Administrationshandbuch Collax V-Cube 6.8

Administrationshandbuch

Collax V-Cube

Version 6.8

Administrationshandbuch Collax V-Cube
Version 6.8

Stand: 5.11.2014

Collax GmbH
Gutenbergstr. 1 · D-85737 Ismaning
Tel. +49 (0) 89 / 99 01 57-0
Fax +49 (0) 89 / 99 01 57-11
<http://www.collax.com>

Inhaltsverzeichnis

Vorwort 1

1 Übersicht 3

2 Inbetriebnahme 5

2.1 Installation Softwareversion 5
2.2 Voreinstellungen 6

3 Administration 7

3.1 Web-Oberfläche 7
3.2 Erste Schritte 10
3.3 Konfiguration 11
3.4 Assistenten 22

4 Benutzungsrichtlinien 33

4.1 Einführung 33
4.2 Vordefinierte Gruppen 35
4.3 Berechtigungen 36
4.4 Gruppenplanung 37
4.5 Schritt für Schritt: Anlegen einer Gruppe 43
4.6 GUI-Referenz: Richtlinien 50
4.7 GUI-Referenz: Umgebung 70

5 Authentifizierung 79

5.1 LDAP 79
5.2 Unterstützung von Windows-Domänen 84

6 Verschlüsselung 99

6.1 Einführung 99
6.2 Schritt für Schritt: Erstellen eines Serverzertifikats 112
6.3 GUI-Referenz: X.509-Zertifikate 115
6.4 GUI-Referenz: Certificate Signing Requests (CSR) 130

7 Netzwerke 137

7.1 Einführung 137
7.2 Schritt für Schritt: Einrichten des lokalen Netzes 152
7.3 GUI-Referenz: Netze 155
7.4 GUI-Referenz: Links 159
7.5 Schritt für Schritt: Internetzugang einrichten 176

8 Hardwarekonfiguration 181

8.1 Grundlagen 181
8.2 GUI-Referenz: Hardware 185
8.3 GUI-Referenz: iSCSI Initiator 205
8.4 GUI-Referenz: iSCSI-Knoten 207
8.5 GUI-Referenz: iSCSI-Knoten Status 211

9 Firewall 215

9.1 Einführung 215
9.2 GUI-Referenz: Firewall 217
9.3 Schutz vor Brut-Force-Attacken 221

10 DNS und DHCP 225

10.1 Einführung 225
10.2 Schritt für Schritt: DNS für lokale Domain einrichten 236
10.3 GUI-Referenz: DNS 244
10.4 Schritt für Schritt: DHCP aktivieren 266
10.5 GUI-Referenz: DHCP 270

11 E-Mail 279

11.1 GUI-Referenz: SMTP-Versand 279

12 Fileserver 283

12.1 Einführung 283
12.2 Schritt für Schritt: Ein Share anlegen 284
12.3 GUI-Referenz: File-Shares 288
12.4 GUI-Referenz: Antivirus Dateiprüfung 293

13 Datensicherung 297

13.1 Bacula Datensicherung - Einführung 297
13.2 Schritt für Schritt: Datensicherung auf Windows-Freigabe einrichten 297
13.3 GUI-Referenz: Datensicherung Allgemein 299
13.4 GUI-Referenz: Zuordnungen 304
13.5 GUI-Referenz: Sicherungsziele 308
13.6 GUI-Referenz: Inhaltslisten 316
13.7 GUI-Referenz: Clients 321
13.8 GUI-Referenz: Pläne 324
13.9 GUI-Referenz: Monitor-Zugriff 328
13.10 GUI-Referenz: Status und Betrieb 331
13.11 GUI-Referenz: Datenwiederherstellung 335
13.12 GUI-Referenz: Katalog-Wiederherstellung 335

14 Virtualisierung 339

14.1 Einführung 339
14.2 Paravirtualisierung 339
14.3 Allgemein 340
14.4 GUI-Referenz: Virtualisierung 341

15 Cluster und Cluster Management 393

15.1 Hochverfügbarkeit 393
15.2 Cluster-Domain 394
15.3 Shared Storage 394
15.4 Erstkonfiguration eines Clusters 395
15.5 Konfiguration der Cluster-Domain 401
15.6 Virtuelle Maschinen 443
15.7 Netzwerktechnik und -aufbau 464
15.8 Status und Monitoring 469

16 Verschiedene Dienste 481

16.1 Datum und Zeit 481
16.2 Netzwerküberwachung 485
16.3 Server Management mit Spotlight 494
16.4 USV 501

17 Lizenzierung, Update und Softwaremodule 509

17.1 Lizenz 509
17.2 Systemsoftware 515
17.3 GUI-Referenz: Update-Konfiguration 521

18 Systembetrieb 523

18.1 GUI-Referenz: Netzwerk-Tools 523
18.2 Festplattenverwaltung 528
18.3 GUI-Referenz: Shutdown und Reboot 539

19 Systeminformationen 541

19.1 Systeminformationen 541
19.2 Dienste 542
19.3 Netzwerkstatus 543
19.4 Mailqueue 544
19.5 Auswertungen 545
19.6 System-Logdateien 545
19.7 GUI-Referenz: Status 547
19.8 GUI-Referenz: Auswertungen 564

20 Software neu installieren oder Auslieferungszustand wiederherstellen 571

20.1 Brennen der ISO-Datei 571
20.2 Installation 572
20.3 Administration 572

Index 573

Vorwort

Vielen Dank, dass Sie sich für den V-Cube entschieden haben, die Linux-basierte Serverlösung für kleine und mittelständische Unternehmen.

Der V-Cube integriert die Kontrolle über alle Ihre Serveranwendungen und -funktionen in eine grafische Benutzeroberfläche. So können Sie Ihre private Cloud mit Virtualisierung und Hochverfügbarkeit leichter verwalten.

Sie benötigen lediglich Kenntnisse über vernetzte IT-Systeme, um Ihren V-Cube in Betrieb nehmen und konfigurieren zu können.

Dieses Handbuch zeigt Ihnen Schritt für Schritt, wie Sie Ihren Server so einrichten können, dass er am besten zu Ihren geschäftlichen Erfordernissen passt.

Bitte kontaktieren Sie das Collax-Support-Team über Telefon, E-Mail oder Fax, wenn Sie Fragen oder Probleme haben, die Sie selbst nicht beantworten oder lösen können.

Weitere aktuelle Informationen finden Sie im Web unter: <http://www.collax.com>

1 Übersicht

Mit dem V-Cube wurde ein leistungsfähiges System für Serveranwendungen geschaffen, welches gleichzeitig sehr einfach zu bedienen ist.

Der Anwender steuert das System mit einem nahezu beliebigen Browser über eine durchgängig einheitliche Weboberfläche. Unter dieser Oberfläche läuft eine speziell angepasste Linux-Variante. Bei dieser wurde gezielt die beste auf dem Markt verfügbare freie Software für eine jeweilige Aufgabenstellung ausgesucht. Dieser „Best of Breed“-Ansatz führt zu einem schlanken und übersichtlichen System, welches durch Konzentration auf das Wesentliche sehr sicher gehalten werden kann.

Mit den Wurzeln dieser Software, die weit in die Unix-Welt reichen, eignet sich der V-Cube zudem besonders gut für alle verknüpften Dienste wie Storage-, CPU- und Netzwerkvirtualisierung oder die Hochverfügbarkeit von virtuellen Maschinen mittels des KVM-Hypervisors.

Grundsätzlich sind alle Dienste zunächst deaktiviert. Der Anwender entscheidet, was er überhaupt einsetzen möchte. Assistenten helfen ihm, eine sinnvolle Konfiguration des V-Cubes auf einfache Weise zu erstellen.

Das vorliegende Handbuch wird alle Aspekte der Konfiguration und des Betriebs des V-Cubes behandeln. Bei einigen zentralen Themen werden zudem notwendige Hintergrundinformationen gegeben, um die Funktionsweise des Systems besser zu verstehen.

Mit beinahe jedem Softwareupdate werden weitere sinnvolle Funktionen zum V-Cube hinzugefügt. Dieses Handbuch dient daher der Orientierung im System. Detaillierte Hinweise zu einzelnen sel-

tenen oder zum Zeitpunkt der Drucklegung noch nicht vorhandenen Funktionen finden sich in der Onlinehilfe des Systems. Die Onlinehilfe wird regelmäßig automatisch aktualisiert.

2 Inbetriebnahme

Der V-Cube ist in zwei grundsätzlichen Ausführungen erhältlich, einmal als reine Softwareversion und einmal als vollständiges Hardware-Appliance-System. Für die Softwareversion wird ein Hardware-System mit x86_64-kompatibler CPU benötigt. Bei der Installation der Software wird die Festplatte vollständig gelöscht.

Zum Testen des V-Cubes kann von der CD ein „Live-System“ gestartet werden. Dabei werden keinerlei automatische Änderungen an der Festplatte vorgenommen.

Die Hardware-Appliance ist in unterschiedlich leistungsfähigen Ausbaustufen erhältlich und reicht von kleinen kompakten Geräten bis zu ausgewachsenen Serversystemen in 19-Zoll-Technik.

2.1 Installation Softwareversion

Zur Installation der Software muss das System von der CD oder einem USB-Image gebootet werden.

Hinweis: Bei Installation der V-Cube-Software wird die gesamte Festplatte gelöscht. Es gibt keine Möglichkeit, bereits vorhandene Partitionen oder Daten zu erhalten.

Nach dem Start der Installation des V-Cubes folgen Sie einfach den Anweisungen. Wenn die Installation abgeschlossen ist, kann das System neu gestartet werden.

2.2 Voreinstellungen

Werden bei der Installation der Software bzw. über das Display oder das Konsolen-Werkzeug setip am Server keine Änderungen vorgenommen, ist der V-Cube auf folgenden Voreinstellungen konfiguriert:

- Netzwerkschnittstelle eth0
- IP-Adresse 192.168.9.9
- Netzmaske 255.255.255.0
- Netzwerk 192.168.9.0
- Default-Gateway 192.168.9.1

3 Administration

3.1 Web-Oberfläche

Die Administration des V-Cubes erfolgt vollständig über eine Web-Oberfläche. Der Zugriff erfolgt immer verschlüsselt über HTTPS. Für die Administration wird ein separater Webserver verwendet, der Anfragen auf Port 8001 entgegennimmt. Die URL zum Zugriff lautet daher: „https://192.168.9.9:8001“. Statt „192.168.9.9“ muss die bei der Installation eingestellte IP-Adresse eingesetzt werden.

Beim ersten Anmelden muss zunächst ein „EULA“ akzeptiert werden, danach werden die Passwörter für die beiden Systemkonten *admin* und *root* gesetzt. Auf der Weboberfläche meldet sich immer *admin* an, *root* wird nur auf der Kommandozeile verwendet. Das Root-Passwort ist dennoch das wichtigste Passwort auf dem System und sollte entsprechend sorgfältig aufbewahrt werden. Bei Verlust dieser beiden Passwörter ist das komplette Zurücksetzen des V-Cubes in den Auslieferungszustand erforderlich.

Werden Passwörter gewählt, sollten diese ebenfalls ein gewisses Maß an Sicherheit bieten. Tabu sollten Passwörter wie „geheim“, „joshua“, der Firmenname oder der Name der Ehefrau sein. Ähnlich schlecht sind Passwörter aus normalen Wörtern, die mit einem Wörterbuchangriff geraten werden können. Ein Passwort sollte eine gute Mischung aus Groß- und Kleinbuchstaben sowie Ziffern aufweisen. Dabei sollte kein sinnvolles Wort in irgendeiner Sprache gebildet werden. Leerzeichen sollten vermieden werden.

Nach dem Anmelden präsentiert sich die Oberfläche mit einem Dashboard, mit welchem die wichtigen Informationen über den Zustand des Produkts eingesehen werden können.

3.1.1 Dashboard

Über das Dashboard wird der Gesamtstatus auf einen Blick dargestellt. In mindestens vier grafischen Gruppierungen zeigt der V-Cube Auswertungen über die folgenden Informationsbereiche. Klicken Sie auf eines der Felder, um direkt weitere Informationen oder Einstellungen vorzunehmen.

