerverwaltung	
> Benutzergruppenmanager	> Benutzergruppe hinzufügen	Benutzerverwaltung	
	(Benutzergruppen bearbeiten)	Benutzerverwaltung	Über Benutzergruppenprofil
	> Benutzergruppe	Benutzerverwaltung	

Menü > Untermenü	Menüelement	Erforderliche Berechtigung	Beschreibung
	löschen		
	> Benutzer der Gruppe zuweisen	Benutzerverwaltung	
	> Benutzer abmelden	Benutzerverwaltung	
	Knotenüberwachung	Benutzerverwaltung	
Geräte	Dieses Menü und die Benutzerstrukturansicht stehen nur Benutzern mit folgenden Berechtigungen zur Verfügung: Geräte-, Port- und Knotenverwaltung Device Configuration and Upgrade Management		
	Geräte erkennen	Geräte-, Port- und Knotenverwaltung	
> Gerätemanager	> Gerät hinzufügen	Geräte-, Port- und Knotenverwaltung	
	(Geräte bearbeiten)	Geräte-, Port- und Knotenverwaltung	Über das Geräteprofil
	> Gerät löschen	Geräte-, Port- und Knotenverwaltung	
	> Massenkopieren	Geräte-, Port- und Knotenverwaltung	
	> Gerät aktualisieren	Device Configuration and Upgrade Management	
>> Konfiguration	>> Sicherung	Device Configuration and Upgrade Management	
	>> Wiederherstellen	Device Configuration and Upgrade Management	
	>> Konfiguration kopieren	Device Configuration and Upgrade Management	
	> Gerät neu starten	Geräte-, Port- und Knotenverwaltung oder Gerätekonfiguration und Aktualisierungsverwaltung	
	> Gerät anpingen	Geräte-, Port- und Knotenverwaltung oder Gerätekonfiguration und Aktualisierungsverwaltung	

Menü > Untermenü	Menüelement	Erforderliche Berechtigung	Beschreibung
	> Verwaltung unterbrechen	Geräte-, Port- und Knotenverwaltung oder Gerätekonfiguration und Aktualisierungsverwaltung	
	> Gerätestromman ager	Geräte-, Port- und Knotenverwaltung und Stromversorgungssteuerung für Knoten	
	> Administration starten	Geräte-, Port- und Knotenverwaltung oder Gerätekonfiguration und Aktualisierungsverwaltung	
	> Benutzerstation-A dministration starten	Geräte-, Port- und Knotenverwaltung	
	> Benutzer trennen	Geräte-, Port- und Knotenverwaltung oder Gerätekonfiguration und Aktualisierungsverwaltung	
	> Topologieansicht	Geräte-, Port- und Knotenverwaltung	
> Ansicht ändern	> Benutzerdefiniert e Ansicht erstellen	Geräte-, Port- und Knotenverwaltung oder Gerätekonfiguration und Aktualisierungsverwaltung	
	> Strukturansicht	Geräte-, Port- und Knotenverwaltung oder Gerätekonfiguration und Aktualisierungsverwaltung	
> Portmanager	> Verbinden	Geräte-, Port- und Knotenverwaltung und Out-of-Band-Zugriff für Knoten	
	> Ports konfigurieren	Geräte-, Port- und Knotenverwaltung	
	> Port trennen	Geräte-, Port- und Knotenverwaltung	
	> Ports löschen	Geräte-, Port- und Knotenverwaltung	
	> Powerstripport-M	Geräte-, Port- und Knotenverwaltung und	

Menü > Untermenü	Menüelement	Erforderliche Berechtigung	Beschreibung
	anager	Stromversorgungssteuerung für Knoten	
	> Powerstrip hinzufügen	Geräte-, Port- und Knotenverwaltung	
> Portsortieroptionen	> Nach Portname	Geräte-, Port- und Knotenverwaltung oder Gerätekonfiguration und Aktualisierungsverwaltung	
	> Nach Portstatus	Geräte-, Port- und Knotenverwaltung oder Gerätekonfiguration und Aktualisierungsverwaltung	
	> Nach Portnummer	Geräte-, Port- und Knotenverwaltung oder Gerätekonfiguration und Aktualisierungsverwaltung	
Knoten	Dieses Menü und die Knotenstrukturansicht stehen nur Benutzern mit folgenden Berechtigungen zur Verfügung: Geräte-, Port- und Knotenverwaltung Node In-Band Access (In-Band Knotenzugriff) Node Out-of-Band Access (Out-of-Band Knotenzugriff) Node Power Control		
	Knoten hinzufügen	Geräte-, Port- und Knotenverwaltung	
	(Knoten bearbeiten)	Geräte-, Port- und Knotenverwaltung	Über das Knotenprofil
	Knoten löschen	Geräte-, Port- und Knotenverwaltung	
	<Schnittstellenname>	Node In-Band Access oder Out-of-Band-Zugriff für Knoten	
	Trennen	Eine der Folgenden: Node In-Band Access oder Node Out-of-Band Access oder Geräte-, Port- und Knotenverwaltung oder Device Configuration and	

Menü > Untermenü	Menüelement	Erforderliche Berechtigung	Beschreibung
		Upgrade Management	
	Virtualisierung	Device-, Port- and Node Management	
	Massenkopieren	Device-, Port- and Node Management	
	Stromversorgungssteuerung	Stromversorgungssteuerung	
	Dienstkonten	Geräte-, Port- und Knotenverwaltung	
	Dienstkonten zuweisen	Geräte-, Port- und Knotenverwaltung	
	Gruppenstromversorgungssteuerung	Stromversorgungssteuerung	
	Blades konfigurieren	Geräte-, Port- und Knotenverwaltung	
	Knoten anpingen	Geräte-, Port- und Knotenverwaltung	
	Lesezeichen für Knotenschnittstelle	Node In-Band Access oder Out-of-Band-Zugriff für Knoten	
> Knotensortieroptionen	> Nach Knotenname	Eine der Folgenden: Geräte-, Port- und Knotenverwaltung oder Node In-Band Access oder Node Out-of-Band Access oder Stromversorgungssteuerung	
	> Nach Knotenstatus	Eine der Folgenden: Geräte-, Port- und Knotenverwaltung oder Node In-Band Access oder Node Out-of-Band Access oder Node Power Control	
> Chat	> Chatsitzung starten	Node In-Band Access oder Node Out-of-Band Access	

Menü > Untermenü	Menüelement	Erforderliche Berechtigung	Beschreibung
		oder Node Power Control	
	> Chatsitzung anzeigen	Node In-Band Access oder Node Out-of-Band Access oder Node Power Control	
	> Chatsitzung beenden	Node In-Band Access oder Node Out-of-Band Access oder Node Power Control	
> Ansicht ändern	> Benutzerdefinierte Ansicht erstellen	Eine der Folgenden: Device-, Port- and Node Management Node In-Band Access oder Node Out-of-Band Access oder Node Power Control	
	> Strukturansicht	Eine der Folgenden: Geräte-, Port- und Knotenverwaltung oder Node In-Band Access oder Node Out-of-Band Access oder Node Power Control	
Zuordnungen	Dieses Menü steht nur Benutzern zur Verfügung, die die Berechtigung „User Security Management“ (Benutzersicherheitsverwaltung) aufweisen.		
	> Zuordnung	User Security Management	Umfasst Funktionen zum Hinzufügen, Bearbeiten und Löschen.
	> Gerätegruppen	User Security Management	Umfasst Funktionen zum Hinzufügen, Bearbeiten und Löschen.
	> Knotengruppen	User Security Management	Umfasst Funktionen zum Hinzufügen,

Menü > Untermenü	Menüelement	Erforderliche Berechtigung	Beschreibung
			Bearbeiten und Löschen.
	> Richtlinien	User Security Management	Umfasst Funktionen zum Hinzufügen, Bearbeiten und Löschen.
Berichte	Dieses Menü steht nur Benutzern mit beliebigen administrativen Berechtigungen zur Verfügung, ausgenommen für Benutzer, die nur die Berechtigung "Benutzersicherheitsverwaltung" aufweisen.		
	Überwachungsliste	CC Setup And Control	
	Fehlerprotokoll	CC Setup And Control	
	Zugriffsbericht	Geräte-, Port- und Knotenverwaltung	
	Verfügbarkeitsbericht	Geräte-, Port- und Knotenverwaltung oder Gerätekonfiguration und Aktualisierungsverwaltung	
> Benutzer	> Aktive Benutzer	Benutzerverwaltung	
	> Gesperrte Benutzer	CC Setup And Control	
	> Alle Benutzerdaten	Zum Anzeigen aller Benutzerdaten: Benutzerverwaltung Zum Anzeigen Ihrer eigenen Benutzerdaten: Keine	
	> Benutzergruppendaten	Benutzerverwaltung	
> Geräte	> Geräteanlagebericht	Geräte-, Port- und Knotenverwaltung oder Gerätekonfiguration und Aktualisierungsverwaltung	
	> Gerätegruppendaten	Geräte-, Port- und Knotenverwaltung	
	> Port abfragen	Geräte-, Port- und Knotenverwaltung	
> Knoten	> Knotenanlageberi	Geräte-, Port- und Knotenverwaltung	

Menü > Untermenü	Menüelement	Erforderliche Berechtigung	Beschreibung
	cht		
	> Aktive Knoten	Geräte-, Port- und Knotenverwaltung	
	> Knotenerstellung	Geräte-, Port- und Knotenverwaltung	
	> Knotengruppendaten	Geräte-, Port- und Knotenverwaltung	
> Active Directory	AD-Benutzergruppenbericht	CC Setup and Control oder User Management	
	Geplante Berichte	CC-Setup und -Steuerung oder Device Configuration and Upgrade Management	
Zugang			
	WS-API hinzufügen	CC Setup And Control	
Administration	Dieses Menü steht nur Benutzern mit einer der folgenden Berechtigung zur Verfügung: CC Setup And Control Kombination aus Geräte-, Port- und Knotenverwaltung, Benutzerverwaltung und Benutzersicherheitsverwaltung		
	Setup-Assistent	Alle der Folgenden: Geräte-, Port- und Knotenverwaltung, Benutzerverwaltung und Benutzersicherheitsverwaltung	
	Tipp des Tages einrichten	CC Setup And Control	
	Anwendungen	CC Setup And Control	
	Firmware	CC-Setup und -Steuerung oder Device Configuration and Upgrade Management	
	Konfiguration	CC Setup And Control	

Menü > Untermenü	Menüelement	Erforderliche Berechtigung	Beschreibung
	Clusterkonfiguration	CC Setup And Control	
	Umgebung	CC Setup And Control	
	Sicherheit	CC Setup And Control	
	Benachrichtigungen	CC Setup And Control	
	Aufgaben	CC Setup And Control	
	Kompatibilitätsmatrix	Geräte-, Port- und Knotenverwaltung oder Gerätekonfiguration und Aktualisierungsverwaltung	
> Importieren	Kategorien importieren	CC-Setup und -Steuerung und User Security Management	
	Benutzer importieren	CC-Setup und -Steuerung und Benutzerverwaltung	
	Knoten importieren	CC-Setup und -Steuerung und Geräte-, Port- und Knotenverwaltung	
	Geräte importieren	CC-Setup und -Steuerung und Geräte-, Port- und Knotenverwaltung	
	Powerstrips importieren	CC-Setup und -Steuerung und Geräte-, Port- und Knotenverwaltung	
> Exportieren	Kategorien exportieren	CC-Setup und -Steuerung und User Security Management	
	Benutzer exportieren	CC-Setup und -Steuerung und Benutzerverwaltung	
	Knoten exportieren	CC-Setup und -Steuerung und Geräte-, Port- und Knotenverwaltung	
	Geräte exportieren	CC-Setup und -Steuerung und Geräte-, Port- und	

Menü > Untermenü	Menüelement	Erforderliche Berechtigung	Beschreibung
		Knotenverwaltung	
	Power IQ-Daten exportieren	CC-Setup und -Steuerung und Geräte-, Port- und Knotenverwaltung	
Systemwartung			
	Sicherungsknoten	CC Setup And Control	
	Wiederherstellen	CC Setup And Control	
	Zurücksetzen	CC Setup And Control	
	Neu starten	CC Setup And Control	
	Aktualisieren	CC Setup And Control	
	Herunterfahren	CC Setup And Control	
> Wartungsmodus	> Wartungsmodus starten	CC Setup And Control	
	> Wartungsmodus beenden	CC Setup And Control	
Ansicht		Keine*	
Fenster		Keine*	
Hilfe		Keine*	

Anhang D SNMP-Traps

CC-SG stellt die folgenden SNMP-Traps bereit:

SNMP-Trap	Beschreibung
ccUnavailable	Die CC-SG-Anwendung ist nicht verfügbar.
ccAvailable	Die CC-SG-Anwendung ist verfügbar.
ccUserLogin	Ein Benutzer hat sich bei CC-SG angemeldet.
ccUserLogout	Ein Benutzer hat sich bei CC-SG abgemeldet.
ccPortConnectionStarted	CC-SG-Sitzung wurde gestartet.
ccPortConnectionStopped	CC-SG-Sitzung wurde angehalten.
ccPortConnectionTerminated	CC-SG-Sitzung wurde beendet.
ccImageUpgradeStarted	CC-SG-Abbildaktualisierung wurde gestartet.
ccImageUpgradeResults	Ergebnisse der CC-SG-Abbildaktualisierung.
ccUserAdded	Neuer Benutzer wurde zu CC-SG hinzugefügt.
ccUserDeleted	Benutzer wurde aus CC-SG gelöscht.
ccUserModified	Ein CC-SG-Benutzer wurde bearbeitet.
ccUserAuthenticationFailure	CC-SG-Fehler bei der Benutzerauthentifizierung.
ccLanCardFailure	CC-SG hat einen LAN-Kartenfehler erkannt.
ccHardDiskFailure	CC-SG hat einen Festplattenfehler erkannt.
ccLeafNodeUnavailable	CC-SG hat einen Verbindungsfehler zu einem Endknoten erkannt.
ccLeafNodeAvailable	CC-SG hat einen verfügbaren Endknoten erkannt.
ccIncompatibleDeviceFirmware	CC-SG hat ein Gerät mit inkompatibler Firmware erkannt.
ccDeviceUpgrade	CC-SG hat die Firmware auf einem Gerät aktualisiert.
ccEnterMaintenanceMode	CC-SG befindet sich im Wartungsmodus.
ccExitMaintenanceMode	CC-SG hat den Wartungsmodus verlassen.
ccUserLockedOut	CC-SG-Benutzer wurde gesperrt.
ccDeviceAddedAfterCCNOCNotification	CC-SG hat ein Gerät nach einer Benachrichtigung von CC-NOC hinzugefügt.
ccScheduledTaskExecutionFailure	Der Grund, warum eine geplante Aufgabe nicht durchgeführt werden konnte.