Unter *Hochverfügbarkeit* wird angezeigt ob alle Nodes im Cluster aktiv sind. Dieser Status wird mit einem grünen Häkchen als OK deklariert. Ein Klick auf diesen Informationsbereich führt in den Dialog *Cluster Nodes*, damit weitere Details eingeholt oder bestimmte Wartungsaktionen vorgenommen werden können. Ist nur ein Node nicht aktiv im Cluster, wird dies sofort in der entsprechenden Signalfarbe gekennzeichnet.

Zusätzlich können sogenannte Ressourcen des Clusters beobachtet werden. Ressourcen bilden die zentrale Elemente eines Clusters: Alle wesentlichen Konzepte der HA-Lösung werden durch Ressourcen beschrieben - so ist letztendlich eine Virtuelle Maschine eine Ressource. Aber auch Festplattenabbilder für die virtuellen Maschinen oder das Fencing Device sind Ressourcen. Diese Ressourcen sind vollkommen automatisch verwalten und bedürfen keinerlei Eingriffe seitens des Bedieners.

Im Bereich *Virtuellen Maschinen* wird die Anzahl der laufenden Instanzen angezeigt. Um zur Verwaltung von virtuellen Maschinen zu gelangen, kann hier per Klick der Dialog aufgerufen werden.

Plattenbelegung kennzeichnet die wichtigsten Datenbereiche mit deren Füllgrad. Dahinter stehen die Festplatten-Bereiche für VMs und dem gemeinsamen Ablage-Storage „Cluster Share“.

Der Bereich *Überwachung* gibt auf einen Blick Auskunft, ob die Bereiche Dienste und Hardware ordnungsgemäß funktionieren. Ein Ereignis-Log kann per Klick aufgerufen werden, um weitere Details zu erfahren.

3.1.2 Stapelverwaltung der Dialoge

In der modern entworfenen Oberfläche werden bestimmte Dialoge innerhalb von Stapeln parallel verwaltet. Diese Stapel werden in der Kopfzeile der Oberfläche angezeigt. Zwischen diesen Stapeln kann mit der Fokussierung per Maus oder mit der Tastenkombination „Shift Tab“ gewechselt werden. Daraus resultiert der Vorteil, dass oft genutzte Dialoge geöffnet bleiben können und sofort in der Administration zur Verfügung stehen.

Die folgenden Dialoge können in separaten Stapeln adressiert werden. Unterdialoge werden innerhalb des einen geöffneten Stapel angezeigt.

- Dashboard, Einstellungen mit genereller Menüstruktur, Infrastruktur, Integriertes Administrationshandbuch, Suchergebnisse, Aktivierungsdialog, Statistiken.

Die Dialogreihe innerhalb eines Stapels wird in der Zeile über dem Dialog angezeigt. Klicken Sie als Beispiel im Dashboard auf den Informationsbereich *virtuelle Maschinen* dann auf *Neue VM anlegen* so wird diese Dialogreihe angezeigt: *Virtuelle Maschinen – Assistent für virtuelle Maschinen*

Die Dialogreihe innerhalb eines Stapels wird direkt über einem Dialog angezeigt. Klicken Sie als Beispiel auf *Menü*, *Assistenten*, und dann auf *Benutzer* so wird diese Dialogreihe angezeigt: *Menü – System – Assistenten*
– Assistent für Benutzer

3.1.3 Nützliche Tastaturkürzel

- STRG + F1: Administrationshandbuch
- STRG + F9: Einstellungen sofort aktivieren
- STRG + UMSCHALT + F: Suche
- ESC: Dialog schließen

3.2 Erste Schritte

Um den V-Cube für Ihre Anforderungen einzurichten, empfiehlt es sich, zunächst eine Grundkonfiguration zur Anbindung an das lokale Netz und ans Internet vorzunehmen. Danach können Sie das System registrieren und ggf. auf den aktuellen Softwarestand updaten.

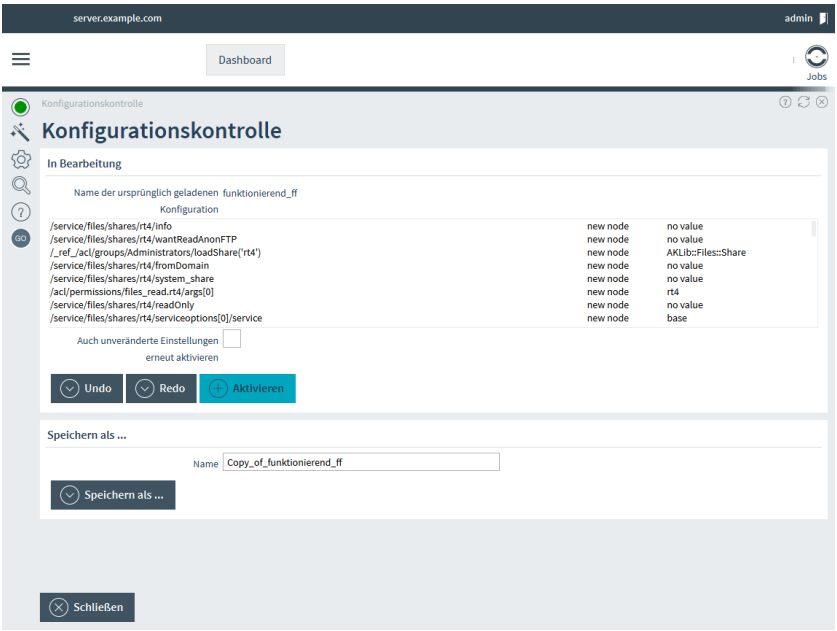
Bei der Konfiguration des Systems werden Sie auf Wunsch durch Assistenten unterstützt, die für bestimmte Konfigurationsaufgaben alle notwendigen Parameter abfragen und dann die entsprechenden Einstellungen vorbereiten. Diese von den Assistenten vorgenommenen Einstellungen können von Ihnen später manuell angepasst werden.

Im Anschluss sollten Sie sich mit dem im V-Cube genutzten Steuerungen für Festplattenverwaltung, Ethernet-Geräte und für Virtualisierung vertraut machen

3.3 Konfiguration

Der V-Cube speichert intern verschiedene Konfigurationsstände. Dazu gehört die aktuell aktive Konfiguration des Systems, dann die aktuell im Webinterface sichtbare Konfiguration und zusätzlich der Konfigurationsstand der vorherigen Konfigurationsaktivierung.

Änderungen in der Weboberfläche werden nicht direkt im System umgesetzt. Vielmehr muss eine Konfiguration explizit „aktiviert“ werden. So ist es möglich, auch eine komplexe Konfiguration über die Weboberfläche zu erstellen und anschließend komplett zu aktivieren.



Im normalen Betrieb sollte die Konfiguration des Systems mit der in der Weboberfläche einsehbaren identisch sein. Sind beide jedoch

durch Änderungen innerhalb der Weboberfläche verschieden, wird dies durch ein animiertes Symbol rechts oben in der Weboberfläche signalisiert. Das Anklicken dieses Symbols führt auf die Seite zur *Konfigurationskontrolle*. Hier werden die durchgeführten Änderungen aufgelistet und können aktiviert werden. Einzelne Änderungen können über *Undo* zurückgenommen bzw. durch *Redo* wiederhergestellt werden.

3.3.1 Schritt für Schritt: Aktivieren der Konfiguration

- Um eine Konfiguration zu aktivieren, klicken Sie auf das animierte Symbol in der Weboberfläche.
- In den Details unter *Änderungen* sehen Sie, wie viele Änderungen durchgeführt wurden.
- Sie können nun entweder *Änderungen aktivieren* oder eine *Vollständige Konfiguration* ausführen. Normalerweise aktivieren Sie nur die Änderungen. Bei der vollständigen Konfiguration werden alle Konfigurationsdateien neu geschrieben. Dies empfiehlt sich beispielsweise, wenn eine importierte Konfiguration aktiviert werden soll.
- Der Konfigurationsdurchlauf wird durch eine Animation visualisiert. In der Zeile darunter wird angezeigt, welcher Dienst gerade bearbeitet wird. Warten Sie, bis mit *Done* das Ende angezeigt wird.
- Durch Anklicken der Animation wird ein Terminalfenster geöffnet, in dem detaillierte Ausgaben zu sehen sind. Beachten Sie, dass hier auch Meldungen auftauchen, die wie eine Fehlermeldung erscheinen, aber die korrekte Funktion des Systems nicht beeinflussen.
- Sollte die Konfiguration nicht bis *Done* durchlaufen, kann dies

daran liegen, dass Sie die IP-Adresse des Systems geändert haben. Dann wird innerhalb des Konfigurationsdurchlaufs die neue IP-Adresse aktiviert. Geben Sie dann in der URL-Zeile Ihres Browsers die neue IP-Adresse ein und verbinden Sie sich erneut mit dem V-Cube.

3.3.2 Schritt für Schritt: Export und Import

- Wechseln Sie zur *Konfigurationskontrolle*.
- Unter *Speichern als ...* tragen Sie einen Namen für die aktuelle Konfiguration ein. Drücken Sie anschließend den Schalter *Speichern als*.
- Sie gelangen nun auf die Seite *Konfiguration – Konfigurationsdateien*.
- Unter *Eigene Konfigurationen* ist die gerade gespeicherte Konfiguration aufgelistet. Diese kann nun über das Kontextmenü mit *Exportieren* auf den eigenen Rechner gespeichert werden. Dazu öffnet sich der Download-Dialog Ihres Webbrowsers, sofern sie diesen nicht auf automatisches Speichern eingerichtet haben.
- Eine solche Konfigurationsdatei können Sie über den Schalter *Importieren* in die Liste der *Eigenen Konfigurationen* aufnehmen. Durch Anklicken des Schalters öffnet sich ein Dialog, der über *Durchsuchen* einen Dialog zur Dateiauswahl in Ihrem Browser startet. Wählen Sie die gewünschte Datei auf Ihrer Festplatte aus und klicken Sie anschließend *Importieren*.
- Die Konfiguration ist nun nur auf dem V-Cube gespeichert, aber weder in der Weboberfläche einsehbar noch aktiviert.
- Im Kontextmenü der Konfigurationsdatei können Sie diese durch *Bearbeiten* in die Weboberfläche „laden“.
- Nun können Sie die Konfiguration in der Weboberfläche bearbeiten oder über den gewohnten Mechanismus aktivieren.

3.3.3 GUI-Referenz: *Konfigurationskontrolle*

(Dieser Dialog befindet sich unter *Konfiguration – Konfigurationskontrolle*)

In diesem Dialog wird der Name der geladenen Konfiguration angezeigt. Die aktuell in der Weboberfläche sichtbare Konfiguration kann hier (innerhalb des V-Cubes) gespeichert werden.

3.3.3.1 Abschnitt *In Bearbeitung*

Felder in diesem Abschnitt

- *Name der ursprünglich geladenen Konfiguration*: Hier wird der Name der ursprünglich zur Bearbeitung geladenen Konfiguration angezeigt.
- *Änderungen*: Hier wird die Anzahl der Änderungen in den jeweiligen Bereichen angezeigt. Mit Klicken auf *Details* werden genauere Informationen angezeigt.
- *Auch unveränderte Einstellungen erneut aktivieren*: Mit dieser Option werden alle Einstellungen des Systems, auch unveränderte, aktiviert. Dieser Vorgang kann einige Zeit in Anspruch nehmen.

  Hinweis: Ändert sich bei einer Konfiguration die IP-Adresse des Systems, ist die Konfigurationsoberfläche nicht mehr erreichbar. Es muss dann eine Verbindung zu der neuen IP-Nummer aufgebaut werden.

Aktionen für diesen Dialog

- *Undo*: Diese Aktion macht die Änderungen stufenweise rückgängig. Es werden pro Stufe immer alle Änderungen in einem Dialog zurückgenommen.

- *Redo*: Diese Aktion stellt zurückgenommene Änderungen wieder her.
- *Aktivieren*: Diese Aktion aktiviert die Änderungen, die gerade in der aktuellen Konfiguration vorgenommen wurden.