SNMP-Trap	Beschreibung
ccDiagnosticConsoleLogin	Benutzer hat sich in der CC-SG-Diagnosekonsole angemeldet.
ccDiagnosticConsoleLogout	Benutzer hat sich von der CC-SG-Diagnosekonsole abgemeldet.
ccUserGroupAdded	Eine neue Benutzergruppe wurde CC-SG hinzugefügt.
ccUserGroupDeleted	CC-SG-Benutzergruppe wurde gelöscht.
ccUserGroupModified	CC-SG-Benutzergruppe wurde bearbeitet.
ccSuperuserNameChanged	CC-SG-Superuser-Benutzername wurde geändert.
ccSuperuserPasswordChanged	CC-SG-Superuser-Kennwort wurde geändert.
ccLoginBannerChanged	CC-SG-Anmeldebanner wurde geändert.
ccMOTDChanged	CC-SG-Tipp des Tages wurde geändert.
ccDominionPXReplaced	Ein Dominion PX-Gerät wurde durch ein anderes Dominion PX-Gerät ersetzt.
ccSystemMonitorNotification	CC-SG hat nicht genügend Speicher.
ccNeighborhoodActivated	Die CC-SG-Netzwerkumgebung wurde aktiviert.
ccNeighborhoodUpdated	Die CC-SG-Netzwerkumgebung wurde aktualisiert.
ccDominionPXFirmwareChanged	Eine Dominion PX-Firmwareversion wurde geändert.
ccClusterFailover	Beim primären CC-SG-Knoten trat ein Fehler auf, und der CC-SG-Sicherungsknoten ist nun als primärer CC-SG-Knoten betriebsbereit.
ccClusterBackupFailed	Beim CC-SG-Sicherungsknoten trat ein Fehler auf.
ccClusterWaitingPeerDetected	Der primäre CC-SG-Knoten stellte einen Peer im Wartemodus fest.
ccClusterOperation	Ein Clustervorgang wurde ausgeführt.
ccCSVFileTransferred	Eine CSV-Datei wurde importiert.
ccPIQAvailable	CC-SG hat festgestellt, dass Power IQ verfügbar ist.
ccPIQUnavailable	CC-SG hat festgestellt, dass Power IQ nicht verfügbar ist.

Anhang E CSV-Dateiimporte

Dieser Abschnitt enthält weitere Informationen zu CSV-Dateiimporten.

In diesem Kapitel

Häufige Anforderungen für CSV-Dateien 434
Einträge in der Überwachungsliste für Importe 435
Problembehebung bei CSV-Dateien 436

Häufige Anforderungen für CSV-Dateien

Wenn Sie eine CSV-Datei erstellen möchten, empfehlen wir Ihnen, eine Datei aus CC-SG zu exportieren und diese exportierte CSV-Datei anschließend als Muster zum Erstellen Ihrer eigenen Datei zu nutzen. In der Exportdatei sind als erstes Kommentare enthalten, die jedes Element in der Datei beschreiben. Die Kommentare können als Anweisungen zum Erstellen einer Datei oder zum Importieren verwendet werden.

Es wird empfohlen, die Importdatei in einem Tabellenkalkulationsprogramm wie Microsoft Excel zu erstellen. Geben Sie jedes Element in eine eigene Zelle ein. Wenn Sie die Datei speichern, wählen Sie CSV als Dateityp aus. Dadurch werden am Ende jeder Zelle automatisch Kommas als Trennzeichen eingefügt, sodass die Daten in durch Kommas getrennte Spalten eingeteilt werden. Sie können die CSV-Datei in einem Texteditor bearbeiten, dann müssen Sie allerdings nach jedem Element manuell Kommas einfügen.

Wenn Sie die Datei zum ersten Mal in Excel speichern, wählen Sie "Speichern unter" und STELLEN SIE SICHER, dass Sie CSV als Dateityp auswählen. Anschließend speichert Excel die Datei automatisch als CSV-Datei.

Wenn Sie den Dateityp nicht korrekt festlegen, wird die Datei beschädigt und kann nicht für den Import verwendet werden.

- Alle Importdateien müssen über das ASCII-Textformat verfügen.
- Die erste Spalte jeder Zeile muss den Befehl `ADD` (Hinzufügen) beinhalten. Die Grundstruktur lautet "Befehl, Tag, Attribut", wobei `ADD` (Hinzufügen) der Befehl ist.
- Spaltennamen werden nicht unterstützt. Sie können Kommentarzeilen oberhalb der Datenzeilen einfügen, solange jede Zeile mit dem Symbol `#` beginnt.
- Um für ein Feld den Standardwert zu verwenden, geben Sie den Wert ein oder lassen Sie das Feld leer.
- Weitere Informationen zu den Regeln, die von CC-SG für die Länge von Namen verwendet werden, finden Sie unter ***Benennungskonventionen*** (siehe "***Benennungsregeln***" auf Seite 457).
- Wenn sie die CSV-Datei in einem Texteditor und nicht in einem Tabellenkalkulationsprogramm erstellen, müssen Sie Kommas und doppelte Anführungszeichen auf andere Weise verwenden. Ein Wert, der ein Komma oder doppelte Anführungszeichen enthält, muss von doppelten Anführungszeichen umschlossen sein. Jedem Zeichen mit doppelten Anführungszeichen innerhalb des Werts muss ebenso ein doppeltes Anführungszeichen vorangestellt sein.

  Beispiel:

Wert mit Sonderzeichen	Formatiert für CSV-Datei
GerätA,B	"GerätA,B"
Gerät"A"	"Gerät""A"""

Einträge in der Überwachungsliste für Importe

Jedes in CC-SG importierte Element wird in die Überwachungsliste eingetragen. Übersprungene Duplikate werden nicht in der Überwachungsliste aufgeführt.

Die folgenden Aktionen werden in der Überwachungsliste unter dem Meldungstyp "Konfiguration" aufgezeichnet.

- CSV-Dateiimport gestartet
- CSV-Dateiimport abgeschlossen, einschließlich Anzahl an erfolgreich hinzugefügten Datensätzen, fehlgeschlagenen Datensätzen und Duplikaten, die ignoriert wurden.

Alle Änderungen, die beim Importieren von Datensätzen auftreten, werden in der Überwachungsliste aufgezeichnet. Diese Einträge erscheinen zwischen den Einträgen für "Import gestartet" und "Import abgeschlossen". Sie werden abhängig vom Importtyp unter einem anderen Meldungstyp gespeichert.

- Benutzerimporte werden unter "Benutzerverwaltung" aufgezeichnet.
- Geräteimporte werden unter "Gerät/Knoten/Port" aufgezeichnet.
- Knotenimporte werden unter "Gerät/Knoten/Port" aufgezeichnet.
- Kategorieimporte werden unter "Konfiguration" aufgezeichnet.
- Powerstrip-Importe werden unter "Gerät/Knoten/Port" aufgezeichnet.

Um alle den Import betreffenden Einträge anzuzeigen, filtern Sie auf der Seite der Überwachungsliste nach Datum und Uhrzeit.

Für jeden importierten Datensatz können mehrere Einträge in der Überwachungsliste vorgenommen worden sein.

Problembehebung bei CSV-Dateien

So beheben Sie Fehler bei der CSV-Dateivalidierung:

Im Problembereich der Importseite werden Fehlermeldungen angezeigt. Durch die Fehlermeldungen werden Probleme angezeigt, die während der Validierung in der CSV-Datei gefunden wurden.

Sie können die Fehlerliste als CSV-Datei speichern.

Jeder Fehler enthält die Zeilennummer der CSV-Datei, in der der Fehler aufgetreten ist.

Die Kommentare oben in den Exportdateien unterstützen Sie dabei, die Fehler zu korrigieren. Wenn die Datei korrigiert wurde, validieren Sie sie erneut.

So beheben Sie Fehler beim CSV-Dateiimport:

Im Problembereich der Importseite werden Warn- und Fehlermeldungen angezeigt, die Sie auf Probleme beim Import hinweisen.

Wenn ein Fehler angezeigt wird, wurden die Daten in dieser Zeile der Datei nicht importiert.

Doppelte Einträge werden nicht importiert und werden nicht in der Überwachungsliste angezeigt.

- Wenn Sie CC-SG von Ihrem Webbrowser aus starten, benötigen Sie ein Java-Plug-in. Wenn Ihr Gerät eine falsche Version verwendet, werden Sie von CC-SG durch die entsprechenden Installationsschritte geführt. Verfügt Ihr Computer nicht über ein Java-Plug-in, kann CC-SG nicht automatisch gestartet werden. In dem Fall müssen Sie Ihre alte Java-Version deinstallieren oder deaktivieren und für einwandfreien Betrieb die Konnektivität über einen seriellen Port zu CC-SG herstellen.
- Wird CC-SG nicht geladen, überprüfen Sie die Webbrowsereinstellungen.
  - Überprüfen Sie, dass im Internet Explorer Java (Sun) aktiviert ist.
  - Öffnen Sie das Java-Plug-in über die Systemsteuerung, und passen Sie die Einstellungen für Ihren Browser an.
- Treten beim Hinzufügen von Geräten Probleme auf, überprüfen Sie, ob diese Geräte mit den korrekten Firmwareversionen ausgestattet sind.
- Wird das Netzwerkschnittstellenkabel zwischen dem Gerät und CC-SG getrennt, warten Sie den Zeitraum der konfigurierten Heartbeat-Minuten ab, bevor Sie das Netzwerkschnittstellenkabel erneut anschließen. Während des konfigurierten Heartbeat-Zeitraums wird das Gerät im eigenständigen Modus betrieben, und der Zugriff ist über RRC, MPC oder RC möglich.
- Wenn Sie eine Fehlermeldung erhalten, dass Ihre Clientversion von der Serverversion abweicht und das Verhalten ggf. unvorhersehbar ist, sollten Sie den Browser-Cache und den Java-Cache löschen und den Browser neu starten. Weitere Informationen finden Sie unter ***Browser-Cache löschen*** (auf Seite 275) und ***Java-Cache löschen*** (auf Seite 275).
- Wenn Sie den Internet Explorer verwenden und beim Zugriff über die MPC-Schnittstelle auf einen KX2-Port Probleme auftreten, löschen Sie den Cache-Speicher des Browsers, und greifen Sie erneut auf den Port zu. Siehe ***Browser-Cache löschen*** (auf Seite 275).
- Wenn die Speicherauslastung erheblich zunimmt oder die Browsersitzung nicht mehr auf Ihre Aktionen reagiert, müssen Sie möglicherweise die Java-Heap-Größe für den Client erhöhen.
  a. Öffnen Sie das Java-Plug-in in der Systemsteuerung.
  b. Klicken Sie auf die Registerkarte "Java".
  c. Klicken Sie auf "Anzeigen" im Gruppenfeld "Java-Applet-Laufzeiteinstellungen".

d. Wählen Sie die Zeile der aktuellen Java-Version, die Sie verwenden, und geben Sie in der Spalte "Java Runtime-Parameter" `-Xmx<Größe>m` ein. Geben Sie z. B. `-Xmx300m` ein, wenn Sie die Java-Heap-Größe auf maximal 300 MB erhöhen möchten.

Es wird empfohlen, die Java-Heap-Größe nicht höher als die Hälfte der Speicherkapazität des Clientcomputers einzustellen. Wenn der Clientcomputer beispielsweise über einen RAM-Speicher von 1,0 GB verfügt, setzen Sie den Parameter auf maximal `-Xmx512m`.

- Wenn Sie über denselben Client und unter Verwendung von Firefox auf mehr als eine CC-SG-Einheit zugreifen, wird möglicherweise eine Meldung angezeigt, dass die sichere Verbindung fehlgeschlagen ist. Dies bedeutet, dass Sie über ein ungültiges Zertifikat verfügen. Löschen Sie das ungültige Zertifikat vom Browser und versuchen Sie es erneut.

  a. Wählen Sie in Firefox "Extras > Einstellungen".

  b. Klicken Sie auf "Erweitert".

  c. Öffnen Sie die Registerkarte "Verschlüsselung".

  d. Klicken Sie auf "Zertifikate anzeigen" und suchen Sie "Raritan" in der Liste.

  e. Wählen Sie das Element "CommandCenter" aus und klicken Sie auf "Löschen". Klicken Sie zum Bestätigen auf OK.

Anhang G Diagnoseprogramme

CC-SG enthält einige Diagnoseprogramme, die für Sie oder den technischen Support von Raritan sehr hilfreich sind, um die Ursache von CC-SG-Problemen zu analysieren und die Fehler zu beheben.

In diesem Kapitel

Speicherdiagnose 439
Debug-Modus 440
CC-SG-Laufwerksüberwachung 441

Speicherdiagnose

CC-SG enthält das Diagnoseprogramm "Memtest86+", das über das Menü "GRUB" aufgerufen wird. Führen Sie bei Speicherproblemen den Diagnosetest "Memtest86+" für die Problembehandlung aus.

1: Führen Sie das Diagnoseprogramm "Memtest86+" aus:

1. Starten Sie CC-SG neu. Siehe ***CC-SG mit der Diagnosekonsole neu starten*** (siehe "***CC-SG mit der Diagnosekonsole neu hochfahren***" auf Seite 376).
2. Wenn die folgende Meldung angezeigt wird, drücken Sie innerhalb von fünf Sekunden eine beliebige Taste, um das Menü "GRUB" aufzurufen, wie z. B. Esc oder eine Pfeiltaste.

   ```
   Press any key to enter the menu (Drücken Sie eine
   beliebige Taste, um das Menü aufzurufen)
   ```

   ```
   Booting CentOS (x.x.x) in x seconds.... (Boote CentOS
   (x.x.x) in x Sekunden....)
   ```
3. Markieren Sie mit den Pfeiltasten nach oben oder unten die Option "Memtest86+ vX.X" (wobei vX.X die aktuelle Version ist), und drücken Sie die Eingabetaste.
4. CC-SG lädt das Diagnoseprogramm "Memtest86+" und führt es aus. Lassen Sie das Programm mindestens einmal vollständig durchlaufen, d. h. bis in der Spalte "Pass" (Durchlauf) die Zahl "1" angezeigt wird. Um einen ausführlichen Test auszuführen, lassen Sie das Programm über mehrere Stunden oder sogar über Nacht durchlaufen.
5. Überprüfen Sie diese Elemente, um festzustellen, ob Speicherfehler vorliegen.
   - Speicher: Die Größe des Gesamtspeichers muss mit Ihrem CC-SG-Typ übereinstimmen: 512 MB für G1, 2048 MB für V1 und 4096 MB für E1.
   - Fehler: Die Spalte muss "0" anzeigen.

- Fehlerfensterbereich: Der Bereich befindet sich unten direkt unterhalb der Zeile "WallTime". Wenn in diesem Bereich nichts angezeigt wird, liegen keine Fehler vor.

Wenn eines dieser Elemente auf Speicherfehler hinweist, können Sie Folgendes ausführen:

- Nehmen Sie den Bildschirm "Memtest86+" mit den Speicherfehlern auf, und kontaktieren Sie den technischen Support von Raritan.
- Fahren Sie CC-SG herunter, und installieren Sie die DIMM-Speichermodule neu, um sicherzustellen, dass der Kontakt ordnungsgemäß vorhanden ist. Führen Sie anschließend die Diagnose "Memtest86+" aus, um zu prüfen, ob der Fehler behoben ist.

2: Beenden Sie das Diagnoseprogramm "Memtest86+":

1. Drücken Sie die Esc-Taste.
2. CC-SG wird zurückgesetzt und neu gestartet.

Debug-Modus

Obwohl das Aktivieren des Debug-Modus für die Problembehandlung äußerst sinnvoll ist, kann sich dies auf den Betrieb und die Leistung des CC-SG auswirken. Daher dürfen Sie **den Debug-Modus nur aktivieren, wenn Sie vom technischen Support von Raritan dazu aufgefordert werden.** Deaktivieren Sie den Debug-Modus, nachdem die Problembehandlung abgeschlossen ist.

1: Aktivieren Sie den Debug-Modus:

1. Verwenden Sie einen unterstützten Internetbrowser, und geben Sie folgenden URL ein: `http(s)://<IP-Adresse>:8080/jmx-console/`, wobei `<IP-Adresse>` für die IP-Adresse von CC-SG steht. Beispiel: `https://10.20.3.30:8080/jmx-console/`.
2. Geben Sie "admin" in das Feld "Benutzername" ein.
3. Geben Sie das Kennwort des Superusers in das Feld "Kennwort" ein.
4. Führen Sie einen Bildlauf durch, bis `com.raritan.cc.bl.logger` angezeigt wird.
5. Klicken Sie auf diesen Hyperlink: `service=LoggerService`. Auf dem Bildschirm wird eine Liste mit Debug-Optionen angezeigt.
6. Ändern Sie den Wert der Debug-Option entsprechend der Aufforderung des technischen Supports von Raritan von INFO in DEBUGGEN.

7. Klicken Sie unten im Fenster auf "Apply Changes" (Änderungen anwenden).
8. Reproduzieren Sie das Problem, und nehmen Sie einen Schnappschuss auf. Siehe ***Systemschnappschuss aufnehmen*** (auf Seite 396).

2: Deaktivieren Sie den Debug-Modus:

1. Öffnen Sie das Fenster mit den Debug-Optionen, indem Sie die ersten vier Schritte des vorherigen Abschnitts ausführen.
2. Ändern Sie die Wert der Debug-Option von DEBUGGEN in INFO.
3. Klicken Sie unten im Fenster auf "Apply Changes" (Änderungen anwenden).

CC-SG-Laufwerksüberwachung

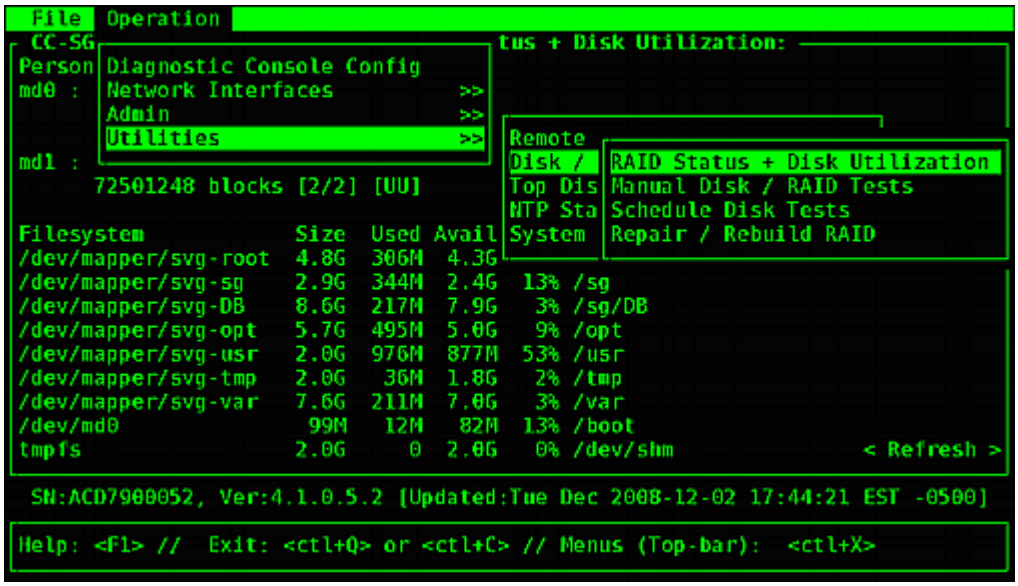
Wenn die CC-SG-Laufwerkskapazität in mindestens einem Dateisystem ausgeschöpft ist, kann sich dies negativ auf den Betrieb auswirken und sogar zum Verlust von einigen Technikdaten führen. Deshalb müssen Sie die CC-SG-Laufwerksauslastung überwachen und die erforderlichen Maßnahmen zum Vermeiden oder Lösen potenzieller Probleme anwenden. Sie können die Laufwerksüberwachung entweder über die Diagnosekonsole oder über den Webbrowser ausführen. Ein erfahrener Benutzer kann auch die gkrellm-Remoteüberwachung verwenden. Siehe ***Überwachung des Remotesystems konfigurieren*** (auf Seite 385).

Wichtig: Für CC-SG-Einheiten in einer Clusterkonfiguration müssen Sie beide CC-SG-Einheiten überwachen.

So überwachen Sie die Laufwerkskapazität über die Diagnosekonsole:

1. Melden Sie sich bei der Diagnosekonsole an, und rufen Sie die Seite "Disk Status" (Festplattenstatus) auf. Siehe ***RAID-Status und Laufwerksauslastung anzeigen*** (auf Seite 387).
2. Prüfen Sie die Informationen für das Laufwerk, und wenden Sie gegebenenfalls die erforderlichen Maßnahmen an.
   - Beide RAID-Partitionen müssen als [UU] und nicht als [U_] oder [_U] angezeigt werden. Andernfalls wird ein Laufwerksfehler angezeigt, und Sie müssen den technischen Support von Raritan kontaktieren.

- Die Werte `Use%` (Verwenden%) der Dateisysteme (fünfte Spalte im Bildschirm) dürfen nicht größer als 50 % sein. Verschiedene Dateisysteme enthalten unterschiedliche Daten, für die unterschiedliche Maßnahmen erforderlich sind.



Dateisystem	Daten	Maßnahme
/sg/DB	CC-SG-Datenbank	Wenden Sie sich an den technischen Support von Raritan.
/opt	CC-SG-Sicherungen und Schnappschüsse	1. Speichern Sie neue Schnappschussdateien auf einem Remote-Client-PC. Informationen zum Abrufen finden Sie unter ***Systemschnappschuss aufnehmen*** (auf Seite 396). 2. Rufen Sie das Menü "System Snapshot" (Systemschnappschuss) auf. Siehe ***Systemschnappschuss aufnehmen*** (auf Seite 396). 3. Wählen Sie den Bereich "Pre-Clean-up SNAP" (Bereinigen SNAP) aus. 4. Wählen Sie den Bereich "Pre-Clean-up UPLOAD" (Bereinigen UPLOAD) aus. 5. Deaktivieren Sie "SNAP". 6. Deaktivieren Sie "Package (Paket) & Export (Export)". 7. Klicken Sie auf "Submit" (Übertragen), oder wählen Sie dies aus. 8. Wenn die Speicherprobleme weiterhin auftreten, verwenden Sie den Administrations-Client, um sich bei CC-SG anzumelden, die CC-SG-Sicherungen auf einen Client-PC zu laden und sie anschließend von

Dateisystem	Daten	Maßnahme
		CC-SG zu löschen.
/var	Protokolldateien und Systemaktualisierungen	Wenden Sie sich an den technischen Support von Raritan.
/tmp	Bereich "Scratch" (Temp) (wird von Schnappschüssen verwendet)	1. Rufen Sie das Menü "System Snapshot" (Systemschnappschuss) auf. Siehe ***Systemschnappschuss aufnehmen*** (auf Seite 396). 2. Deaktivieren Sie "SNAP". 3. Deaktivieren Sie "Package (Paket) & Export (Export)". 4. Wählen Sie "Clean-up /tmp" (Bereinigen /tmp). 5. Klicken Sie auf "Submit" (Übertragen), oder wählen Sie dies aus.

So überwachen Sie die Laufwerkskapazität über den Webbrowser:

Diese Vorgehensweise ist nur für CC-SG Version 4.0 oder höher möglich. Sie müssen die Optionen für die Webstatuskonsole in der Diagnosekonsole aktivieren, bevor Sie die Laufwerkskapazität mithilfe des Webbrowsers aktivieren können. Siehe ***Auf die Statuskonsole über den Webbrowser zugreifen*** (auf Seite 355).

1. Verwenden Sie einen unterstützten Internetbrowser, und geben Sie folgenden URL ein: `http(s)://<IP-Adresse>/status/`, wobei `<IP-Adresse>` für die IP-Adresse von CC-SG steht. Der Schrägstrich (/) nach "/status" ist obligatorisch. Beispiel: `https://10.20.3.30/status/`.
2. Es wird eine Statusseite geöffnet. Diese Seite enthält dieselben Informationen wie die Statuskonsole.
3. Klicken Sie unten auf der Seite unterhalb von "Evaluation" (Bewerten) auf "CC-SG Monitors" (CC-SG-Monitore).
4. Prüfen Sie die Informationen für das Laufwerk, und wenden Sie gegebenenfalls die erforderlichen Maßnahmen an. Weitere Informationen finden Sie im vorherigen Abschnitt.

Hinweis: Wenden Sie sich an den technischen Support von Raritan, wenn Dateisystemprobleme auftreten, die nicht in diesem Abschnitt beschrieben werden, oder wenn die Probleme nicht mithilfe der erforderlichen Maßnahme gelöst werden können.

Anhang H Zwei-Faktoren-Authentifizierung

CC-SG kann so konfiguriert werden, dass es auf einen RSA RADIUS-Server zeigt, der die Zwei-Faktoren-Authentifizierung über einen verknüpften RSA-Authentifizierungsmanager unterstützt. CC-SG funktioniert wie ein RADIUS-Client und sendet die Benutzerauthentifizierungsanfragen an den RSA RADIUS-Server. Die Authentifizierungsanfrage umfasst die Benutzer-ID, ein festgelegtes Kennwort und einen Code für den dynamischen Token.