  Hinweis: Ändert sich bei einer Konfiguration die IP-Adresse des Systems, ist die Konfigurationsoberfläche nicht mehr erreichbar. Es muss dann eine Verbindung zu der neuen IP-Nummer aufgebaut werden.

3.3.3.2 Abschnitt *Speichern als ...*

Die aktuelle Konfiguration kann im System gespeichert werden.

Felder in diesem Abschnitt

- *Name*: Hier wird der Name angegeben, unter dem die Konfiguration gespeichert wird.

Aktionen für diesen Dialog

- *Speichern als ...*: Diese Aktion speichert die Konfiguration.

3.3.3.3 Abschnitt *Aktivierung ...*

Wird die Konfiguration aktiviert, ist in diesem Abschnitt der Fortschritt des Vorgangs sichtbar. Mit einem Klick auf den Fortschrittsbalken wird auf eine detaillierte Ausgabe umgeschaltet. Ein erneuter Klick führt zu dem einfachen Balken zurück.

3.3.3.4 Aktionen für diesen Dialog

- *Zurück*: Mit dieser Aktion gelangen Sie zurück zum Aktivierungsdialog.

3.3.4 GUI-Referenz: *Konfigurationsdateien*

(Dieser Dialog befindet sich unter *Konfiguration – Konfigurationsdateien*)

Dieser Dialog zeigt alle im V-Cube gesicherten Konfigurationen. Sie können hier exportiert, geladen und gelöscht werden. Zusätzlich ist der Import von Konfigurationen möglich.

3.3.4.1 Abschnitt *Konfigurationen*

Hier werden alle vom System automatisch gespeicherten Konfigurationen aufgelistet. Sie können hier in die Weboberfläche geladen werden.

Spalten in der Tabelle

- *Name*: Der Name der Konfiguration. Dies ist eine intern erzeugte Bezeichnung.
- *Kommentar*: Hier wird ein kurzer Kommentartext mit dem exakten Namen der Konfigurationsdatei angezeigt.
- *Datum*: Hier wird das Datum angezeigt, an dem die Konfiguration gespeichert wurde.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion wird die gespeicherte Konfiguration geladen. Dabei werden die Konfigurationseinstellungen in die Weboberfläche übernommen, jedoch nicht aktiviert.

3.3.4.2 Abschnitt *Eigene Konfigurationen*

Alle in der *Konfigurationskontrolle* gespeicherten Konfigurationen sind in diesem Dialog aufgelistet. Sie können hier geladen, exportiert oder gelöscht werden.

Spalten in der Tabelle

- *Name*: Der Name der Konfiguration. Dies ist der Name, der beim Speichern der Konfiguration vergeben wurde.
- *Datum*: Hier wird das Datum angezeigt, an dem die Konfiguration gespeichert wurde.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion wird die gespeicherte Konfiguration geladen. Dabei werden die Konfigurationseinstellungen in die Weboberfläche übernommen, jedoch nicht aktiviert.
- *Exportieren*: Mit dieser Aktion kann die ausgewählte Konfiguration über das Webinterface heruntergeladen und auf dem lokalen Rechner gespeichert werden. Die Konfiguration enthält keine Passwörter, Zertifikate oder Filterlisten.
- *Löschen*: Mit dieser Aktion wird die ausgewählte Konfiguration gelöscht.

3.3.4.3 Aktionen für diesen Dialog

- *Importieren*: Mit dieser Aktion kann eine Konfiguration über die Weboberfläche in das System importiert werden.

3.3.4.4 *Konfiguration importieren*

(Dieser Dialog befindet sich unter *Konfiguration – Konfigurationsdateien*)

Über diesen Dialog kann eine Konfigurationsdatei vom lokalen Rechner in das System importiert werden.

Felder in diesem Dialog

- *Datei*: Über dieses Feld wird auf dem lokalen System ein Dialog geöffnet, über den die Datei auf dem lokalen Rechner ausgewählt werden kann.
- *Ergebnis*: Bei gestartetem Import wird hier die Ausgabe des Vorgangs angezeigt.

Aktionen für diesen Dialog

- *Importieren*: Mit dieser Aktion wird der Import gestartet. Diese Konfiguration wird unter dem Namen *conf_upload* mit angehängtem Datum und Uhrzeit abgespeichert. Um die Konfiguration zu übernehmen, muss sie mit *Bearbeiten* in die Weboberfläche geladen und dann aktiviert werden.

3.3.5 Schritt für Schritt: Export von Benutzerdaten

- Unter *Überwachung/Auswertung – Auswertungen – Export von Benutzerdaten* können die aktuell angelegten Benutzer exportiert werden.
- Um die Liste weiter verarbeiten zu können, bietet sich das CSV-Format an. Dabei handelt es sich um eine Textdatei; jeder Benutzer ist in einer Zeile erfasst, die Werte sind mit Komma getrennt.
- Wählen Sie als Format *CSV-Datei* und klicken Sie auf *Exportieren*. Der Download-Dialog Ihres Browsers öffnet sich, und Sie können die Datei auf Ihrem Rechner speichern.
- Sie können diese Datei mit einem Texteditor bearbeiten oder in eine Tabellenkalkulation oder Datenbank importieren.
- Sie können in diesem Format eine Benutzerliste vorbereiten und unter *Benutzungsrichtlinien – Benutzer – Benutzer importieren* importieren.

3.3.6 GUI-Referenz: Benutzerdaten exportieren

3.3.6.1 *Export von Benutzerdaten*

Über diesen Dialog kann eine PDF- oder CSV-Datei mit den Daten der Benutzer erstellt werden. In dem erstellten PDF-Dokument stehen der FQDN dieses Systems sowie Login und Passwort der ausgewählten Benutzer. Für jeden Benutzer wird dabei eine eigene Seite erstellt, die ihm ausgehändigt werden kann. Die CSV-Datei wird als reine Textdatei erstellt und enthält Login, Titel, Vorname, Nachname, Passwort und Telefonnummer. Sie dient hauptsächlich zum vereinfachten Import von Benutzerprofilen in andere Systeme.

3.3.6.2 Felder in diesem Dialog

- *Exportiere Benutzerdaten in eine*: Über dieses Feld wird ausgewählt, ob eine PDF- oder CSV-Datei mit den Daten der Benutzer erstellt wird.
- *Sprache des PDF*: Das PDF kann wahlweise in Deutsch oder Englisch erstellt werden.
- *Alle Benutzer oder einzelne auswählen?*: Hier wird festgelegt, ob die Daten aller lokal auf dem System angelegten Benutzer oder nur die Daten ausgewählter Benutzer exportiert werden.
- *Benutzer auswählen*: Hier muss mindestens ein Benutzer ausgewählt werden, dessen Daten in ein PDF exportiert werden.

3.3.6.3 Aktionen für diesen Dialog

- *Exportieren*: Mit dieser Aktion wird der Export der Benutzerdaten gestartet.

3.3.7 GUI-Referenz: Konfigurationsreport

3.3.7.1 *Konfigurationsreport*

Über diesen Dialog kann ein Report der aktuellen Server-Konfigurationsdatei erstellt werden. Der Report wird in der gewählten Sprache generiert und als PDF-Dokument zur Verfügung gestellt.

In dem erzeugten Report sind aufbereitete Informationen über die Serverkonfiguration beinhaltet. So wird im Report der Bezug zwischen Berechtigungen und den einzelnen Elementen von Berechtigungsgruppen dargestellt. Der Report gibt auf einen Blick Aufschluss darüber, welcher Benutzer welche Berechtigungen besitzt. Aufgeli-

stet werden darin Zusammenfassungen von Gruppen, Benutzern, Berechtigungen, Netzwerken und Rechnern.

Je nach Umfang der Serverkonfiguration wird der Bericht zwischen 6 und 500 Seiten stark.

3.3.7.2 Felder in diesem Dialog

- *Sprache des Reports*: Hier wird die Sprache des Konfigurationsreports gewählt. Der Report kann in Deutsch oder Englisch erstellt werden.
- *Konfigurationsdatei*: Hier wird die Datei ausgewählt, über die der Report erstellt werden soll.

3.3.7.3 Aktionen für diesen Dialog

- *Report generieren*: Mit dieser Aktion wird der Report erzeugt und zum Herunterladen bereitgestellt.

3.3.8 GUI-Referenz: Benutzer importieren

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Benutzer – Benutzer importieren*)

In diesem Dialog kann eine Datei im CSV-Format mit Benutzerdaten importiert werden. Über diese Funktion und den vorhergehenden Export von Benutzerdaten auf einem anderen System können Benutzer mit ihren Passwörtern auf ein zweites System übernommen werden (S. 64).

Die Datei muss pro Zeile einen Benutzer enthalten; die einzelnen

Felder werden durch Komma getrennt. Es werden der Reihe nach folgende Werte erwartet: Login, Titel, Vorname, Nachname, Passwort und Telefonnummer. Weitere Einstellungen wie Mail-Aliase oder Fax-Nummer müssen über die Oberfläche des V-Cubes vorgenommen werden.

3.4 Assistenten

Die grundlegende Konfiguration des V-Cubes kann mit Hilfe von Assistenten durchgeführt werden. Die Assistenten sind in die Weboberfläche integrierte Dialoge, die für bestimmte Aufgaben die notwendigen Parameter erfragen, diese mit weiteren sinnvollen Annahmen bzw. Vorgabewerten kombinieren und Konfigurationseinstellungen vornehmen.

Alle von den Assistenten durchgeführten Konfigurationen sind in der normalen Administrationsoberfläche sichtbar und als solche erkennbar. Neu angelegte Objekte sind immer im Kommentarfeld als „Generated by Wizard“ bezeichnet. Die am System durchgeführten Einstellungen sind damit im Nachhinein nachvollziehbar und können durch den Administrator geändert werden.

In den folgenden Abschnitten werden die einzelnen Assistenten vorgestellt. Im Abschnitt „Ablauf“ ist jeweils skizziert, welche Fragen der Assistent stellt und welche Informationen er erwartet. Der Abschnitt „Konfiguration“ ist technisch anspruchsvoller und erläutert, welche Konfigurationsänderungen der Assistent im Einzelnen durchführt. Mit diesen Informationen ist es möglich, die Änderungen am V-Cube durch einen Assistenten nachzuvollziehen und anzupassen.

Da manche Assistenten teilweise Konfigurationen löschen bzw. bei mehrfachem Aufruf manuelle Anpassungen teilweise verwerfen,

sollte nur die erste Installation des Systems über die Assistenten durchgeführt werden. Danach sollten die Assistenten mit einiger Vorsicht genutzt werden, insbesondere wenn parallel eine manuelle Konfiguration des Systems erfolgt.

3.4.1 *Bare Metal Restore*

(Dieser Dialog befindet sich unter *Assistenten – Bare Metal Restore*)

Benutzen Sie diesen Assistenten, um schnellstmöglich Ihren Server nach einem vollständigen Systemcrash wieder in Betrieb zu nehmen (Bare Metal Restore, Desaster-Recovery).

3.4.1.1 Ablauf und Konfiguration

Im ersten Schritt wird eine Recovery Token-Datei (recovery-token_host_datum.rto) gewählt, welche der Administrator per E-Mail erhielt.

Im nächsten Schritt werden folgende Aktionen automatisch ausgeführt:

- Überprüfung des Recovery Token
- Installation der Lizenz
- Installation der lizenzierten Zusatzmodule
- Einrichtung des Sicherungsziels und des Sicherungssystems
- Wiederherstellung des Inhaltsverzeichnisses (Katalog) aller Sicherungsdaten

Im letzten Schritte werden Informationen zur weiteren Vorgehensweise angezeigt. Es sind alle Einstellungen vorhanden, um auf alle gesicherten Daten zuzugreifen und diese wieder herzustellen.

Es ist zu beachten, dass während einer vollständigen Datenwie-

derherstellung in das laufende System keine manuellen Interaktionen mit dem System oder einzelnen Diensten getätigt werden sollen.

3.4.2 *Assistent für die Stammdaten*

(Dieser Dialog befindet sich unter *Assistenten – Stammdaten*)

Dieser Assistent fragt wichtige Daten über den Standort des Unternehmens ab. Diese Daten sind für die Registrierung und Aktivierung der Lizenz sowie später bei der Erstellung von Zertifikaten notwendig.

3.4.2.1 Ablauf

Dieser Assistent fragt die Adresse des Unternehmens ab. Bei mehreren V-Cube innerhalb eines Unternehmens sollte die Abteilung bzw. der Standort passend zu jedem System gesetzt werden.

Weiterhin erfragt der Assistent die Einstellungen für das Telefonsystem wie Landesvorwahl, Ortsnetz und Amtsholung.

3.4.2.2 Konfiguration

Die übergebenen Werte werden nach *Benutzungsrichtlinien – Umgebung – Standort* übernommen und können dort jederzeit angepasst werden.

3.4.3 *Assistent für die Einrichtung des Netzwerks*

(Dieser Dialog befindet sich unter *Assistenten – Netzwerk*)

Mit Hilfe dieses Assistenten wird die Netzwerkverbindung des Servers eingerichtet. Zusätzlich wird für den V-Cube ein Serverzertifikat erzeugt, welches von einer eigenen CA signiert wird.

3.4.3.1 Ablauf

Dieser Assistent fragt den Hostnamen des V-Cubes ab. Dabei soll der FQDN angegeben werden, also der vollständige Name inkl. der Domain.

Anschließend wird die IP-Adresse und danach die zugehörige Netzmaske abgefragt, die der V-Cube auf der ersten Netzwerkschnittstelle (*eth0*) verwenden soll.

Im dritten Schritt fragt der Assistent ab, welcher DNS-Server verwendet werden soll. Ist im Netzwerk schon ein DNS-Server aktiv, kann hier dessen IP-Adresse eingetragen werden. Soll der V-Cube als DNS-Server verwendet werden, kann als IP-Adresse *127.0.0.1* eingetragen werden. Wenn erforderlich, kann auch ein alternativer Nameserver gesetzt werden.

Für die Anbindung an andere Netze, wie z. B. das Internet, wird nun noch ein Default-Gateway eingetragen.

3.4.3.2 Konfiguration

Zunächst wird überprüft, ob die angegebene IP-Adresse für die Schnittstelle *eth0* zu einem vorhandenen Netzwerk gehört. Falls nicht, wird ein neues Netz *LocalNet* angelegt. Existiert bereits ein Netzwerk

dieses Namens, wird dem neu angelegten Netz eine fortlaufende Nummer angehängt.

Nun wird überprüft, ob es bereits einen Ethernet-Link gibt, der die angegebene IP-Adresse besitzt. Falls nicht, wird ein neuer Link angelegt. Dieser Link wird auf die höchste Priorität gesetzt, falls bereits Links mit dem gleichen erreichbaren Netz existieren.

Im Anschluss wird eine Gruppe *LocalNetworks* angelegt. Das angelegte lokale Netz wird als Mitglied aufgenommen, und die Berechtigungen für *DNS* (inkl. *rekursiver Anfragen*), *Webadmin* und *SSH-Connect* werden aktiviert.

Der Nameserver wird aktiviert, die (Sub-)Domain aus dem FQDN des Systems selbst wird in die Domainsuchliste aufgenommen. Das Weiterleiten von DNS-Anfragen wird deaktiviert, der V-Cube befragt die Root-Nameserver.

Für die (Sub-)Domain aus dem FQDN des V-Cubes wird im DNS eine Vorwärtszone angelegt, zu der der V-Cube *Master* ist.

Für das angelegte lokale Netzwerk wird im DNS eine Rückwärtszone erzeugt. Auch hier ist der V-Cube *Master*.

Aus den Daten des *Standort* wird ein zehn Jahre gültiges CA-Zertifikat erzeugt. Das CA-Zertifikat wird mit der Passphrase gesichert.

Ein weiteres Zertifikat wird zur Verwendung durch die Serverdienste im V-Cube erstellt. Dieses ist von der CA signiert und ebenfalls zehn Jahre gültig.

Abschließend werden die Konfigurationsänderungen aktiviert. Wurde für das lokale Netz die IP-Adresse geändert, ist der V-Cube nicht mehr unter der alten IP-Adresse erreichbar.

3.4.4 *Registrierung des Servers*

(Dieser Dialog befindet sich unter *Assistenten – Registrierung*)

Mit Hilfe dieses Assistenten wird der V-Cube registriert. Dieser Assistent zeigt die beim Hersteller hinterlegten Daten des Kunden an. Falls Kundendaten nicht vorhanden sind, werden diese vom Assistenten abgefragt.

3.4.4.1 Ablauf

Im ersten Schritt wird die Erreichbarkeit des Collax Lizenzierungs-Servers getestet. Anschließend kann die erhaltene Lizenznummer eingegeben werden.

Falls Daten des Kunden vorhanden sind, werden diese nachfolgend zur Überprüfung angezeigt. Gegebenenfalls ist eine E-Mail-Adresse anzugeben. Wenn keine Daten vorhanden sind, kann die Registrierung mit einem Collax Web Account-Login oder mit der Eingabe von Kundendaten erfolgen. Im Anschluss werden die Daten zur Kontrolle angezeigt.

Über den Administrations-Newsletter können wichtige Informationen über Produkt-Updates, neue Funktionen oder Sicherheitsinformationen empfangen werden.

Der Server wird nach der Zusammenfassung registriert. Durch die Registrierung kann die Software-Update-Funktionen des Servers und der registrierten Software-Module für die Dauer der Laufzeit genutzt werden. Detailinformationen über die Lizenz können über das Collax Web Account unter http://www.collax.com abgerufen werden.

3.4.5 *Assistent für Benutzer*

(Dieser Dialog befindet sich unter *Assistenten – Benutzer*)

Mit diesem Assistenten können einzelne Benutzer angelegt werden. Alternativ kann eine vorbereitete Datei im CSV-Format importiert werden, in der die Benutzer in Listenform hinterlegt sind.

3.4.5.1 Ablauf

Der Assistent fragt zunächst ab, ob ein einzelner Benutzer angelegt werden soll oder eine Liste im CSV-Format importiert werden soll.

Bei einem einzelnen Benutzer werden Vorname, Nachname und Login abgefragt. Der Assistent prüft, ob das Login bereits vergeben ist. In diesem Fall muss ein anderes Login gewählt werden. Danach wird das Kennwort für den Benutzer abgefragt, zu dem der Assistent einen Vorschlag liefert, der übernommen werden kann.

Beim Import der Liste muss eine Datei im CSV-Format ausgewählt und über einen Web-Upload auf den V-Cube transferiert werden.

3.4.5.2 Konfiguration

Der Benutzer wird neu angelegt und der Gruppe *Users* hinzugefügt.

Abschließend werden die Änderungen der Konfiguration aktiviert.

3.4.6 *Datensicherung*

3.4.6.1 Felder in diesem Formular

- : Wählen Sie aus, ob Sicherungspläne für lokale Sicherungen erstellt werden sollen, oder ob Medien für eine Virtual Tape Library mit USB oder eSATA-Laufwerken eingerichtet werden soll.

3.4.7 *Assistent für Datensicherung*

(Dieser Dialog befindet sich unter *Assistenten – Datensicherung*)

Mit Hilfe dieses Assistenten richten Sie Sicherungspläne für Datensicherungen ein. Diese Sicherungspläne sind gleichermaßen für Sicherungen Ihres Collax Servers wie für Client-Rechner gültig und notwendig. Im Allgemeinen genügen diese generierten Sicherungspläne auch fortgeschrittenen Anwendungsfällen. Detaillierte, manuelle Modifikationen dieser Pläne sind möglich.

3.4.7.1 Ablauf

Im ersten Schritt wird die Periode für Vollsicherungen festgelegt. Es kann zwischen monatlicher, wöchentlicher oder täglicher Vollsicherung gewählt werden. Ergänzende Inkrementelle Sicherungen werden zu einem späteren Zeitpunkt konfiguriert.

Danach wählen Sie genauere Spezifikationen Ihrer Sicherungszeitpunkte.

Im dritten Schritt fragt der Assistent nach der Backup-Strategie.

Hierbei kann zwischen „Lineare Sicherung“, „Einfache Rotation“ und, abhängig von der Wahl der Periode, zwischen „Türme von Hanoi“ und „Großvater, Vater, Sohn“ gewählt werden.

Bei „Linearer Sicherung“ wird fortlaufend auf das jeweilige Ziel gesichert; neue Medien werden angelegt beziehungsweise angefordert, sobald das letzte Medium voll ist.

Bei „Einfacher Rotation“ werden Medien zyklisch für Sicherungen benutzt; die Zyklusdauer richtet sich nach der Periode für Vollsicherungen.

Ziel des Schemas „Türme von Hanoi“ ist es, so lange wie möglich auf alte Sicherungsdaten zurückgreifen zu können, ohne dabei zu viel Platz zu verbrauchen. Es ist aber zu beachten, dass der Platzbedarf dieses Schemas höher ist als der der anderen Schemata.

Das Schema „Großvater, Vater, Sohn“ hält drei Generationen von Sicherungen vor. Dabei wird monatlich eine Sicherung auf gesonderte Medien geschrieben, wöchentlich auf einen zweiten Satz, und täglich auf die Standardmedien. Viele Administratoren sichern die Vater- und Sohn-Generationen als differenzielle beziehungsweise inkrementelle Sicherungen. Diese Veränderung kann leicht im generierten Plan vorgenommen werden.

Bestimmen Sie im vierten Schritt, wie lange gesicherte Daten aufbewahrt werden sollen. Gemeinsam mit der Datenmenge ergibt sich daraus die benötigte Anzahl an Bändern bzw. der Gesamtplatzbedarf der Sicherung.

Im letzten Schritt wird eine Zusammenfassung der im Assistenten vorgenommenen Einstellungen angezeigt. Der Sicherungsplan wird mit einem Klick auf „Fertigstellen“ erstellt.

3.4.7.2 Konfiguration

Der Assistent erstellt einen Sicherungsplan, für den automatisch ein Name, der auf den konfigurierten Eigenschaften basiert, gewählt wird.

Weiterhin wird eine Zuordnung erstellt, die den neuen Plan mit dem lokalen Default-Ziel und dem lokalen System verbindet. Dies gescheit nur, wenn das Default-Ziel existiert und in der vorangegangenen Maske die Checkbox „Benutze diesen Sicherungsplan für eine lokale Sicherung“ aktiviert wurde.

Danach wird die Konfiguration aktiviert.

3.4.8 *Assistent für Virtual Tape Libraries mit Wechselmedien*

3.4.8.1 Felder in diesem Formular

- : Mit Hilfe dieses Assistenten richten Sie Virtuelle Bandwechsler auf Wechselmedien wie USB- oder eSATA-Platten ein.

4 Benutzungsrichtlinien

4.1 Einführung

Über die Benutzungsrichtlinien wird der Zugriff auf die einzelnen Dienste im V-Cube gesteuert. Dahinter verbirgt sich ein ausgefeiltes Konzept mit mehrstufiger Sicherheit. Die Benutzungsrichtlinien bilden somit ein zentrales Element in der Konfiguration des Systems.

Grundlage der Richtlinien sind die „Gruppen“. Jede Gruppe beinhaltet „Mitglieder“ und gewährt diesen „Berechtigungen“. Mitglied einer Gruppe können jeweils Benutzer, Computersysteme („Hosts“) oder auch ganze Netze sein. Die Berechtigungen sind in weiten Grenzen einstellbar.

Ein Benutzer identifiziert sich gegenüber dem V-Cube durch Angabe eines Logins mit zugehörigem Passwort. Ein Computersystem benutzt im Netzwerk eine IP-Adresse (mehr dazu im Abschnitt Netzwerke (S. 137)). Diese IP-Adresse sieht der V-Cube als Identifikation, wenn er Pakete von dem Computer empfängt. In einem lokalen Netz werden IP-Adressen aus einem zusammenhängenden Bereich vergeben, dieser Bereich wird als „Netz“ oder „Netzwerk“ bezeichnet.