In diesem Kapitel

Unterstützte Umgebungen für die Zwei-Faktoren-Authentifizierung 444
Setupanforderungen für die Zwei-Faktoren-Authentifizierung 444
Bekannte Probleme bei der Zwei-Faktoren-Authentifizierung.....445

Unterstützte Umgebungen für die Zwei-Faktoren-Authentifizierung

Die folgenden Komponenten der Zwei-Faktoren-Authentifizierung funktionieren mit CC-SG.

- RSA RADIUS Server 6.1 unter Windows Server 2003
- RSA Authentication Manager 6.1 unter Windows Server 2003
- RSA Secure ID SID700 Hardware Token

Frühere RSA-Produktversionen sollten auch mit CC-SG funktionieren, dies wurde jedoch noch nicht getestet.

Setupanforderungen für die Zwei-Faktoren-Authentifizierung

Die folgenden Aufgaben müssen für ein Zwei-Faktoren-Authentifizierungs-Setup abgeschlossen werden. Weitere Informationen finden Sie in der RSA-Dokumentation.

1. Token importieren
2. CC-SG-Benutzer erstellen und Token dem Benutzer zuordnen
3. Benutzerkennwort erstellen
4. Agent Host für den RADIUS-Server erstellen
5. Agent Host (Typ: Kommunikationsserver) für CC-SG erstellen.
6. RADIUS CC-SG-Client erstellen

Bekannte Probleme bei der Zwei-Faktoren-Authentifizierung

Der Modus RSA RADIUS „New PIN“, der ein Herausforderungskennwort/PIN erfordert, funktioniert nicht. Benutzern in diesem Schema müssen stattdessen festgelegte Kennwörter zugeordnet werden.

Anhang I Häufig gestellte Fragen (FAQs)

In diesem Kapitel

Allgemeine häufig gestellte Fragen (FAQs) 446
Häufig gestellte Fragen (FAQs) zur Authentifizierung.....449
Häufig gestellte Fragen (FAQs) zur Sicherheit.....449
Häufig gestellte Fragen (FAQs) zu Konten 451
Häufig gestellte Fragen (FAQs) zur Leistung 451
Häufig gestellte Fragen (FAQs) zu Gruppen.....452
Häufig gestellte Fragen (FAQs) zur Interoperabilität.....453
Häufig gestellte Fragen (FAQs) zur Autorisierung 453
Häufig gestellte Fragen (FAQs) zur Benutzerfreundlichkeit.....453
Häufig gestellte Fragen zur Lizenzierung.....455

Allgemeine häufig gestellte Fragen (FAQs)

Frage	Antwort
Allgemein	
Was ist CC-SG?	CC-SG ist ein Netzwerkverwaltungsgerät zum Aggregieren und Integrieren mehrerer in einem Rechenzentrum implementierter Server und Netzwerkgeräte, die an einem IP-fähigen Raritan-Gerät angeschlossen sind.
Wozu kann ich CC-SG einsetzen?	Mit zunehmender Anzahl an Servern und Geräten im Rechenzentrum wird deren Verwaltung immer komplexer. CC-SG ermöglicht dem Systemadministrator über nur ein Gerät auf alle Server, Geräte und Benutzer zuzugreifen und diese zu verwalten und anzuzeigen.
Welche Raritan-Produkte unterstützt CC-SG?	Weitere Informationen finden Sie in der Kompatibilitätsmatrix auf der Raritan-Website im Abschnitt "Support" unter "Firmware und Dokumentation".
Wie wird CC-SG in andere Raritan-Produkte integriert?	CC-SG verwendet eine einmalige und proprietäre Such- und Erkennungstechnologie zum Herstellen einer Verbindung mit ausgewählten Raritan-Geräten mit bekannten Netzwerkadressen. Nach der Verbindungsherstellung und Konfiguration von CC-SG erhalten Sie eine transparente Übersicht über alle an CC-SG angeschlossenen Geräte, die leicht betrieben und verwaltet werden können.

Frage	Antwort
Wird der Status von CC-SG durch den Status der Geräte beschränkt, für die es als Proxy eingesetzt wird?	Nein. Da die CC-SG-Software auf einem dedizierten Server ausgeführt wird, haben Sie auch dann Zugriff auf CC-SG, wenn ein Gerät ausgeschaltet ist, für das CC-SG als Proxy fungiert.
Kann ich auf neuere Versionen der CC-SG-Software aktualisieren, wenn sie erhältlich sind?	Ja. Wenden Sie sich hierzu an einen Raritan-Vertriebsmitarbeiter oder direkt an Raritan, Inc.
Wie viele Knoten und/oder Dominion- und/oder IP-Reach-Geräte können an CC-SG angeschlossen werden?	Für die Anzahl an Knoten und/oder Dominion- und/oder IP-Reach-Geräten, die an CC-SG angeschlossen werden können, gibt es keinen festgelegten Höchstwert. Allerdings können auch nicht unendlich viele Ports/Geräte angeschlossen werden. Die Leistung des Prozessors und der Arbeitsspeicher des Hostservers bestimmen, wie viele Knoten tatsächlich angeschlossen werden können.
Wie gehe ich vor, wenn ich CC-SG keinen Konsolenport/seriellen Port hinzufügen kann?	Wenn das Konsolengerät/serielle Gerät ein Dominion-Produkt ist, stellen Sie Folgendes sicher: - Das Dominion-Gerät ist aktiviert. - Die maximale Anzahl konfigurierter Benutzerkonten für das Dominion-Gerät wurde noch nicht erreicht.
Welche Java-Version unterstützt Raritan CC-SG?	Weitere Informationen finden Sie in der Kompatibilitätsmatrix auf der Raritan-Website im Abschnitt "Support" unter "Firmware und Dokumentation".
Ein Administrator hat der CC-SG-Datenbank einen neuen Knoten hinzugefügt und mir diesen Knoten zugeordnet. Wie kann ich den Knoten in meiner Knotenstruktur anzeigen?	Klicken Sie auf der Symbolleiste auf die Schaltfläche "Aktualisieren", um die Struktur zu aktualisieren und den neu zugewiesenen Knoten anzuzeigen. Vergessen Sie nicht, dass beim Aktualisieren von CC-SG alle derzeitigen Konsolensitzungen geschlossen werden.
Inwiefern wird der Windows-Desktop in Zukunft unterstützt?	Der Zugriff auf CC-SG von außerhalb der Firewall wird durch Konfigurieren der richtigen Ports an der Firewall ermöglicht. Die folgenden Ports sind Standardports: 80: für HTTP-Zugriff über einen Webbrowser 443: für HTTPS-Zugriff über einen Webbrowser 8080: für den CC-SG-Serverbetrieb

Frage	Antwort
	2400: für Verbindungen im Proxymodus 5001: für IPR-/DKSX-/DKX-/P2-SC-Ereignisbenachrichtigung Wenn sich zwischen zwei Clusterknoten eine Firewall befindet, sollten die folgenden Ports für den problemlosen Betrieb des Clusters geöffnet werden: 8732: für den Clusterknotenheartbeat 5432: für Clusterknoten-DB-Replikation
Welche Richtlinien gelten für den Entwurf umfangreicher Systeme? Sind Beschränkungen oder Voraussetzungen vorhanden?	Raritan bietet zwei Modelle für die Serverskalierbarkeit: das Rechenzentrummodell und das Netzwerkmodell. Das Rechenzentrummodell verwendet Paragon zum Skalieren auf Tausende von Systemen in einem Rechenzentrum. Dies ist die effektivste und kostengünstigste Methode zum Skalieren eines einzelnen Standorts. Diese Methode unterstützt auch das Netzwerkmodell mit IP-Reach und der IP-Benutzerstation (UST-IP). Das Netzwerkmodell skaliert mittels TCP/IP-Netzwerk und aggregiert den Zugriff über CC-SG, weshalb die Benutzer weder IP-Adressen noch die Topologie von Zugriffsgeräten kennen müssen. Außerdem ist nur eine Anmeldung erforderlich.
Erkennt CC-SG die Blade-Chassis-Konfiguration automatisch und wird sie automatisch aktualisiert, wenn ich das Blade-Chassis von einem KX2-Port zu einem anderen KX2-Port verschiebe?	Wenn Sie das Blade-Chassis zu einem anderen KX2-Port oder Gerät verschieben, erkennt CC-SG deren Konfiguration nicht automatisch und aktualisiert sie auch nicht. Die Konfiguration ist nicht mehr vorhanden. Sie müssen das Blade-Chassis in CC-SG erneut konfigurieren.
Wie führe ich den Blade-Server-Knoten und den virtuellen Hostknoten zusammen, wenn sie auf denselben Server verweisen?	Konfigurieren Sie die Virtualisierungsfunktion, bevor Sie die Blade-Slots konfigurieren. Geben Sie beim Konfigurieren des Blade-Slots den Namen des virtuellen Hostknotens ein, und fügen Sie diese Schnittstelle zum vorhandenen Knoten hinzu, wenn die entsprechende Meldung angezeigt wird.

Häufig gestellte Fragen (FAQs) zur Authentifizierung

Frage	Antwort
Authentifizierung	
Wie viele Benutzerkonten können für CC-SG erstellt werden?	Überprüfen Sie die Bestimmungen in Ihrer Lizenz. Für die Anzahl an Benutzerkonten, die für CC-SG erstellt werden können, liegt keine festgelegte Beschränkung vor. Es kann jedoch auch keine unbegrenzte Anzahl an Konten erstellt werden. Die Größe der Datenbank, die Leistung des Prozessors und der Arbeitsspeicher des Hostservers beeinflussen die Anzahl der Benutzerkonten, die erstellt werden können.
Kann ich einem bestimmten Benutzer einen spezifischen Knotenzugriff zuordnen?	Ja, wenn Sie Administratorberechtigungen besitzen. Administratoren haben die Möglichkeit, jedem Benutzer bestimmte Knoten zuzuordnen.
Wie erfolgt die Verwaltung bei mehr als 1000 Benutzern? Wird Active Directory unterstützt?	CC-SG ist mit Microsoft Active Directory, Sun iPlanet oder Novell eDirectory kompatibel. Ist ein Benutzerkonto bereits auf einem Authentifizierungsserver vorhanden, unterstützt CC-SG die Remoteauthentifizierung mittels AD/TACACS+/RADIUS/LDAP.
Welche Optionen sind für die Authentifizierung mit Verzeichnisdiensten und Sicherheitstools verfügbar (z. B. LDAP, AD, Radius usw.)?	CC-SG lässt sowohl die lokale Authentifizierung als auch die Remoteauthentifizierung zu. Zu den unterstützten Remoteauthentifizierungsservern zählen: AD, TACACS+, RADIUS und LDAP.
Warum wird die Fehlermeldung "Benutzername und/oder Kennwort falsch" angezeigt, nachdem ich einen gültigen Benutzernamen und ein gültiges Kennwort für die Anmeldung bei CC-SG eingegeben habe?	Überprüfen Sie das Benutzerkonto in AD. Wenn AD so eingerichtet wurde, dass sich nur bestimmte Computer bei der Domäne anmelden können, können Sie sich nicht bei CC-SG anmelden. Löschen Sie in diesem Fall die Einschränkung "Logon To" (Anmelden bei) in AD.

Häufig gestellte Fragen (FAQs) zur Sicherheit

Frage	Antwort
Sicherheit	
Beim Anmelden wird	Bei jeder Anmeldung in CC-SG wird eine

Frage	Antwort
manchmal eine Meldung mit dem Hinweis angezeigt, dass die falschen Anmeldeinformationen verwendet worden seien, obwohl ich sicher bin, dass ich den korrekten Benutzernamen und das richtige Kennwort eingebe. Woran liegt das?	sitzungsspezifische ID gesendet. Diese ID verfügt über eine Timeoutfunktion. Wenn Sie sich nach diesem Timeout beim Gerät anmelden, ist die Sitzungs-ID ungültig. Wenn Sie bei gedrückter Umschalttaste auf den Befehl zum erneuten Laden klicken, wird die Seite von CC-SG aktualisiert. Sie können auch das aktuelle Browserfenster schließen, ein neues Browserfenster öffnen und sich dann erneut anmelden. Dieses Verfahren verbessert die Sicherheit, da die im Webcache gespeicherten Informationen nicht für den Zugriff auf die Einheit verwendet werden können.
Wie werden Kennwörter gesichert?	Kennwörter werden mittels MD5-Verschlüsselung, einem unidirektionalen Hash, verschlüsselt. Hierdurch erhalten sie zusätzliche Sicherheit, um den Zugriff nicht autorisierter Benutzer auf die Kennwortliste zu verhindern.
Manchmal wird beim Klicken auf ein beliebiges Menü in CC-SG der Hinweis angezeigt, dass ich nicht mehr angemeldet bin, nachdem ich meine Arbeitsstation eine Zeit lang nicht verwendet habe. Woran liegt das?	CC-SG misst die Zeit jeder Benutzersitzung. Findet während eines vordefinierten Zeitraums keine Aktivität statt, meldet CC-SG den Benutzer ab. Die konfigurierbare Länge dieses Zeitraums ist auf 60 Minuten voreingestellt. Es wird empfohlen, dass die Benutzer CC-SG nach Abschluss einer Sitzung beenden.
Da Raritan Stammzugriff auf den Server erhält, kann dies zu Schwierigkeiten mit Regierungsbehörden führen. Können Kunden ebenfalls Zugriff auf Stammebene erhalten, oder bietet Raritan eine Methode diesen Zugriff zu überprüfen oder für diesen Zugriff Verantwortung zu übernehmen?	Nachdem ein Gerät von Raritan, Inc. ausgeliefert wurde, hat niemand mehr Zugriff auf den Server.
Erfolgt die SSL-Verschlüsselung sowohl intern als auch extern (nicht nur WAN, sondern auch LAN)?	Sowohl intern als auch extern. Die Sitzung wird unabhängig von der Quelle (LAN/WAN) verschlüsselt.
Unterstützt CC-SG die CRL-Liste, d. h., die LDAP-Liste ungültiger Zertifikate?	Nein

Frage	Antwort
Unterstützt CC-SG Client Certificate Request?	Nein

Häufig gestellte Fragen (FAQs) zu Konten

Frage	Antwort
Kontoführung	
Die Ereigniszeiten im Überwachungslistenbericht scheinen nicht zu stimmen. Woran liegt das?	Die Protokollereigniszeiten werden gemäß den Zeiteinstellungen des Client-Computers protokolliert. Sie können die Zeit- und Datumseinstellungen des Computers anpassen.
Besteht die Möglichkeit festzustellen, wer einen Netzschalter ein- oder ausgeschaltet hat?	Das direkte Ausschalten des Netzschalters wird nicht protokolliert. Allerdings wird das Ein-/Ausschalten über CC-SG protokolliert.

Häufig gestellte Fragen (FAQs) zur Leistung

Frage	Antwort
Leistung	
Als CC-SG Administrator habe ich über 500 Knoten hinzugefügt und diese alle mir zugewiesen. Nun dauert das Anmelden bei CC-SG recht lange.	Wenn Sie sich als Administrator viele Knoten zugeordnet haben, lädt CC-SG beim Anmelden alle Knoteninformationen. Der Anmeldvorgang wird dadurch beträchtlich verlangsamt. Administratorkonten sollten in erster Linie zum Verwalten der Konfiguration von CC-SG verwendet werden. Diese Konten sollten nur Zugriff auf wenige Knoten haben.
Wie ist die Bandbreitennutzung pro Client?	Der Remotezugriff auf eine serielle Konsole über TCP/IP verursacht die gleiche Netzwerkaktivität wie eine telnet-Sitzung. Allerdings ist der Durchsatz auf die RS232-Bandbreite des Konsolenports plus SSL/TCP/IP-Overhead beschränkt. Der Raritan Remote Client (RRC) steuert den Remotezugriff auf eine KVM-Konsole. Diese Anwendung bietet eine konfigurierbare Bandbreite: von der LAN-Bandbreite bis zu einer für einen Remotebenutzer geeigneten Bandbreite.

Häufig gestellte Fragen (FAQs) zu Gruppen

Frage	Antwort
Gruppierung	
Kann ein bestimmter Server mehreren Gruppen hinzugefügt werden?	Ja. Genau so, wie ein Benutzer mehreren Gruppen angehören kann, kann auch ein Gerät mehreren Gruppen angehören. Beispiel: Eine Sun-Station in New York City kann den Gruppen Sun: „Betriebssystemtyp = Solaris“ und der Gruppe New York City: "Standort = NYC" angehören.
Welche andere Verwendung würde durch die aktive Verwendung des Konsolenports blockiert werden (z. B. einige UNIX-Varianten, die über Netzwerkschnittstellen keine Verwaltung zulassen)?	Eine Konsole gilt allgemein als sicherer und zuverlässiger Zugriffspfad. Einige UNIX-Systeme erlauben den Zugriff auf Stammebene nur an der Konsole. Aus Sicherheitsgründen verhindern andere Systeme u. U. mehrere Anmeldungen, weshalb Benutzern der Zugriff verweigert wird, wenn der Administrator angemeldet ist. Der Administrator kann außerdem, falls notwendig, die Netzwerkschnittstellen von der Konsole aus deaktivieren, um den gesamten anderen Zugriff zu blockieren. Die normale Eingabe von Befehlen an der Konsole hat keine andere Auswirkung als die Eingabe gleicher Befehle an jeder anderen Schnittstelle. Da die Konsolenanmeldung nicht vom Netzwerk abhängig ist, unterstützt ein überlastetes System, das auf eine Netzwerkanmeldung nicht mehr reagiert, trotzdem die Konsolenanmeldung. Ein weiterer Vorteil des Konsolenzugriffs sind die Problembehandlung und Diagnose bei System- und Netzwerkproblemen.
Wie sollte der Tausch von CIMS auf physischer Ebene mit Änderungen in der logischen Datenbank gehandhabt werden? Was passiert beispielsweise, wenn ich ein CIM mit Zielserver physisch von einem Port zu einem anderen bewege (entweder am selben Gerät oder an einem anderen Gerät)? Was geschieht mit den Portnamen? Was passiert mit dem Knoten? Was passiert mit den Schnittstellen?	Jedes CIM besitzt eine Seriennummer und einen Zielsystemnamen. Raritan-Systeme gehen davon aus, dass ein CIM am benannten Ziel angeschlossen bleibt, wenn seine Verbindung zwischen Switches verschoben wird. Dieses Verschieben wird automatisch bei den Ports und Schnittstellen in CC-SG berücksichtigt; der Portname und der Schnittstellenname wird aktualisiert, um die Änderung zu berücksichtigen. Die Schnittstelle erscheint unter dem Knoten, der mit dem Port verknüpft ist. Der Knotenname ändert sich jedoch nicht. Sie müssen den Knoten manuell umbenennen, indem Sie den Knoten bearbeiten. Dieses Szenario geht davon aus, dass alle betroffenen Ports bereits konfiguriert wurden. Wenn Sie den Zielserver und das CIM physisch zu einem anderen, nicht konfigurierten Port verschieben, können Sie den Port anschließend in

Frage	Antwort
	CC-SG konfigurieren, dann wird der Knoten automatisch erstellt.

Häufig gestellte Fragen (FAQs) zur Interoperabilität

Frage	Antwort
Interoperabilität	
Wie wird CC-SG in andere Blade Chassis-Produkte integriert?	CC-SG unterstützt jedes Gerät mit einer KVM-Schnittstelle oder seriellen Schnittstelle als transparentes Durchgangsgerät.
Bis zu welchem Grad ist CC-SG in KVM-Tools anderer Anbieter bis zur KVM-Port-Ebene oder Standardkonfigurationsebene integrierbar?	Die Integration in KVM-Switches von Drittanbietern erfolgt normalerweise über Tastaturmakros, wenn KVM-Drittanbieter die Kommunikationsprotokolle für diese Switches nicht veröffentlichen. Je nach Fähigkeiten der KVM-Switches von Drittanbietern variiert der Grad der Integration.
Wie kann ich die Beschränkung von vier gleichzeitigen Pfaden über ein IP-Reach-Gerät umgehen und eine 8-Pfad-Lösung realisieren?	Die beste derzeitige Implementierung ist das Aggregieren von IP-Reach-Geräten mit CC-SG. Raritan beabsichtigt, die gleichzeitigen Zugriffspfade pro Gerät in Zukunft zu erhöhen. Dieses Vorhaben befindet sich noch in der Entwicklungsphase, da andere Projekte Vorrang haben. Wir freuen uns jedoch über Anregungen zu Nachfrage und Verwendungsbeispielen einer 8-Pfad-Lösung.

Häufig gestellte Fragen (FAQs) zur Autorisierung

Frage	Antwort
Autorisierung	
Ist die Autorisierung über RADIUS/TACACS/LDAP möglich?	LDAP und TACACS werden nur zur Remoteauthentifizierung und nicht zur Autorisierung verwendet.

Häufig gestellte Fragen (FAQs) zur Benutzerfreundlichkeit

Frage	Antwort
Benutzerfreundlichkeit	
Bei der Konsolenverwaltung	Das Anmelden in CC-SG über die CC-SG-Konsole

Frage	Antwort
über Netzwerkports oder lokale serielle Ports (z. B. COM2): Was geschieht mit der Protokollierung? Erfasst CC-SG lokale Verwaltung?	gleicht dem Zuweisen der Stammberechtigung für das Betriebssystem (Linux), das im CC-SG ausgeführt wird. Syslog zeichnet diese Art von Ereignis auf. Die Benutzereingabe an der CC-SG-Konsole geht jedoch verloren.

Häufig gestellte Fragen zur Lizenzierung

Befolgen Sie die nachstehenden Regeln, wenn Sie Ihre installierten Lizenzen ersetzen müssen.

Basislizenzen müssen zuerst ersetzt werden.	Wenn Sie z. B. die eigenständigen Lizenzen CC-E1-51 CCL-512 durch die Clusterlizenzen CC-2XE1-512 und ersetzen, muss die Basislizenz CC-E1-512 vor der Add-On-Lizenz CCL-512 ersetzt werden. Während die Add-On-Funktion CCL-512 für die eigens Lizenz und die Clusterlizenz identisch ist, hätte die Liz eine Host-ID für die eigenständige Lizenz und zwei Ho die Clusterlizenz. Die Add-On-Lizenzen müssen in die ebenfalls ersetzt werden.
Beim Ersetzen einer Basislizenz werden alle Add-On-Lizenzen ersetzt, wenn diese einen anderen Typ aufweisen.	Wenn Sie eine eigenständige Basislizenz durch eine Cluster-Basislizenz oder umgekehrt ersetzen, werden Add-On-Lizenzen automatisch gelöscht, und neue Lize den richtigen Host-IDs sind erforderlich.
Beim Ersetzen einer Basislizenz werden nicht alle Add-On-Lizenzen gelöscht, wenn sie den gleichen Typ aufweisen und die Host-IDs übereinstimmen.	CC-E1-512 könnte z. B. als Ersatz für CC-E1-256 verw werden. Sind die Host-IDs bei beiden Lizenzen gleich, die Add-On-Lizenzen gültig.
In einem Cluster mit eigenständigen Lizenzen muss der Cluster zum Ersetzen von eigenständigen Lizenzen gelöscht und anschließend erneut hinzugefügt werden.	Da eigenständige Lizenzen von den Clustermitgliedern gemeinsam genutzt werden, müssen alle CC-SGs in e Cluster mit eigenständigen Lizenzen die gleiche Kapaz lizenzierte Knoten haben. Anstatt jeder der CC-SG-Einheiten Kapazität für lizenz Knoten hinzuzufügen, könnten Kunden den Umstieg a Clusterlizenzen vorziehen, damit die Lizenzen von den CC-SG-Einheiten gemeinsam genutzt werden können. Löschen Sie den Cluster vorübergehend, ersetzen Sie Lizenzen, und erstellen Sie den Cluster anschließend
Beim Ersetzen einer Basislizenz muss der Benutzer Funktionen auschecken.	Nachdem die Lizenzen ersetzt wurden, rufen Sie die S "Lizenzmanager" auf, prüfen Sie die verfügbaren Funk und checken Sie sie ggf. aus. Sie werden nicht automa ausgecheckt. Siehe ***Installieren und Auschecken de*** (auf Seite 26).

Anhang J Tastenkombinationen

Die folgenden Tastenkombinationen können im Java-basierten Administrations-Client verwendet werden.

Vorgang	Tastenkombinationen
Aktualisieren	F5
Fenster drucken	Strg + P
Hilfe	F1
Zeile in Verknüpfungstabelle einfügen	Strg + I

Anhang K Benennungsregeln

Dieser Anhang enthält Informationen zu den Benennungsregeln, die in CC-SG verwendet werden. Beachten Sie die maximale Zeichenlänge beim Benennen aller Teile der CC-SG-Konfiguration.

In diesem Kapitel

Benutzerinformationen 457
Knoteninformationen 457
Standortinformationen 458
Kontaktinformationen.....458
Dienstkonten.....458
Geräteinformationen.....458
Portinformationen 459
Zuordnungen 459
Administration.....459

Benutzerinformationen

Feld in CC-SG	Zulässige Anzahl an Zeichen in CC-SG
Benutzername	64
Vollständiger Name	64
Benutzerkennwort (kein sicheres Kennwort)	6-16
Benutzerkennwort (sicheres Kennwort)	Konfigurierbar Minimum: 8 Maximum: 16-64
Benutzer-E-Mail-Adresse	60
Benutzertelefonnummer	32
Benutzergruppenname	64
Benutzergruppenbeschreibung	160

Knoteninformationen

Feld in CC-SG	Zulässige Anzahl an Zeichen in CC-SG
Knotenname	64

Feld in CC-SG	Zulässige Anzahl an Zeichen in CC-SG
Knotenbeschreibung	160
Notizen	256
Überwachungsinformationen	256

Standortinformationen

Feld in CC-SG	Zulässige Anzahl an Zeichen in CC-SG
Abteilung	64
Standort	64
Standort	128

Kontaktinformationen

Feld in CC-SG	Zulässige Anzahl an Zeichen in CC-SG
Erster Ansprechpartner	64
Telefonnummer	32
Mobilfunknummer	32
Zweiter Ansprechpartner	64
Telefonnummer	32
Mobilfunknummer	32

Dienstkonten

Feld in CC-SG	Zulässige Anzahl an Zeichen in CC-SG
Dienstkontoname	64
Benutzername	64
Kennwort	64
Beschreibung	128

Geräteinformationen

Feld in CC-SG	Zulässige Anzahl an Zeichen in CC-SG
Gerätename	64
PX-Gerätenamen dürfen keine Punkte enthalten. Wenn Sie einen PX-Gerätenamen mit Punkten importieren, werden diese in Bindestriche umgewandelt.	
Gerätebeschreibung	160
Geräte-IP/Hostname	64
Benutzername	64
Kennwort	64
Notizen	256

Portinformationen

Feld in CC-SG	Zulässige Anzahl an Zeichen in CC-SG
Portname	32

Zuordnungen

Feld in CC-SG	Zulässige Anzahl an Zeichen in CC-SG
Kategoriename	32
Elementname	32
Gerätegruppenname	40
Knotengruppenname	40

Administration

Feld in CC-SG	Zulässige Anzahl an Zeichen in CC-SG
Clustername	64
Netzwerkumgebungsname	64
Modulname der Authentifizierung	31
Sicherungsname	64

Feld in CC-SG	Zulässige Anzahl an Zeichen in CC-SG
Sicherungsdateibeschreibung	255
Broadcastnachricht	255

Anhang L Startmeldungen der Diagnosekonsole

Vor Version 4.0 zeigt die CC-SG-Diagnosekonsole mehrere Meldungen auf dem Bildschirm an, sobald das Gerät gestartet wird. Diese Meldungen sind Linux-Standarddiagnosemeldungen und -Warnungen und weisen nicht auf Systemprobleme hin. Die Tabelle enthält eine kurze Beschreibung zu einigen häufig angezeigten Meldungen.