Die Kombination von zwei völlig unterschiedlichen Arten von Mitgliedern (Computersystemen und menschlichen Benutzern) zu einer Gruppe bietet weitreichende Möglichkeiten, um den Zugriff auf Dienste zu sichern.

Bei einfachen Diensten, wie beispielsweise dem Nameserver, wird die Zugriffskontrolle nur anhand der anfragenden IP-Adresse durchgeführt. Üblicherweise wird der Zugriff auf lokale Dienste nur für interne Netze und aus Sicherheitsgründen nicht aus dem Internet gestattet. In diesem Fall muss die IP-Adresse eines Computers, dem

der Zugriff auf den Nameserver gestattet werden soll, Mitglied der Gruppe sein. Dazu kann entweder der Computer als einzelner Host oder das Netzwerk, zu dem seine IP-Adresse gehört, als Mitglied in die Gruppe aufgenommen werden.

Bei komplexeren Diensten, wie dem Abruf von E-Mail über POP3 oder IMAP, ist zusätzlich eine Benutzerauthentifizierung erforderlich. Über dieses Login kann der Serverdienst das richtige Postfach öffnen. Über das Passwort kann er sicherstellen, dass nur berechtigte Benutzer Zugriff auf die E-Mail erhalten. Die Mitgliedschaft der IP-Adresse wird auch hier geprüft. Kommt der Zugriff aus einem unberechtigten Netzwerkbereich, wird der Zugriff in der Firewall geblockt und nicht zum E-Mail-Dienst durchgelassen.

Bei manchen Diensten ist die Authentifizierung optional möglich. Beim Webproxy kann sie deaktiviert werden. Damit ist der Webproxy von allen Computern aus nutzbar, deren IP-Adresse bzw. deren Netzwerk Mitglied der entsprechenden Gruppe ist.

Andere Dienste erfordern nur die Mitgliedschaft eines Benutzers, nicht jedoch eines Computers. Bei der ISDN-Einwahl wird beispielsweise Login und Passwort abgefragt. Da der Anruf über ISDN kommt, ist keinerlei IP-Adresse des einwählenden Computers prüfbar.

Durch die Einstellungen in der Gruppenverwaltung wird in den meisten Fällen außer der Konfiguration der Dienste immer eine Firewall-Konfiguration vorgenommen, die bestimmte IP-Adressen zulässt und andere sperrt. Im Fall des E-Mail-Beispiels ist es daher nicht ausreichend, lediglich den Benutzer in die Gruppe aufzunehmen. In diesem Fall würde die Firewall den Zugriff des Rechners abblocken, so dass keinerlei Kommunikation zwischen E-Mail-Client und Mail-Dienst im V-Cube zustande kommt.

Je nach Einstellung protokolliert die Firewall erfolgreiche und fehlgeschlagene Zugriffe in der Logdatei. Dies kann bei fehlschlagenden Zugriffen auf Dienste, die im V-Cube selbst laufen, dazu verleiten,

in der Firewallmatrix (S. 217) Berechtigungen zu setzen. Dies wäre jedoch falsch. Für Zugriffe auf Dienste im V-Cube sind immer die Rechte in den *Benutzungsrichtlinien* ausschlaggebend.

Eine Mitgliedschaft in mehreren Gruppen ist möglich. Die Rechte sind additiv, d. h., es reicht die Berechtigung in einer einzigen Gruppe, um dieses Recht zu besitzen.

4.2 Vordefinierte Gruppen

Serienmäßig sind bereits mehrere Gruppen angelegt. Die Gruppe *Internet* beinhaltet als Mitglied das Netz „Internet“ und damit alle IP-Adressen außerhalb der eigenen Netzwerkbereiche. Alle Berechtigungen, die über diese Gruppe erteilt werden, gelten damit für alle Computer irgendwo im Internet. Diese Gruppe sollte daher mit so wenig Rechten wie möglich ausgestattet werden.

Die Gruppe *LocalNet* hingegen beinhaltet im Gegensatz als Mitglied das lokale Netz und gestattet diesem Zugriffe auf Dienste im V-Cube.

Über die Gruppen *Users* und *Admins* können Berechtigungen für lokale Benutzer vergeben werden. *Admins* sollen dabei lokale Benutzer sein, denen administrative Zugriffe erlaubt werden, etwa auf den Fax-Dienst oder auf das Viren-Quarantäneverzeichnis. In diesen Gruppen ist das lokale Netz ebenfalls Mitglied, damit in der Firewall der Zugriff auf die Dienste freigeschaltet wird.

Der Zugriff auf die Benutzungsrichtlinien kann von zwei Seiten erfolgen, einerseits über die Konfigurationsdialoge zu den Benutzungsrichtlinien selbst und andererseits bei der Konfiguration der Dienste. Dazu sind in der Weboberfläche jeweils Reiter *Berechtigungen* vorhanden. Über diese erscheint ein Dialog, in dem einzelne Berechtigungen des Dienstes an eine oder mehrere Gruppen vergeben werden können.

4.3 Berechtigungen

In den *Grundeinstellungen* lässt sich für jede Gruppe festlegen, ob sie in der Benutzerverwaltung sichtbar ist. Dies ist sinnvoll für Gruppen, die eine Benutzermitgliedschaft erfordern. So kann ein neuer Benutzer beim Anlegen direkt den entsprechenden Gruppen zugeordnet werden. Weiterhin lassen sich für jede Gruppe Quotas (S. 283) festlegen. Dies sind Begrenzungen des verfügbaren Speicherplatzes für Freigaben (Shares) und E-Mail.

Die übrigen Berechtigungen sind über den Reiter bzw. das Kontextmenü *Berechtigungen* einstellbar. Auf dieser Seite gibt es verschiedene Kategorien mit einzelnen Berechtigungen. Einige Kategorien sind auf einzelne Dienste beschränkt (*Fax*, *LDAP*, *Mail* usw.).

Unter der Kategorie *Firewall* sind alle Dienste im V-Cube aufgeführt, deren Berechtigung nur anhand einer IP-Adresse vergeben wird. Hierzu müssen keine Benutzer angelegt werden. Durch eine gesetzte Berechtigung wird der entsprechende Netzwerkport in der Firewall für die zugehörigen Netze oder Rechner geöffnet.

Im Abschnitt *RAS* werden die Berechtigungen zur Einwahl auf den V-Cube vergeben, u. a. ist hier mit *SSH* die verschlüsselte Konsolenverbindung auf den V-Cube selbst einstellbar.

Im V-Cube besteht die Möglichkeit, einzelnen Benutzern die gesamte oder Teile der Administration freizuschalten. Dazu können im Abschnitt *Role* die gewünschten Kategorien aktiviert werden.

4.4 Gruppenplanung

Mit den vordefinierten Gruppen können bereits viele Konfigurationen abgedeckt werden. Es empfiehlt sich jedoch, für bestimmte Aufgaben bedarfsweise eigene Gruppen anzulegen und in den Gruppen *Users* bzw. *LocalNet* nur den Zugriff auf die Basisdienste (DNS, NTP usw.) zu regeln, bei denen keine Zugriffsbeschränkungen zu erwarten sind.

Für den gesamten Komplex „E-Mail“ kann beispielsweise eine eigene Gruppe angelegt werden. Damit können lokale Benutzer angelegt werden, die keinerlei E-Mail-Berechtigung erhalten, weil sie nicht Mitglied dieser Gruppe werden. Durch die Mitgliedschaft in anderen Gruppen kann ihnen aber die Nutzung weiterer Dienste im Netzwerk ermöglicht werden.

Die notwendigen Gruppen sollten bereits zu Beginn der Konfiguration festgelegt und angelegt werden. So können die notwendigen Rechte den entsprechenden Gruppen in den Konfigurationsdialogen der einzelnen Dienste zugewiesen werden.

Beim Anlegen von Gruppen gibt es zwei unterschiedliche Strategien: Die „benutzerbezogene“ und die „dienstbezogene“ Verwaltung der Gruppen.

Bei benutzerbezogener Verwaltung werden die Benutzer nach Arbeitsbereichen in Gruppen aufgeteilt. Beispiele für Gruppen wären dann „Azubis“, „Buchhaltung“, „Vertrieb“ usw. Jeder Benutzer sollte nur Mitglied in einer einzigen Gruppe sein.

Bei der dienstbezogenen Verwaltung wird für jeden Dienst eine Gruppe angelegt. Dabei können Dienste zu einem bestimmten Komplex zusammengefasst werden, beispielsweise die Dienste SMTP, POP3 und IMAP in einer Gruppe „Mailusers“. Diese Vorgehensweise ist wesentlich flexibler und übersichtlicher, da alle Einstellungen

zu einem Dienst(-bereich) zentral in einer Gruppe vorgenommen werden.

Oft werden beide Methoden gemischt genutzt. Bei gut angelegten Gruppenstrukturen ist dies auch bei größeren Installationen übersichtlich.

4.4.1 Beispiel: Benutzerbezogene Gruppen

Als Beispiel für benutzerbezogene Gruppen soll eine Schule betrachtet werden. Das Netzwerk der Schule lässt sich in drei Bereiche unterteilen: zunächst zwei Klassenräume mit Computern, an denen die Schüler unterrichtet werden und in bestimmten Stunden unter Aufsicht selbständig arbeiten dürfen. Den zweiten Bereich bildet das Lehrerzimmer, in dem einige Computer stehen, die von den Lehrern zur Unterrichtsvorbereitung und für E-Mail-Verkehr genutzt werden. Der dritte Bereich schließlich ist die Verwaltung mit den Computern des Direktors, seines Stellvertreters und der Sekretärin. Hier werden Dokumente mit Schulinterna bearbeitet sowie E-Mail ausgetauscht.

Für die Klassenräume soll nur Internetsurfen auf einigen wenigen festgelegten Webseiten erlaubt sein. Die Schüler erhalten keine eigene E-Mail-Adresse.

Die Lehrer erhalten unbeschränkten Zugriff auf alle Webseiten. Diese müssen jedoch über einen Proxy aufgerufen werden, der eine Filterung auf Viren durchführt. Die Lehrer bekommen zudem ein Postfach mit einer schulbezogenen E-Mail-Adresse und können einen zentralen Fileserver nutzen.

Bei benutzerbezogener Verwaltung müssen unterschiedliche Gruppen von Benutzern identifiziert werden. Dies führt hier zu den Gruppen „Schüler“, „Lehrer“ und „Verwaltung“.

Alle Computer können im gleichen Netzwerkbereich sein. Sinnvoll

ist jedoch eine Trennung der Klassenräume von dem Bereich Lehrerzimmer/Verwaltung durch eine Firewall.

Von den im V-Cube vordefinierten Gruppen bleibt „Internet“ bestehen. Diese Gruppe reguliert Zugriffe aus dem Internet auf dem V-Cube. Die anderen Gruppen können entfernt werden.

Nun werden die drei Gruppen „Schueler“, „Lehrer“ und „Verwaltung“ angelegt. Ist in der Schule nur ein physikalisches Netz vorhanden (*LocalNet*), wird dieses als Mitglied in alle drei Gruppen aufgenommen. Wurde eine Trennung der Netze durchgeführt, sollte das *SchuelerNetz* als Mitglied in die Gruppe „Schueler“ aufgenommen werden, und entsprechend das „LehrerNetz“ in die anderen beiden Gruppen. Anschließend werden die Benutzer angelegt und den Gruppen zugeordnet.

Einen Dienst, den alle drei Gruppen nutzen müssen, ist DNS. Dieser Dienst wird in den Benutzungsrichtlinien aller drei Gruppen gesetzt.

Bei der Einrichtung des E-Mail-Systems erhalten in den Benutzungsrichtlinien nur die Gruppen „Lehrer“ und „Verwaltung“ ein Postfach und die entsprechende Zugangsberechtigung.

Nun wird eine Laufwerksfreigabe für die Lehrer angelegt, auf die die Gruppe „Lehrer“ Schreib- und Lesezugriff erhält. Auf die gleiche Freigabe erhält auch die Gruppe „Verwaltung“ Schreib- und Leseberechtigung. So ist ein Datenaustausch möglich.