Meldung	Beschreibung
hda:	Die Meldung weist darauf hin, dass ein Element des Systems versucht, mit dem DVD-ROM-Laufwerk zu kommunizieren. Die Meldung kann durch verschiedene Szenarien ausgelöst werden. Beispiel: • Ein Benutzer öffnet oder schließt die Klappe des DVD-ROM-Laufwerks, oder • das Betriebssystem prüft das DVD-ROM-Laufwerk und findet keine darin enthaltenen Medien beim Starten. Es gibt weitere Szenarien, welche die Meldung auslösen, die jedoch hier nicht beschrieben werden.
avc:	Die Meldung wird von einem internen Sicherheitsüberwachungs- und Steuerungssystem – SELinux-Subsystem – angezeigt. Das System gibt Warnungen aus, ohne eine Sicherheitsrichtlinie zu erzwingen, d. h. diese Warnungen weisen nicht auf ein Problem mit dem System hin.
ipcontracks:	Die Meldung wird immer angezeigt, wenn CC-SG gestartet wird.

Beachten Sie, dass CC-SG diese Meldungen seit Version 4.0 nicht mehr anzeigt, sie jedoch weiterhin in internen Protokollen zur Verfügung stehen. Wenn Sie CC-SG von Version 3.x auf 4.x aktualisieren, werden diese Meldungen der Diagnosekonsole nicht mehr angezeigt.

Index

A

Active Directory mit CC-SG synchronisieren - 236
AD-Benutzergruppen importieren - 235
AD-Benutzergruppenbericht - 260
AD-Gruppeneinstellungen - 232, 234, 235
Administration - 459
Administratorkonsole - 361
AD-Module bearbeiten - 234
AD-Module zu CC-SG hinzufügen - 229
AD-Vertrauenseinstellungen - 233, 234
AES-Verschlüsselung - 316
AES-Verschlüsselung zwischen Client und CC-SG voraussetzen - 317
Aktivieren der AKC-Download-Serverzertifikat-Validierung - 152, 300
Aktualisieren eines Clusters - xvi, 276, 277, 309, 310
Alle AD-Module synchronisieren - 234, 235, 236, 237, 238, 333
Alle Benutzergruppen mit Active Directory synchronisieren - 234, 235, 237
Alle Konfigurationsdaten auf einem KX2-, KSX2- oder KX2-101-Gerät wiederherstellen - 100, 103
Alle Konfigurationsdaten mit Ausnahme der Netzwerkeinstellungen auf einem KX2-, KSX2- oder KX2-101-Gerät wiederherstellen - 102
Allgemeine AD-Einstellungen - 229, 234
Allgemeine häufig gestellte Fragen (FAQs) - 446
Allgemeine LDAP-Einstellungen - 241
Allgemeine RADIUS-Einstellungen - 246
Allgemeine TACACS+-Einstellungen - 245
Ältere Version der Anwendung öffnet sich nach Aktualisierung - 38, 284
An KX2 angeschlossenes Blade-Chassis-Gerät konfigurieren - 74
Ändern der HTTP- und HTTPS-Ports für ein KX2-Gerät - 68
Anforderungen an CSV-Dateien – Benutzer - 199
Anforderungen an CSV-Dateien – Geräte - 83, 93
Anforderungen an CSV-Dateien – Kategorien und Elemente - 52
Anforderungen an CSV-Dateien – Knoten - 165
Anforderungen für CC-SG-Cluster - 305
Anmeldeeinstellungen - 319
Anmeldeeinstellungen anzeigen - 319
Anmelden bei CC-SG - 26
Anmelden bei Diagnosekonsole und Einstellen der IP-Adresse für CC-SG - 25
Ansicht nach Kategorie - 216
Anwendungen für den Zugriff auf Knoten - 283
Anwendungen für den Zugriff auf Knoten konfigurieren - 283
Anwendungen hinzufügen - 37, 284
Anwendungen löschen - 285
Anwendungsversionen prüfen und aktualisieren - 37, 283
Anzahl an KVM-Sitzungen pro Benutzer einschränken - 46, 189, 190, 192
Auf die Administratorkonsole zugreifen - 274, 361
Auf die Diagnosekonsole über VGA-/Tastatur-/Mausport zugreifen - 353
Auf die Diagnosekonsole zugreifen - 353, 354
Auf die Statuskonsole über den Webbrowser zugreifen - 354, 355, 443
Auf die Statuskonsole über VGA-/Tastatur-/Mausport oder SSH zugreifen - 354
Auf die Statuskonsole zugreifen - 354
Auf einen CC-SG-Cluster zugreifen - 305, 306
Aufeinander folgende Aufgaben planen - 331
Auffinden der Host-ID Ihrer physischen Appliance und Überprüfen der Anzahl der Knoten in der Datenbank - 13, 15, 17
Aufgaben löschen - 338
Aufgaben neu planen - 338
Aufgaben planen - 106, 107, 236, 239, 278, 332, 337, 338, 405
Aufgaben planen, die einer anderen Aufgabe ähneln - 338
Aufgaben suchen und anzeigen - 332
Aufgabenarten - 331
Aufgabenmanager - 9, 35, 261, 264, 296, 329, 330, 403
Ausfall des Lizenzservers - 27
Ausgänge auf einem PowerStrip konfigurieren - 114, 116, 119

Authentifizierungsfluss - 225

B

Basis-DNs festlegen - 227
Bearbeiten von IP-Adressen mit CSV-Datei-Import - 178
Befehlszeilenprogramme zum Verwalten des Lizenzservers - 28
Beispiel
Webbrowser-Schnittstelle zu einem PX-Knoten hinzufügen - 157, 159
Beispiel-CSV-Datei für Benutzer - 204
Beispiel-CSV-Datei für Geräte - 98
Beispiel-CSV-Datei für Kategorien und Elemente - 53
Beispiel-CSV-Datei für Knoten - 176
Beispiele mit Platzhaltern - 62
Bekannte Probleme bei der Zwei-Faktoren-Authentifizierung - 445
Benachrichtigungsmanager - 329, 331
Benennungsregeln - 39, 51, 52, 64, 66, 71, 72, 87, 122, 130, 131, 150, 157, 180, 188, 194, 206, 211, 400, 434, 457
Benutzer abmelden - 207
Benutzer aus einer Gruppe löschen - 196, 198
Benutzer bearbeiten - 195
Benutzer einer Gruppe zuordnen - 195, 197
Benutzer exportieren - 199, 205
Benutzer hinzufügen - 194, 255
Benutzer hinzufügen, bearbeiten und löschen - 194
Benutzer importieren - 204
Benutzer löschen - 196
Benutzer per CSV-Dateiimport hinzufügen - 198
Benutzer und Benutzergruppen - 86, 179, 185, 215, 226, 245, 246
Benutzerdefinierte Ansicht als Standard für Knoten festlegen - 220
Benutzerdefinierte Ansicht als Standard für Knoten und alle Benutzer festlegen - 220
Benutzerdefinierte Ansicht für Geräte als Standard zuordnen - 223
Benutzerdefinierte Ansicht für Knoten ändern - 218
Benutzerdefinierte Ansicht für Knoten anwenden - 218
Benutzerdefinierte Ansicht für Knoten hinzufügen - 217
Benutzerdefinierte Ansicht für Knoten löschen - 219
Benutzerdefinierte Ansicht von Geräten als Standard für alle Benutzer zuordnen - 224
Benutzerdefinierte Ansichten für Geräte - 220
Benutzerdefinierte Ansichten für Geräte ändern - 222
Benutzerdefinierte Ansichten für Geräte anwenden - 221
Benutzerdefinierte Ansichten für Geräte hinzufügen - 220
Benutzerdefinierte Ansichten für Geräte löschen - 223
Benutzerdefinierte Ansichten für Geräte und Knoten - 123, 216
Benutzerdefinierte Ansichten für Knoten - 217
Benutzerdefinierte JRE-Einstellungen konfigurieren - 6, 301
Benutzergruppen bearbeiten - 190
Benutzergruppen hinzufügen - 188, 192
Benutzergruppen hinzufügen, bearbeiten und löschen - 129, 188
Benutzergruppen löschen - 191
Benutzergruppen und Benutzer hinzufügen - 46
Benutzergruppenberechtigungen - 188, 255, 421
Benutzerinformationen - 457
Benutzerkonten - 226
Benutzernamen des CC-SG-Superusers ändern - 207
Benutzernamen für Active Directory festlegen - 227
Benutzerverbindung trennen - 109
Benutzerverwaltung - 39, 46
Bericht - 254, 255, 256, 259, 260, 262, 337
Berichte - 248, 333
Berichte drucken - 249
Berichte in Dateien speichern - 250, 260
Berichte verwenden - 248
Berichte zu Historical Data Trending (Trendermittlung für Datenhistorie) anzeigen - 361, 386
Berichtsdaten aus CC-SG leeren - 250, 251, 252, 296
Berichtsdaten sortieren - 248
Berichtsdetails anzeigen - 249
Berichtsfilter ausblenden oder einblenden - 250
Bildschirm der Administratorkonsole - 362
Blade-Chassis mit integriertem KVM-Switch - 75

Blade-Chassis ohne integrierten KVM-Switch - 75
Blade-Chassis-Gerät auf einen anderen Port verschieben - 80
Blade-Chassis-Gerät bearbeiten - 79, 131
Blade-Chassis-Gerät hinzufügen - 75, 81
Blade-Chassis-Gerät löschen - 80
Blade-Server-Ports als normale KX2-Ports wiederherstellen - 59, 81
Blade-Server-Status ändern - 78
Browser auf AES-Verschlüsselung überprüfen - 317
Browserbasierter Zugriff über CC-SG-Administrations-Client - 5
Browser-Cache löschen - 275, 437
Browser-Verbindungsprotokoll konfigurieren HTTP oder HTTPS/SSL - 318

C

CC Users-Gruppe - 188
CC-NOC - 352
CC-SG aktualisieren - 33, 273, 277
CC-SG beenden - 280, 281
CC-SG Clustering - 415
CC-SG herunterfahren (CC-SG Shutdown) - 276, 277, 279
CC-SG herunterfahren (Powering Down CC-SG) - 280
CC-SG mit der Diagnosekonsole neu hochfahren - 376, 397, 439
CC-SG mit der Diagnosekonsole neu starten - 276, 277, 279, 375
CC-SG nach dem Herunterfahren neu starten - 279
CC-SG neu starten - 272, 292, 375
CC-SG sichern - 265, 272, 273, 275, 278, 301, 333
CC-SG und Client für IPMI, iLO/RILOE, DRAC, RSA - 418
CC-SG und Netzwerkkonfiguration - 412
CC-SG und Raritan-Geräte - 414
CC-SG und SNMP - 418
CC-SG verlassen - 280
CC-SG wiederherstellen - 266, 268, 278
CC-SG zurücksetzen - 270
CC-SG-Administrations-Client - 8
CC-SG-Cluster konfigurieren - 17, 304, 358
CC-SG-Datenbank migrieren - xvi, 277, 278
CC-SG-Kennwörter - 320
CC-SG-Kommunikationskanäle - 414
CC-SG-LAN-Ports - 289, 290, 292
CC-SG-Laufwerksüberwachung - 361, 441
CC-SG-Name, Datum und Uhrzeit - 356
CC-SG-Netzwerk konfigurieren - 229, 288
CC-SG-Seriennummer auffinden - 350
CC-SG-Serverzeit festlegen - 35
CC-SG-Serverzeit und -datum konfigurieren - 296
CC-SG-Sitzung beenden - 280
CC-SG-Standardeinstellungen - 25
CC-SG-System über die Diagnosekonsole ausschalten - 280, 377
CC-SG-Verwaltung eines Geräts unterbrechen - 106, 333
CC-SG-Zugriff über NAT-fähige Firewall - 419
Chat verwenden - 163
Clientbrowser-Anforderungen - 4
Cluster aktualisieren - 309
Cluster erstellen - 17, 277, 305
Cluster löschen - 309
Cluster wiederherstellen - 307, 308
Cluster-Einstellungen konfigurieren - 307
Clusterlizenzen - xvi, 276, 310
CommandCenter Secure Gateway unter VMware ESX Server 4.0 installieren - 24
CSV-Dateiimporte - 433