Abschließend wird eine eigene Laufwerksfreigabe für die Verwaltung eingerichtet, auf die nur die Gruppe „Verwaltung“ Zugriff erhält.

Kommt nun ein neuer Schüler oder ein neuer Lehrer auf die Schule, wird er als Benutzer angelegt und der entsprechenden Gruppe hinzugefügt. Analog wird eine Person beim Abgang von der Schule gelöscht und damit aus der Gruppe entfernt.

Dieses Beispiel zeigt, dass eine benutzerbezogene Gruppenstruktur dann ihre Vorteile ausspielen kann, wenn sich die Benutzer in

mehrere Gruppen trennen lassen und es keine (oder sehr wenige) Überlappungen gibt.

4.4.2 Beispiel: Dienstbezogene Gruppen

In diesem Beispiel wird ein kleines Büro betrachtet, in dem drei Mitarbeiter an ihren PCs arbeiten. Jeder Mitarbeiter hat eine E-Mail-Adresse und darf über den Webproxy im Internet surfen. Außerdem gibt es eine Laufwerksfreigabe (Share), auf dem Daten gespeichert werden.

Um dienstbezogene Benutzungsrichtlinien umzusetzen, müssen zunächst die verschiedenen Dienste identifiziert werden: Zunächst gibt es Basisdienste wie DNS, die jedem Benutzer bereitgestellt werden müssen. Daneben gibt es den Dienst „Webproxy“, den Dienst „E-Mail“ und den Dienst „Laufwerksfreigabe“.

Die Basisdienste können in den vordefinierten Gruppen *Users* oder *LocalNet* geregelt werden. Weitere Basisdienste neben DNS könnten NTP sowie Druck- und Fax-Dienste sein.

Für die anderen Dienste wird jeweils eine Gruppe angelegt und mit den notwendigen Berechtigungen für den Dienst versehen. Es sind also die Gruppen *ProxyUser*, *MailUser* und *ShareUser* notwendig. Alle Einstellungen zum Webproxy werden in der Gruppe *ProxyUser* vorgenommen, sonst nirgends. Die Konfiguration des E-Mail-Systems und der Freigabe erfolgt analog.

Das *LocalNet* wird bei allen drei Gruppen als Mitglied hinzugefügt. Die drei Mitarbeiter werden als Benutzer angelegt und jeweils allen drei Gruppen als Mitglied hinzugefügt.

Stößt ein vierter Mitarbeiter zu der Mannschaft, wird er als Benutzer angelegt und den entsprechenden Gruppen hinzugefügt.

Handelt es sich dabei um einen Praktikanten, der die Firmenweb-

seite neu gestaltet, ist es möglich, ihn nur in die Gruppen *ProxyUser* und *MailUser* aufzunehmen, nicht aber in der Gruppe *ShareUser*.

Der dienstbezogene Aufbau einer Gruppenstruktur ist sinnvoll, wenn sich die Benutzer nicht in unabhängige Gruppen aufteilen lassen, sondern zu großen Teilen die gleichen Rechte erhalten. Bei Hinzunahme eines weiteren Benutzers kann genau festgelegt werden, welche der Dienste er nutzen darf und welche nicht.

4.4.3 Beispiel: Benutzer- und dienstbezogene Gruppen

Nun wird ein großes Unternehmen mit 100 Mitarbeitern betrachtet. Es gibt verschiedene Abteilungen im Unternehmen, u. a. die Bereiche Vertrieb, Entwicklung und Marketing. Jeder Mitarbeiter im Unternehmen erhält seine eigene E-Mail-Adresse und darf über den Webproxy ins Internet zugreifen. Die PCs im Unternehmen sollen über NTP ihre Uhrzeit mit dem V-Cube abgleichen.

Die einzelnen Abteilungen erhalten alle einen eigenen E-Mail-Verteiler und eine eigene Laufwerksfreigabe (Share) zur Datenspeicherung.

In jeder Abteilung gibt es einige wenige Benutzer, die den Fax-Dienst nutzen dürfen. Im Unternehmen wird E-Mail auf Spam und Viren geprüft. Jede Abteilung benennt dazu zwei „Mailadministratoren“, die Zugriff auf die Quarantäne-Verzeichnisse erhalten.

Grundsätzlich ist es möglich, für dieses Unternehmen eine rein benutzerbezogene oder eine rein dienstbezogene Gruppenstruktur zu erstellen. Bei der Analyse, welches Verfahren genutzt werden soll, deuten jedoch einige Aspekte auf das erste und andere Aspekte auf das zweite. Um die Verwaltung einfach und übersichtlich zu halten, wird daher eine gemischte Gruppenstruktur aufgebaut.

Zunächst werden in der vordefinierten Gruppe *Users* (oder alter-

nativ *LocalNet*) für den IP-Bereich des lokalen Netzes die Basisdienste DNS und NTP erlaubt. Für die Nutzung von E-Mail und Webproxy werden analog zum Beispiel der dienstbezogenen Gruppen die Gruppen *MailUser* und *ProxyUser* angelegt. Das Netzwerk im Unternehmen wird als Mitglied in die Gruppen aufgenommen. Die Benutzer werden angelegt und den beiden Gruppen zugeordnet.

Nun werden die E-Mail-Verteiler angelegt. Dabei handelt es sich um die Adressen „vertrieb@“, „entwicklung@“ und „marketing@“ die jeweils an alle Mitarbeiter in der Abteilung verteilt werden.

Zur Datenspeicherung werden die drei Freigaben „VertriebShare“, „EntwicklungShare“ und „MarketingShare“ angelegt.

Um den Zugriff auf diese Shares bzw. die Mitgliedschaft in den Mailverteilern zu regeln, müssten bei dienstbezogener Strategie zweimal drei Gruppen angelegt werden. Da jedoch alle Mitarbeiter einer Abteilung Zugriff auf alle Abteilungsressourcen erhalten, reicht es aus, benutzerbezogene Gruppen zu erstellen: *VertriebGruppe*, *EntwicklungGruppe* und *MarketingGruppe*.

In jeder dieser drei Gruppen wird in den Berechtigungen die Mitgliedschaft im entsprechenden E-Mail-Verteiler sowie der Zugriff auf die Freigabe geregelt. Die Benutzer werden entsprechend ihrer Abteilungszugehörigkeit den Gruppen zugeordnet.

Für die Nutzung des Fax-Dienstes bietet sich eine dienstbezogene *FaxGruppe* an. Da die Fax-Berechtigung nicht über Authentifizierung erfolgt, müssen die Computer der befugten Nutzer als *Hosts* im V-Cube angelegt sein. Diese Hosts werden als Mitglieder der Gruppe zugeordnet. In den Berechtigungen der Gruppe wird der *Fax-Connect* erlaubt.

Zur Administration der Quarantäneverzeichnisse (die per IMAP exportiert werden) wird ebenfalls eine dienstbezogene Gruppe *MailAdminGruppe* angelegt. Hier werden die jeweils festgelegten Benutzer als Mitglieder aufgenommen und die entsprechenden Berechtigungen gesetzt.

Wird ein neuer Mitarbeiter im Unternehmen angestellt, wird sein Benutzeraccount angelegt, und dieser Benutzer wird den Gruppen *MailUser* und *ProxyUser* sowie seiner *AbteilungsGruppe* zugeordnet.

Soll ein weiterer Mitarbeiter Zugriff auf das Fax-System erhalten, muss sein PC als Host erfasst und der Gruppe *FaxUser* zugeordnet werden.

In diesem Beispiel ist der kombinierte Einsatz von dienst- und benutzerbezogenen Gruppen sinnvoll, weil einerseits durch die Abteilungsstruktur klar abgegrenzte Benutzergruppen existieren. Andererseits gibt es Dienste, die über alle Abteilungen hinweg von allen Benutzern (E-Mail) sowie teilweise von ausgewählten Benutzern (Fax) genutzt werden dürfen.

In jedem Fall ist es ratsam, für die Gruppennamen „sprechende“ Namen zu vergeben, die den Zweck und die dahinterliegenden Berechtigungen der Gruppe möglichst genau erklären. In diesem Beispiel ist es ersichtlich, dass alle Berechtigungen zum Webproxy, inkl. eventuell später einzuführender Filterregeln, in der Gruppe *ProxyUser* abgewickelt werden.

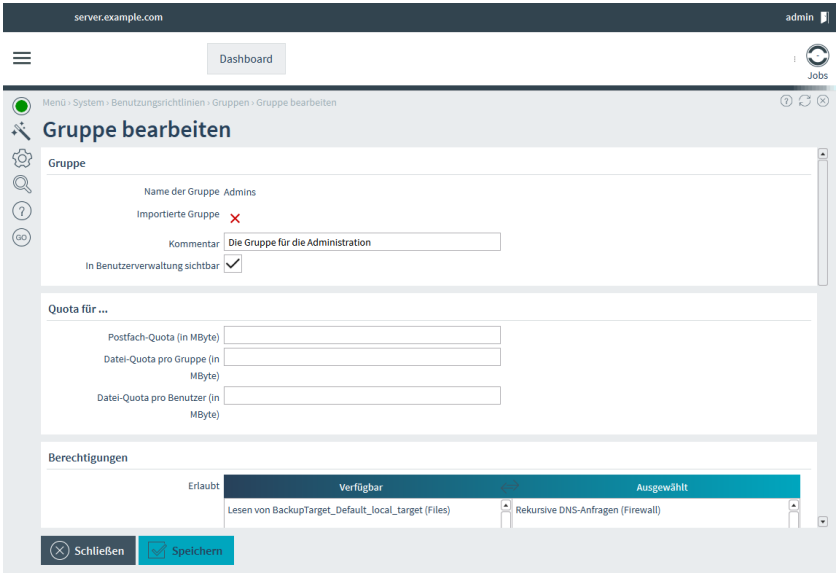
4.5 Schritt für Schritt: Anlegen einer Gruppe

Im folgenden wird exemplarisch eine Gruppe eingerichtet, die die Fernwartung des V-Cubes erlaubt. Obwohl dies eine konkrete Aufgabenstellung ist, ist das Vorgehen allgemeingültig und lässt sich analog für jede andere Gruppe nachvollziehen.

Beispielhaft soll der Web-Admin-Dienst für IP-Adressen aus dem lokalen Netz zugänglich sein. Dort soll sich neben dem *admin* auch ein neu angelegter Benutzer anmelden können, dem die Verwaltung von Zertifikaten, Benutzern und dem Backupsystem erlaubt wird.

Benutzungsrichtlinien

Legen Sie zunächst unter *Benutzungsrichtlinien – Richtlinien – Gruppen* eine neue Gruppe an:

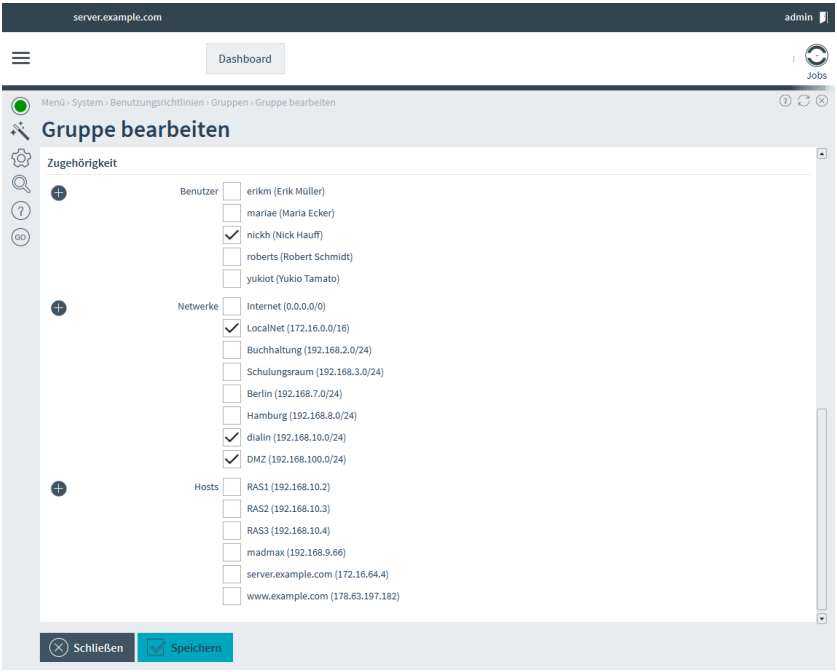


- Tragen Sie bei *Name* und *Kommentar* sinnvolle Texte ein. Der Name der Gruppe kann später nicht mehr geändert werden.
- Da diese Gruppe neu erstellt und nicht von einem Windows-Server o. ä. importiert wird, lassen Sie die Option *importierte Gruppe* deaktiviert. Andernfalls wird der V-Cube versuchen, eine Verbindung zum übergeordneten Server aufbauen und eine Gruppe dieses Namens abzurufen.
- Wenn Sie später Benutzer in die Gruppe aufnehmen möchten, aktivieren Sie die Option *In Benutzerverwaltung sichtbar*. Damit können Sie beim Anlegen eines Benutzers diesen direkt als Mitglied in die Gruppe aufnehmen.
- In den Feldern *Quota* können Sie Beschränkungen des Festplattenspeichers vornehmen. Da diese Gruppe nur dem Konfigura-

tionszugriff auf den V-Cube dient und keine weitere Funktion bieten soll, nehmen Sie hier keine Einstellungen vor.