D

Debug-Modus - 440
Definierte Namen für Active Directory festlegen - 227
Definierte Namen für LDAP festlegen - 227
Definierte Namen für LDAP und Active Directory - 226
Details zur RSA-Schnittstelle - 154
Diagnosekonsole - 5, 353
Diagnoseprogramme - 439
Die Administratorkonsole - 353, 361
Die Administratorkonsole navigieren - 363
Die CC-Superuser-Gruppe - 187
Die Registerkarte - 57
Die Statuskonsole - 353, 354
Dienstkonten - 126, 458
Dienstkonten hinzufügen, bearbeiten und löschen - 127
Direkten Portzugriff auf Knoten konfigurieren - 162
Direktmodus für alle Client-Verbindungen konfigurieren - 298
Dominion PX-Daten von Power IQ importieren und exportieren - 406
Dominion PX-Daten zur Verwendung in Power IQ exportieren - 399, 408
Dominion PX-Geräte hinzufügen - 63, 64, 66

DRAC 5-Verbindungsdetails - 151
Durch das Konfigurieren von Ports erstellte Knoten - 70, 72, 131

E

E1 – Allgemeine technische Daten - 410
E1 – Umgebungsanforderungen - 410
E1-Modell - 410
Eigene E-Mail-Adresse ändern - 207
Eigene Standardsucheinstellungen ändern - 61, 206
Eigenen Namen ändern - 206
Eigenes Kennwort ändern - 206
Einleitung - 1
Einsatzort und Kontakte zu einem Geräteprofil hinzufügen - 60, 69
Einsatzort und Kontakte zu einem Knotenprofil hinzufügen - 124, 132
Einträge in der Überwachungsliste für Importe - 54, 99, 177, 205, 407, 435
Einzelheiten zur IBM IMM-Modulverbindung - xvi, 156
Elemente hinzufügen - 51
E-Mail-Benachrichtigungen für Aufgaben - 331
Empfohlene DHCP-Konfigurationen für CC-SG - 288, 291, 294, 295
Erforderliche geöffnete Ports für CC-SG-Netzwerke
Übersicht - 412
Ergebnisse nach dem Hinzufügen von Schnittstellen - 159
Erhalt Ihrer Lizenz - 13, 19, 21
Erste Schritte - 10
Erweiterte AD-Einstellungen - 231, 234
Erweiterte Administration - 194, 196, 230, 235, 282
Erweiterte LDAP-Einstellungen - 242
Externe SMTP-Server konfigurieren - 329

F

Fehlerbehebung bei Verbindungen zu Power IQ - 401
Fehlerprotokollbericht - 252
Fehlgeschlagene Aktualisierung des primären Knotens - xvi, 276, 277
Fenster - 60
Filter nach Gerätegruppe - 217
Filter nach Knotengruppe - 216
Firefox-Benutzer des Zugriffs-Clients müssen JNLP-Datei herunterladen - 148
Firmware löschen - 288
Firmware-Aktualisierung für Geräte planen - 332, 333, 335, 337, 338

G

Geplante Aufgaben ändern - 337
Geplante Aufgaben und der Wartungsmodus - 264
Geplante Berichte - 261, 262, 331
Gerät aktualisieren - 66, 99, 287
Gerät anpingen - 106
Gerät neu starten - 106, 333
Geräte anzeigen - 57
Geräte bearbeiten - 67
Geräte erkennen - 62, 63
Geräte erkennen und hinzufügen - 41
Geräte exportieren - 93, 99
Geräte hinzufügen - 63
Geräte importieren - 98
Geräte löschen - 60, 70
Geräte- oder Portzuordnung eines PowerStrips ändern (SX 3.0, KSX) - 115, 117
Geräte per CSV-Dateiimport hinzufügen - 92
Geräte suchen - 61
Geräte- und Portsymbole - 57
Geräte, Gerätegruppen und Ports - 56
Geräteanlagenbericht - 256
Geräteeinstellungen - 299
Gerätefirmware verwalten - 287
Gerätegruppen bearbeiten - 91
Gerätegruppen hinzufügen - 87, 91, 210
Gerätegruppen löschen - 91
Gerätegruppen und Knotengruppen hinzufügen - 43
Gerätegruppenmanager - 85
Geräteinformationen - 458
Gerätekonfiguration kopieren - 105, 333
Gerätekonfiguration sichern - 100, 333
Gerätekonfiguration wiederherstellen - 101, 333
Gerätekonfiguration wiederherstellen (KX, KSX, KX101, SX, IP-Reach) - 101
Geräte-Setup - 39, 41
Gerätestrommanager - 108
Geräteverwaltung fortsetzen - 107, 333
Geräteverwaltung mit einer geplanten Aufgabe unterbrechen und fortsetzen - xvi, 107, 333
Gleichzeitige Anmeldung von Benutzern zulassen - 321
Gruppen erstellen - 39, 43

H

Häufig gestellte Fragen (FAQs) - 446
Häufig gestellte Fragen (FAQs) zu Gruppen - 452
Häufig gestellte Fragen (FAQs) zu Konten - 451
Häufig gestellte Fragen (FAQs) zur Authentifizierung - 449
Häufig gestellte Fragen (FAQs) zur Autorisierung - 453
Häufig gestellte Fragen (FAQs) zur Benutzerfreundlichkeit - 453
Häufig gestellte Fragen (FAQs) zur Interoperabilität - 453
Häufig gestellte Fragen (FAQs) zur Leistung - 451
Häufig gestellte Fragen (FAQs) zur Sicherheit - 449
Häufig gestellte Fragen zur Lizenzierung - xvi, 34, 455
Häufige Anforderungen für CSV-Dateien - 52, 93, 165, 199, 434
Hilfe zu SSH-Befehlen erhalten - 340
Hinweise zu einem Geräteprofil hinzufügen - 60, 69
Hinweise zu einem Knotenprofil hinzufügen - 124, 133
Hinzufügen eines mit KX2 verbundenen KVM-Switches - 83

I

IBM LDAP-Konfigurationseinstellungen - 244
Ihr Benutzerprofil - 206
In mehrseitigen Berichten navigieren - 249
Installationsdateien herunterladen - 18, 19
Installationsvoraussetzungen für virtuelle Appliance - 18
Installieren und Auschecken der Lizenz - 26, 27, 455
Integration von Power IQ - 399
Interne CC-SG-Ports - 419
Interne CC-SG-Protokolle leeren - 296
IP-Adresse anpingen - 367
IP-Adresse bestätigen - 35
IP-Reach- und UST-IP-Verwaltung - 110

J

Java RDP-Verbindungsdetails - 152
Java-Cache löschen - 275, 284, 437
JRE-Inkompatibilität - 5, 6

K

Kategorien hinzufügen - 51
Kategorien löschen - 51
Kategorien und Elemente erstellen - 40
Kategorien und Elemente exportieren - 52, 54
Kategorien und Elemente hinzufügen, bearbeiten und löschen - 50
Kategorien und Elemente importieren - 54
Kategorien und Elemente per CSV-Dateiimport hinzufügen - 52
Kennwort des CC-Superusers mit der Diagnosekonsole zurücksetzen - 378
Kennwort für ein Dienstkonto ändern - 128
Kennworteinstellungen der Diagnosekonsole - 361, 378, 381
Knoten - 122
Knoten anpingen - 148
Knoten anzeigen - 123
Knoten auswählen - 180
Knoten bearbeiten - 131, 141
Knoten beschreiben - 181
Knoten exportieren - 156, 165, 175, 177, 178
Knoten hinzufügen - 130, 402
Knoten hinzufügen, bearbeiten und löschen - 130
Knoten importieren - 177, 178
Knoten löschen - 131, 143
Knoten per CSV-Dateiimport hinzufügen - 164
Knoten- und Schnittstellensymbole - 126
Knoten, Knotengruppen und Schnittstellen - 56, 121
Knotenanlagebericht - 162, 258, 260
Knotenerstellungsbericht - 259
Knotengruppen bearbeiten - 184
Knotengruppen hinzufügen - 180, 210
Knotengruppen hinzufügen, bearbeiten und löschen - 179
Knotengruppen löschen - 184
Knoteninformationen - 457
Knotennamen - 122
Knotenprofil - 124
Kombination aus Direktmodus und Proxymodus konfigurieren - 293, 298
Kommunikation mit Lizenzserver - 27
Kompatibilitätsmatrix überprüfen - 36
Konfiguration der Diagnosekonsole bearbeiten - 364
Konfiguration der Netzwerkumgebung verwalten - 314
Konfiguration des Diagnosekonsolen-Kontos - 383

Konfigurationseinstellungen für OpenLDAP (eDirectory) - 243
Konfigurationseinstellungen für Sun One LDAP (iPlanet) - 243
Konfigurieren der mit KX2 2.3 oder höher verbundenen analogen KVM-Switches - 83
Konfigurieren der Synchronisierung von Power IQ und CC-SG - 399, 401, 403, 404, 405
Konfigurieren von CC-SG mit dem Setup-Assistenten - 10, 39, 50, 210
Konfigurieren von Ports auf einem mit KX2 verbundenen analogen KVM-Switch-Gerät - 84
Kontaktinformationen - 458
Kontextmenüoptionen auf der Registerkarte Geräte - 61
KVM- oder serielle Geräte hinzufügen - 63, 64, 76, 83, 116, 118
KVM-Port konfigurieren - 71, 81

L

Laufwerk- oder RAID-Tests ausführen - 388
Laufwerktests planen - 390
LDAP und CC-SG - 240
LDAP-Module (Netscape) zu CC-SG hinzufügen - 240
Leerlaufzeitgeber konfigurieren - 322
Lesezeichen für Schnittstelle - 161, 162, 258
Linux-Server - 19, 23
Lizenserversoftware unter Linux- oder Windows-Server installieren - 19
Lizenz hinzufügen - xvi, 34
Lizenzdatei auf Lizenzserver kopieren - 23
Lizenzierung – Beschränkter Betrieb vor der Lizenzinstallation - 10, 17, 27, 31
Lizenzierung – Bestehende Kunden - 10, 11, 33
Lizenzierung – Cluster – Neue Kunden - 17
Lizenzierung – Erste Schritte – Neue und bestehende Kunden - 10
Lizenzierung – Grundlegende Lizenzinformationen - 11
Lizenzierung – Neue Kunden – Physische Appliance - 10, 11, 13, 14, 17, 18
Lizenzierung – Rehosting - 34
Lizenzierung – Virtuelle Appliance mit Lizenzserver - 10, 11, 18
Lizenzserver starten - 23

M

Massenkopieren für Gerätezuordnungen, Einsatzort und Kontakte - 82
Massenkopieren für Knotenzuordnungen, Einsatzort und Kontakte - 162
Massenkopieren von Benutzern - 208
Methode - 91, 180
MIB-Dateien - 304
Microsoft RDP-Verbindungsdetails - 152
Migrationsvoraussetzungen - xvi, 278
Mitglied aus einer Netzwerkumgebung löschen - 315
Mitglied zu einer Netzwerkumgebung hinzufügen - 313
Module für die Authentifizierung und Autorisierung festlegen - 227

N

Navigationstastenerinnerung - 359
Netzwerkeinrichtung - 3, 35, 288, 305, 365
Netzwerkschnittstellenkonfiguration bearbeiten (Network Interfaces) - 365
Netzwerkumgebung aktualisieren - 316
Netzwerkumgebung bearbeiten - 313
Netzwerkumgebung erstellen - 311
Netzwerkumgebung konfigurieren - 311
Netzwerkumgebung löschen - 316
Neuerungen im CC-SG Handbuch für Administratoren - xvi
Neustart des Lizenzservers nach einem Ausfall - 28
NTP-Status anzeigen - 394
Nur Geräteeinstellungen oder Benutzer- und Benutzergruppendaten auf einem KX2-, KSX2- oder KX2-101-Gerät wiederherstellen - 102

P

Paragon II-Systemcontroller (P2-SC) - 110
Platzhalter für die Suche - 61, 62
Port für die Überwachung des Remotesystems - 420
Portabfragebericht - 256
Portal - 313, 322
Portinformationen - 459
Portnummer für SSH-Zugriff auf CC-SG einstellen - 318
Ports bearbeiten - 73
Ports konfigurieren - 70, 118

Ports löschen - 74
Portsortieroptionen - 58
Power IQ-Dienste konfigurieren - 157, 175, 400, 401, 403
Power IQ-Synchronisierungsrichtlinien - 404, 405
PowerStrip eines KX-, KX2-, KX2-101-, KSX2- oder P2SC-Geräts an einen anderen Port bewegen - 114, 115
PowerStrip eines SX 3.1-Geräts an einen anderen Port bewegen - 118, 119
PowerStrip- oder Dominion PX-Geräte bearbeiten - 68
PowerStrip, der an ein KX-, KX2-, KX2-101-, KSX2- oder P2SC-Gerät angeschlossen ist, löschen - 114, 115
PowerStrip, der an ein SX 3.0- oder KSX-Gerät angeschlossen ist, hinzufügen - 115, 116
PowerStrip, der an ein SX 3.0- oder KSX-Gerät angeschlossen ist, löschen - 115, 117
PowerStrip, der an ein SX 3.1-Gerät angeschlossen ist, hinzufügen - 118, 119
PowerStrip, der an ein SX 3.1-Gerät angeschlossen ist, löschen - 118, 119
PowerStrip-Gerät, das an ein KX-, KX2-, KX2-101-, KSX2- oder P2SC-Gerät angeschlossen ist, hinzufügen - 114
PowerStrip-Geräte hinzufügen - 63, 64, 66
Powerstrips aus Power IQ importieren - 399, 406
PowerStrips konfigurieren, die von einem anderen Gerät in CC-SG verwaltet werden - 111, 113
PowerStrips, die an KX-, KX2-, KX2-101-, KSX2- und P2SC-Geräte angeschlossen sind, konfigurieren - 113, 114
PowerStrips, die an SX 3.0- und KSX-Geräte angeschlossen sind, konfigurieren - 113, 115
PowerStrips, die an SX 3.1-Geräte angeschlossen sind, konfigurieren - 113, 118
Problembehandlung - 437
Problembehebung bei CSV-Dateien - 54, 98, 177, 205, 407, 436
Protokollaktivitäten konfigurieren - 295, 333
Protokolldateien in der Diagnosekonsole anzeigen - 371
Proxymodus für alle Client-Verbindungen konfigurieren - 298

R

RADIUS und CC-SG - 246
RADIUS-Module hinzufügen - 246
RAID-Status und Laufwerksauslastung anzeigen - 387, 389, 441
RDP-Zugriff auf Knoten - 420
Registerkarte - 123, 186
Reihenfolge für externe AA-Server festlegen - 228
Remoteauthentifizierung - 185, 225, 316
Repair (Reparieren) oder Rebuild (Wiederherstellen) von RAID-Laufwerken - 388, 389, 390, 392
Richtlinien bearbeiten - 212
Richtlinien Benutzergruppen zuordnen - xvi, 189, 210, 215
Richtlinien für die Zugriffssteuerung - 45, 50, 85, 185, 189, 210
Richtlinien hinzufügen - 86, 179, 210, 211, 214
Richtlinien löschen - 214
RSA-Kompatibilität mit JRE - 154

S

Schnittstellen - 123, 298
Schnittstellen bearbeiten - 160
Schnittstellen Dienstkonten zuweisen - 129
Schnittstellen für DRAC-Stromversorgungsverbindungen - 150, 153
Schnittstellen für ILO Processor-, Integrity ILO2- und RSA-Stromversorgungsverbindungen - 150, 153
Schnittstellen für In-Band-Verbindungen - 149, 151
Schnittstellen für IPMI-Stromversorgungsverbindungen - 155, 156
Schnittstellen für Out-of-Band KVM-, Out-of-Band serielle Verbindungen - 149, 152
Schnittstellen für Power IQ Proxy-Stromversorgungsverbindungen - 150, 156, 402
Schnittstellen für verwaltete Powerstrip-Verbindungen - 112, 114, 117, 119, 150, 154
Schnittstellen hinzufügen - 130, 148, 160, 402
Schnittstellen hinzufügen, bearbeiten und löschen - 129, 148

Schnittstellen löschen - 142, 160
Seriellen Port konfigurieren - 71
Serieller Administrationsport - 349
Setupanforderungen für die Zwei-Faktoren-Authentifizierung - 444
Sichere Kennwörter für alle Benutzer voraussetzen - 319
Sicherheitsmanager - 316, 339
Sicherungen und Schnappschüsse von virtueller Appliance und Speicherservern konfigurieren - 31
Sicherungsdateien löschen - 268
Sicherungsdateien speichern - 267, 273
Sicherungsdateien speichern und löschen - 265, 267, 270
Sicherungsdateien von Geräten speichern, hochladen und löschen - 103
Slots auf einem Blade-Chassis-Gerät konfigurieren - 61, 75, 76, 77
Slots auf einem Blade-Chassis-Gerät löschen - 79
SNMP konfigurieren - 303
SNMP-Traps - 304, 431
Sonderzugriff auf Paragon II-Systemgeräte - 110
Spaltenbreite in Berichten vergrößern/verkleinern - 248
Speicherdiagnose - 439
Sperreinstellungen - 254, 320
SSH-Befehle und Parameter - 342
SSH-Verbindung zu einem seriellen Gerät herstellen - 346
SSH-Verbindungen beenden - 345, 348
SSH-Zugriff auf CC-SG - 318, 339
SSH-Zugriff auf Knoten - 420
Standardanwendung für Schnittstellen- oder Porttypen einstellen - 287
Standardanwendungen - 286
Standardanwendungen konfigurieren - 286
Standardbenutzergruppen - 187
Standardschriftgrad für CC-SG ändern - 207
Standortinformationen - 458
Startmeldungen der Diagnosekonsole - 461
Static Routes bearbeiten - 293, 367, 369
Statuskonsole - 354, 386
Statuskonsole über den Webbrowser - 360
Statuskonsole über VGA-/Tastatur-/Mausport oder SSH - 356
Statuskonsoleninformationen - 356
Steuerungssystem mit virtuellen Hosts und virtuellen Geräten hinzufügen - 135, 141
Steuerungssysteme und virtuelle Hosts löschen - 143
Steuerungssysteme, virtuelle Hosts und virtuelle Geräte bearbeiten - 141, 143
Stromversorgungssteuerung von Power IQ-IT-Geräten - 111, 113, 175, 399, 406
Stromversorgungssteuerung von Power IQ-IT-Geräten konfigurieren - 402
Synchronisierung von Power IQ und CC-SG - 333, 404
System-, Server- und Netzwerkstatus - 357
Systemadministratorgruppe - 187
Systemschnappschuss aufnehmen - 396, 441, 442, 443
Systemwartung - 263

T

TACACS+ und CC-SG - 245
TACACS+-Module hinzufügen - 245
Tägliche Synchronisierung aller AD-Module aktivieren oder deaktivieren - 239
Tägliche Synchronisierung der virtuellen Infrastruktur aktivieren oder deaktivieren - 145
Täglichen AD-Synchronisierungszeitpunkt ändern - 239
Tastenkombinationen - 456
Technische Daten für V1 und E1 - 409
Terminalemulationsprogramme - 350
Terminologie zur virtuellen Infrastruktur - 133
Terminologie/Abkürzungen - 2, 64, 66, 241, 245, 246, 291, 293, 312, 313, 329, 345, 365, 400
Thick-Client installieren - 7
Thick-Client verwenden - 8
Thick-Client-Zugriff - 6
Tipp des Tages - 357
Tipp des Tages konfigurieren - 282
Tipps für das Hinzufügen einer Webbrowser-Schnittstelle - 158, 174
Tipps zu Befehlen - 342, 345
Top Display mit der Diagnosekonsole anzeigen - 393
Topologieansicht - 61
Traceroute verwenden - 368
Typen von benutzerdefinierten Ansichten - 216

U

Über SSH auf die Diagnosekonsole zugreifen - 353
Überblick über AD und CC-SG - 228
Überblick über Authentifizierung und Autorisierung (AA) - 225
Überblick über Dienstkonten - 126
Überblick über Gerätegruppen - 86
Überblick über Knoten und Schnittstellen - 122
Überblick über Knotengruppen - 179
Überblick über virtuelle Knoten - 135
Übersicht über das Blade-Chassis - 74
Überwachung des Remotesystems konfigurieren - 385, 420, 441
Überwachungslistenbericht - 251
Umbenennen und Verschieben von AD-Gruppen - 240
Unterstützte Umgebungen für die Zwei-Faktoren-Authentifizierung - 444
Unterstützung für virtuelle Medien - 214
Upload - 287

V

V1 – Allgemeine technische Daten - 409
V1 – Umgebungsanforderungen - 409
V1-Modell - 409
Verbindung von PC-Clients mit CC-SG - 416
Verbindung von PC-Clients mit Knoten - 417
Verbindung zu Knoten herstellen - 147
Verbindung zum Knoten mit SSH über serielle Out-of-Band-Schnittstelle herstellen - 347
Verbindungsmodi - 123, 152, 297
Direkt und Proxy - 297, 419
Verfügbare Lizenzen - 11, 15, 269
Verfügbarkeitsbericht - 253, 278
Verwaltete PowerStrips - 56, 63, 66, 111, 113
Verwaltungsseite eines Geräts aufrufen - 109
Verwenden von benutzerdefinierten Ansichten im Administrations-Client - 217
Videoauflösung für Diagnosekonsole ändern - 397
Virtuelle Appliances mit Remote-Speicherservern - 31
Virtuelle Infrastruktur in CC-SG konfigurieren - 133, 148
Virtuelle Infrastruktur löschen - 143
Virtuelle Infrastruktur mit CC-SG synchronisieren - 145
Virtuelle Infrastruktur synchronisieren - 145
Virtuellen Geräteknoten löschen - 143
Virtuellen Host mit virtuellen Geräten hinzufügen - 138, 141
Virtuellen Host neu starten oder Neustart erzwingen - 146
VMware Tools installieren oder aktualisieren - 30
VNC-Zugriff auf Knoten - 420
Vor der Verwendung des Setup-Assistenten - 40
Voraussetzungen für die Verwendung des AKC - 152, 286
Vorbereitungen - 1
vSphere 4-Benutzer müssen ein neues Plug-In installieren - 144

W

Wartungsmodus - 212, 263
Wartungsmodus beenden - 264, 275
Wartungsmodus starten - 37, 264, 274, 277, 283
Was ist der IP-Ausfallsicherungsmodus? - 288, 290
Was ist der IP-Isolationsmodus? - 288, 292
Was ist eine Netzwerkumgebung? - 288, 311, 312, 315
Web Services-API - 350
Webbrowser-Schnittstelle - 150, 157
Werksseitig eingestellte Konfiguration von CC-SG wiederherstellen - 277, 279, 379
Windows-Server - 20, 23, 24
Worin besteht der Unterschied zwischen einer vollständigen und einer Standardsicherung? - 265, 267, 269

Z

Zertifikate - 324
Zertifikate – Aufgaben - 324
Zugreifen auf CC-SG - 5
Zugriff auf die Ansicht für die virtuelle Topologie - 147
Zugriff auf Infrastrukturdienste - 416
Zugriff auf Lizenzen - 27
Zugriffsbericht - 192, 252
Zugriffssteuerungsliste - 327, 381
Zugriffsüberwachung für Benutzergruppen konfigurieren - 125, 193, 195
Zuordnungen - 49, 459
Zuordnungen der Standardanwendung anzeigen - 286
Zuordnungen erstellen - 50
Zuordnungen im Setup-Assistenten - 39, 40

Zuordnungen, Kategorien und Elemente - 49, 60, 65, 67, 86, 116, 124, 130, 179
Zuordnungsbestimmende Kategorien und Elemente - 49
Zuordnungsterminologie - 49
Zwei-Faktoren-Authentifizierung - 247, 444
Zwei-Faktoren-Authentifizierung mit RADIUS - 247
Zwischen primärem und sekundärem Knotenstatus wechseln - 276, 307

USA/Kanada/Lateinamerika

Montag bis Freitag
08:00 bis 20:00 Uhr ET (Eastern Time)
Tel.: 800-724-8090 oder 732-764-8886
CommandCenter NOC: Drücken Sie auf Ihrem Telefon die Zifferntaste 6 und dann die Zifferntaste 1.
CommandCenter Secure Gateway: Drücken Sie auf Ihrem Telefon die Zifferntaste 6 und dann die Zifferntaste 2.
Fax: 732-764-8887
E-Mail-Adresse für CommandCenter NOC: tech-ccnoc@raritan.com
E-Mail-Adresse für alle anderen Produkte: tech@raritan.com

China

Peking
Montag bis Freitag
09:00 bis 18:00 Uhr Ortszeit
Tel.: +86-10-88091890

Shanghai
Montag bis Freitag
09:00 bis 18:00 Uhr Ortszeit
Tel.: +86-21-5425-2499

GuangZhou
Montag bis Freitag
09:00 bis 18:00 Uhr Ortszeit
Tel.: +86-20-8755-5561

Indien

Montag bis Freitag
09:00 bis 18:00 Uhr Ortszeit
Tel.: +91-124-410-7881

Japan

Montag bis Freitag
09:30 bis 17:30 Uhr Ortszeit
Tel.: +81-3-3523-5991
E-Mail: support.japan@raritan.com

Europa

Europa
Montag bis Freitag
08:30 bis 17:00 Uhr GMT+1 MEZ
Tel.: +31-10-2844040
E-Mail: tech.europe@raritan.com

Großbritannien
Montag bis Freitag
08:30 bis 17:00 Uhr GMT
Telefon +44(0)20-7090-1390

Frankreich
Montag bis Freitag
08:30 bis 17:00 Uhr GMT+1 MEZ
Tel.: +33-1-47-56-20-39

Deutschland
Montag bis Freitag
08:30 bis 17:30 Uhr GMT+1 MEZ
Tel.: +49-20-17-47-98-0
E-Mail: rg-support@raritan.com

Melbourne, Australien

Montag bis Freitag
09:00 bis 18:00 Uhr Ortszeit
Tel.: +61-3-9866-6887

Taiwan

Montag bis Freitag
09:00 bis 18:00 Uhr GMT -5 Standardzeit -4 Sommerzeit
Tel.: +886-2-8919-1333
E-Mail: support.apac@raritan.com