- Speichern Sie die Gruppe.

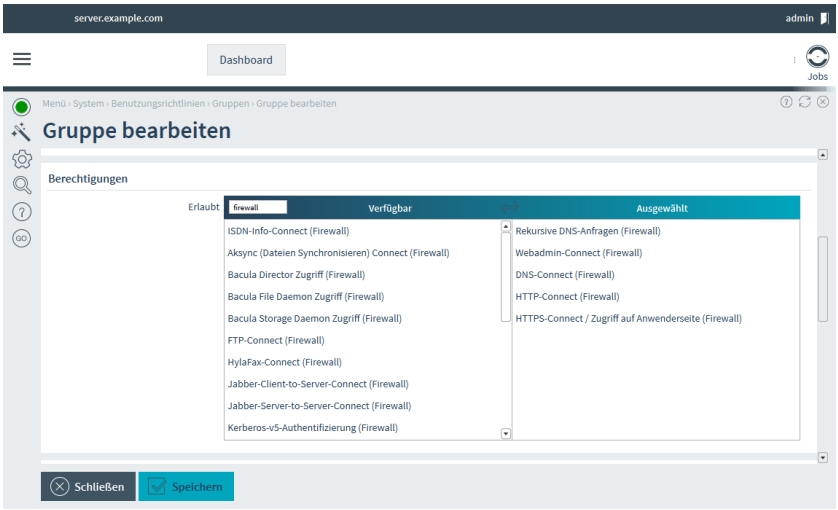
Im nächsten Schritt nehmen Sie das lokale Netz als Mitglied in die Gruppe auf. Dazu markieren Sie die neue Gruppe entweder durch Anklicken (sie wird orange eingefärbt) und wählen rechts oben über den Schalter *Bearbeiten* den Eintrag *Netze* aus, oder Sie öffnen durch einen Klick mit der rechten Maustaste auf die Gruppe das Kontextmenü und wählen dort den Eintrag *Netze*.



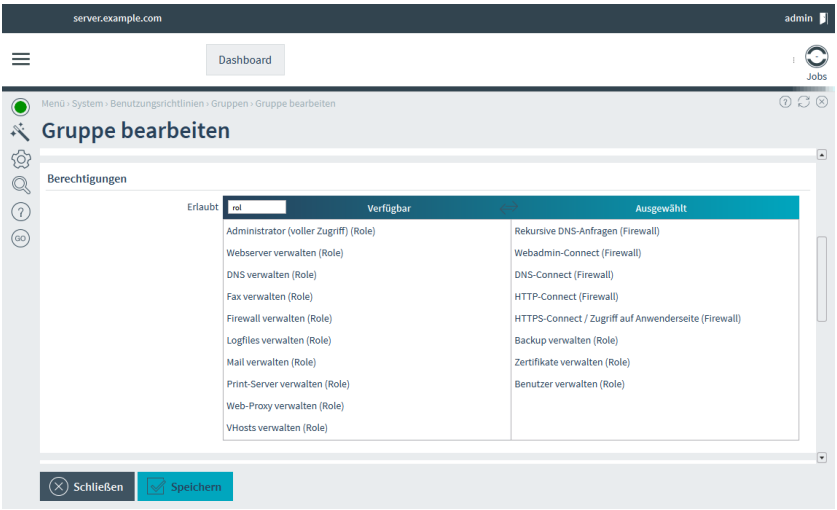
- In dieser Ansicht sind alle angelegten Netze sichtbar. Fügen Sie durch das Aktivieren von *LocalNet* das Netz der Gruppe als Mitglied hinzu.

- Um einzelne Rechner als Mitglied in eine Gruppe aufzunehmen, müssen Sie sie zunächst als *Host* bekannt machen. Danach können Sie sie unter *Rechner* der Gruppe hinzufügen. Dies ist sinnvoll, wenn der Zugriff nur von einem Admin-PC oder von einem einzigen Server im Internet ermöglicht werden soll. In diesem Fall muss das *LocalNet* jedoch aus der Gruppe herausgenommen werden, da andernfalls doch das gesamte lokale Netz zugreifen kann.
- Um einen Dienst für das gesamte Internet zugänglich zu machen (etwa SMTP, um E-Mail direkt anzunehmen, oder SSH zur Fernwartung von überall), müssen Sie keine neue Gruppe anlegen. Verwenden Sie dazu die vorhandene Gruppe *Internet* und setzen Sie die erforderlichen Berechtigungen.

Nun wird festgelegt, welche Rechte die Mitglieder der Gruppe erhalten. Dazu rufen Sie die Konfigurationsseite *Berechtigungen* der Gruppe auf.



- Hier sind mehrere Kategorien aufgeführt, die jeweils bestimmte Berechtigungen enthalten. Durch das Anklicken einer Kategorie öffnen Sie die zugehörigen Berechtigungen.
- Klicken Sie auf *Firewall*. Dadurch werden die internen Dienste des V-Cubes aufgelistet.
- In der Liste befindet sich der Dienst *Webadmin*. Aktivieren Sie diesen für die Gruppe, indem Sie ihn anklicken. Hinter *Webadmin* verbirgt sich die HTTPS-Konfigurationsoberfläche auf Port 8001.

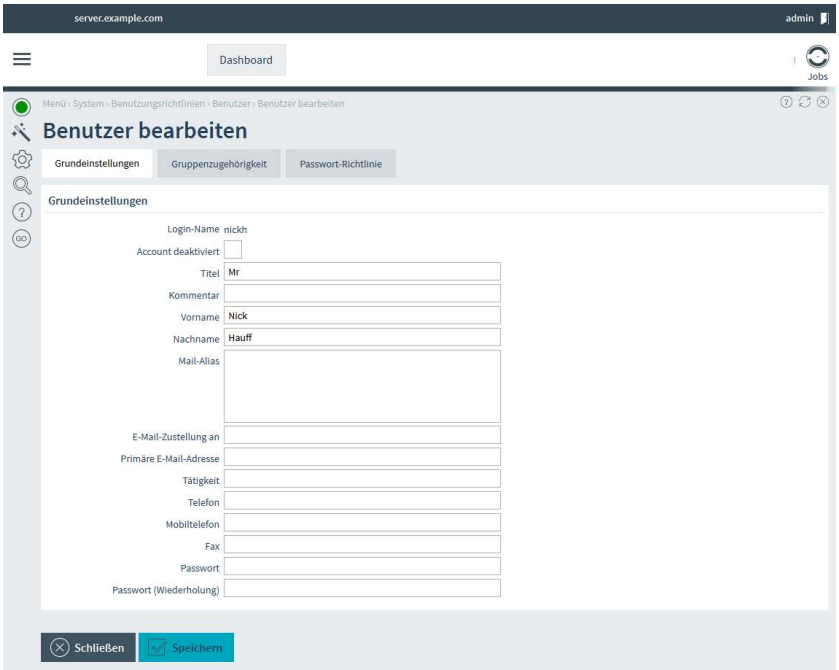


- Öffnen Sie *Role*, indem Sie sie anklicken. Die einzelnen Administrationsbereiche des V-Cubes werden nun aufgelistet.
- Aktivieren Sie gemäß der Aufgabenstellung die Rechte zur Verwaltung von *Backup*, *Zertifikaten* und *Benutzern*.

Mit den bisher unternommenen Schritten ist es nach Aktivierung der Konfiguration möglich, aus dem lokalen Netz heraus eine Verbindung auf die Administrationsoberfläche aufzubauen. Anmelden kann sich hier bisher nur der Systembenutzer *admin*, der alle Bereiche in der Oberfläche bearbeiten darf.

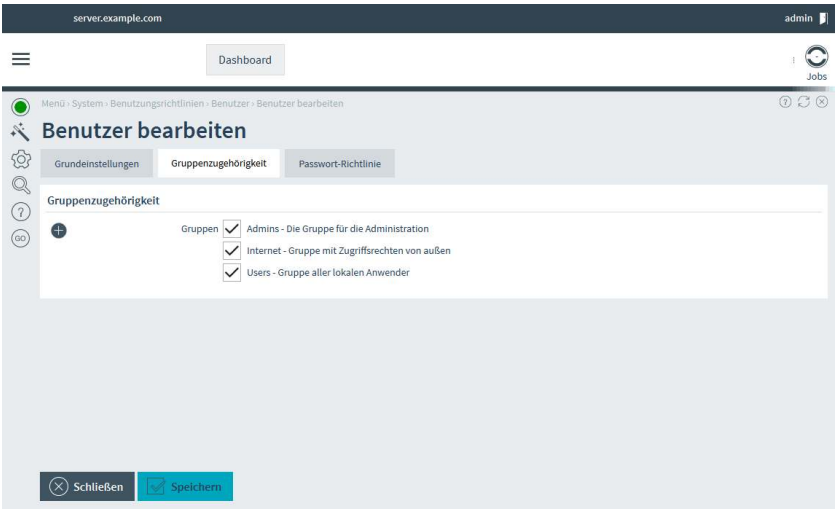
Sie müssen daher noch einen neuen Benutzer anlegen, der als Mitglied in die Gruppe aufgenommen wird. Es ist die Mitgliedschaft eines Netzes oder eines konkreten Rechners notwendig, um die IP-Verbindung zu einem Dienst im V-Cube aufbauen zu können. Zusätzlich muss ein Benutzer Mitglied werden, um sich an dem Dienst anmelden zu können.

Einen neuen Benutzer fügen Sie unter *Benutzungsrichtlinien – Richtlinien – Benutzer – Benutzer anlegen* hinzu.



- In diesem Dialog legen Sie zunächst das *Login* des Benutzers fest. Dieses Login muss innerhalb des Systems eindeutig sein. Es kann keiner der bereits angelegten Systembenutzer verwendet werden, auch wenn diese hier nicht sichtbar sind (z. B. „admin“).

- In den folgenden Feldern geben Sie den Namen des Benutzers, eventuelle Mail-Alias-Adressen und Telefonnummern an. Teilweise haben diese Einstellungen noch zusätzlich in weiteren Diensten des V-Cubes eine Funktion. Beispielsweise wird über die Faxnummer die interne Zustellung eingehender Fax-Mitteilungen vorgenommen.
- Das *Passwort* müssen Sie zweimal eingeben, da es aus Sicherheitsgründen nicht sichtbar ist.



- Unter dem Reiter *Gruppenzugehörigkeit* können Sie die Gruppen aktivieren, zu denen der Benutzer gehören soll.
- Wählen Sie die neu angelegte *WartungsGruppe* aus.
- Nach dem Speichern der Einstellungen und Aktivieren der gesamten Konfiguration kann sich der neu angelegte Benutzer aus dem lokalen Netz auf der Administrationsoberfläche anmelden und hat Zugriff auf die dort für ihn freigeschalteten Bereiche.

4.6 GUI-Referenz: Richtlinien

4.6.1 *Gruppen*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Richtlinien – Gruppen*)

Über die Gruppen wird der Zugriff auf alle Dienste im V-Cube geregelt. In diesem Dialog werden Gruppen angelegt und deren Rechte verwaltet. Eine Gruppe kann dabei aus Benutzern, Rechnern und Netzwerken bestehen.

Dieser Dialog besteht aus mehreren untergeordneten Dialogen.

4.6.1.1 *Gruppe wählen*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Richtlinien – Gruppen*)

In dieser Liste werden die bestehenden Gruppen angezeigt.

Felder in diesem Dialog

- *Name*: Der Name der Gruppe.
- *Kommentar*: Ein Kommentartext zur Gruppe.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion wird die Konfiguration der ausgewählten Gruppe bearbeitet.
- *Berechtigungen*: Mit dieser Aktion werden die Berechtigungen der Gruppe bearbeitet.

- *Benutzer*: Mit dieser Aktion werden alle Benutzer und ihre Mitgliedschaft in der Gruppe angezeigt. Der Mitgliedschaftsstatus kann geändert werden.

  In eine importierte Netzwerkgruppe können keine Benutzer aufgenommen werden. Diese Aktion wird daher nur für lokal angelegte Gruppen angezeigt.
- *Rechner*: Mit dieser Aktion werden alle Rechner und ihr Mitgliedstatus in der Gruppe angezeigt. Der Mitgliedschaftsstatus kann geändert werden.
- *Netze*: Mit dieser Aktion werden alle Netzwerke und ihr Mitgliedstatus in der Gruppe angezeigt. Der Mitgliedschaftsstatus kann geändert werden.
- *Löschen*: Diese Aktion löscht die ausgewählte Gruppe.

Aktionen für diesen Dialog

- *Gruppe anlegen*: Mit dieser Aktion wird eine neue Gruppe angelegt.

4.6.1.2 *Gruppe bearbeiten*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Richtlinien – Gruppen*)

In diesem Dialog wird eine zuvor ausgewählte Gruppe bearbeitet.

Abschnitt *Gruppe*
Felder in diesem Abschnitt

- *Name der Gruppe*: Der Name der Gruppe, er kann nicht nachträglich geändert werden.

- *Importierte Gruppe*: Mit dieser Option wird angegeben, dass die Gruppe auf einem anderen System verwaltet wird. Dies kann beim Anlegen einer Gruppe festgelegt, jedoch später nicht mehr geändert werden.
- *Name der Gruppe*: Hier wird der Name der Gruppe angegeben. Der Name darf nicht mit einer Ziffer beginnen und darf auch keine Leerzeichen enthalten.
- *Importierte Gruppe*: Mit dieser Option wird angegeben, dass die Gruppe auf einem anderen System verwaltet wird, z. B. auf einem Windows-Server. Dies kann beim Anlegen einer Gruppe festgelegt, jedoch später nicht mehr geändert werden.
- *Kommentar*: In diesem Feld kann ein Kommentartext zu dieser Gruppe erstellt werden.
- *In Benutzerverwaltung sichtbar*: Wenn diese Option aktiviert ist, wird die Gruppe in der Benutzerverwaltung angezeigt. Dort kann ein neu angelegter Benutzer direkt in diese Gruppe aufgenommen werden.

Abschnitt *Windows-Gruppen Zuordnung*

Dieser Abschnitt wird eingeblendet, wenn der Collax Server mit dem Authentifizierungs-Modus PDC aktiviert ist.

Felder in diesem Abschnitt

- *Vordefinierte Windows-Gruppe*: Hier kann die Microsoft Windows-Gruppe angegeben werden, deren Rechte auf die Systemgruppe vererbt werden soll.

4.6.1.3 *Berechtigungen*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Richtlinien – Gruppen*)

Abschnitt *Gruppe*
Felder in diesem Abschnitt

- *Name der Gruppe*: Nach dem Anlegen einer Gruppe kann deren Name nicht mehr geändert werden.

Abschnitt *Berechtigungen*

Hier werden die Berechtigungen der Gruppenmitglieder für die verschiedenen Dienste konfiguriert.

Die Berechtigungen sind additiv, d. h., wenn ein Gruppenmitglied zu mehreren Gruppen gehört, in denen dieselbe Berechtigung in einigen aktiviert und in anderen deaktiviert ist, ist die Berechtigung für dieses Mitglied aktiviert. Es reicht aus, wenn eine Berechtigung für das Mitglied in einer einzigen Gruppe aktiviert ist.

Felder in diesem Abschnitt

- *Berechtigungen*: In dieser Liste werden alle Berechtigungen angezeigt.

4.6.1.4 *Benutzer*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Richtlinien – Gruppen*)

In diesem Dialog sind alle angelegten Benutzer sichtbar. Benutzer, die zu der bearbeiteten Gruppe gehören, sind markiert.

In diesem Dialog werden die Mitglieder der Gruppe ausgewählt.

Felder in diesem Dialog

- *Name der Gruppe*: In diesem Feld wird der Name der Gruppe angezeigt.

4.6.1.5 *Rechner*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Richtlinien – Gruppen*)

In diesem Dialog sind alle angelegten Rechner sichtbar. Rechner, die zu der bearbeiteten Gruppe gehören, sind markiert.

In diesem Dialog werden die Rechner ausgewählt, die zu der Gruppe gehören sollen.

Felder in diesem Dialog

- *Name der Gruppe*: Hier wird der Name der Gruppe angezeigt.

4.6.1.6 *Netzwerke*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Richtlinien – Gruppen*)

In diesem Dialog sind alle angelegten Netzwerke sichtbar. Netze, die zu der bearbeiteten Gruppe gehören, sind markiert.

Felder in diesem Dialog

- *Name der Gruppe*: Hier wird der Name der Gruppe angezeigt.

4.6.2 *Importierbare Gruppen*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Richtlinien – Importierbare Gruppen*)

In diesem Dialog werden Gruppen angezeigt, die in der Benutzerverwaltung eines Active Directory benutzt werden. Damit Gruppen aus der Active Directory-Verwaltung angezeigt werden können, muss das System einem Active Directory als Mitglied beigetreten sein und die Funktion *Active Directory-Proxy* auf dem System aktiviert sein. Die aufgelisteten Gruppen können dann in die lokalen Benutzungsrichtlinien eingebunden werden, sobald diese über die Aktion *Zu lokalen Gruppen hinzufügen* in die Verwaltung aufgenommen wurden. Die Benutzer der AD-Gruppen werden weiterhin über das Active Directory verwaltet und sind nicht Bestandteil des lokalen Systems.

4.6.2.1 *Liste der importierbaren Gruppen*

Die Liste zeigt Gruppen an, die Benutzer beinhalten. Der Benutzer Administrator wird nicht als Benutzer gelistet. Enthält eine Gruppe nur den Benutzer Administrator wird dieses Gruppe ebenfalls nicht gelistet.

Abschnitt *Hinweis*
Felder in diesem Abschnitt

- : Wenn der Active Directory-Proxy noch nicht aktiviert wurde, erscheint hier der entsprechende Hinweis.

Spalten in der Tabelle

- *Name*: Zeigt den Namen der Gruppe im Active Directory.
- *Kommentar*: Zeigt weitere Informationen über die Gruppe an.

Aktionen für jeden Tabelleneintrag

- *Benutzer dieser Gruppe*: Über diese Aktion können die Benutzer der AD-Gruppe aufgelistet werden.
- *Zu lokalen Gruppen hinzufügen*: Mit dieser Aktion können AD-Gruppen der lokalen Richtlinienverwaltung zur Verfügung gestellt werden. Diese Gruppen tauchen nachfolgend im Menü *Gruppen* auf.
- *WARNUNG! Diese Gruppe existiert bereits ist aber nicht als Importierte Gruppe markiert. Aus lokalen Gruppen entfernen.*: Falls schon eine lokale Gruppe besteht, deren Name identisch zu einer Gruppe aus dem Active Directory ist, wird gewarnt. Um Konflikte zu vermeiden, empfiehlt es sich diese Gruppe nicht in die Richtlinienverwaltung zu übernehmen.
- *Aus lokalen Gruppen entfernen*: Wurde eine AD-Gruppe der lokalen Richtlinienverwaltung zur Verfügung gestellt und ab sofort nicht mehr benötigt, kann diese mit dieser Aktion entfernt werden.

4.6.2.2 *Mitglieder der entfernten Gruppe*

In diesem Dialog werden alle Benutzer einer entfernten Gruppe angezeigt.

Felder in diesem Formular

- *Name der Gruppe*: Zeigt den Namen der gewählten AD-Gruppe.

Aktionen für dieses Formular

- *Zurück*: Führt zurück in die Übersicht der importierbaren Gruppen.

4.6.3 *Berechtigungen*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Richtlinien – Berechtigungen*)

In diesem Dialog werden die Berechtigungen des Systems verwaltet.

4.6.3.1 *Berechtigungen*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Richtlinien – Berechtigungen*)

Hier werden alle im System definierten Berechtigungen aufgelistet. Statische und dynamische Berechtigungen können bearbeitet und den verschiedenen Gruppen zugewiesen werden. Prinzipiell werden statische oder dynamische Berechtigungen immer durch das System

vordefiniert. Maßgeschneiderte Rollenberechtigungen können unter Administrative Rollen (S. 65) hinzugefügt oder verändert werden.

Felder in diesem Formular

- *Service*: Hier wird die Bezeichnung des Service angezeigt.
- *ID*: Hier wird die ID der Berechtigung angezeigt.
- *Kommentar*: Hier wird ein zusätzlicher Kommentar zur Berechtigung angezeigt.
- *Typ*: Hier wird der Typ der Berechtigung angezeigt. Statische und dynamische Berechtigungen werden vom System vorgegeben, der Typ „custom“ bezeichnet die individuell definierten Berechtigungen für administrative Rollen.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion wird die Konfiguration der ausgewählten Berechtigung bearbeitet.

4.6.3.2 *Berechtigung*

In diesem Formular werden Systemberechtigungen angezeigt. Nur die Gruppenzuweisung kann verändert werden, die Berechtigung selbst kann nicht geändert werden.

Abschnitt*Grundeinstellungen*
Felder in diesem Abschnitt

- *Service*: Hier wird der Service der Berechtigung angezeigt.
- *ID*: Hier wird die interne ID der Berechtigung angezeigt.
- *Beschreibung*: Hier ist eine kurze Beschreibung eingetragen.

Abschnitt *Gruppenzugehörigkeit*
Felder in diesem Abschnitt

- *Berechtigung für Gruppen*: Hier wird eingestellt, für welche Gruppe die Berechtigung gelten soll.

Aktionen für dieses Formular

- *Abbrechen*: Bearbeiten der Berechtigung beenden. Die Änderungen werden verworfen.
- *Speichern*: Bearbeiten der Berechtigung beenden. Die Änderungen werden übernommen.

4.6.4 *Benutzer*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Richtlinien – Benutzer*)

In diesem Dialog werden die Benutzer des Systems verwaltet.

4.6.4.1 *Benutzer auswählen*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Richtlinien – Benutzer*)

Hier werden alle auf dem System angelegten Benutzer angezeigt. Neue Benutzer können hier angelegt, bestehende Benutzer können hier bearbeitet oder gelöscht werden.

Spalten in der Tabelle

- *Login*: Der Login-Name des Benutzers. Dieser wird zur Authentifizierung bei allen Diensten genutzt (beispielsweise am Mailserver). Für den Login-Namen sollten nur Kleinbuchstaben verwendet werden.
- *Vorname*: Der Vorname des Benutzers.
- *Nachname*: Der Nachname des Benutzers.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion wird das Benutzerkonto bearbeitet.
- *Löschen*: Mit dieser Aktion wird Benutzerkonto gelöscht.

Aktionen für diesen Dialog

- *Benutzer anlegen*: Mit dieser Aktion wird ein neues Benutzerkonto erstellt.
- *Benutzer importieren*: Mit dieser Aktion kann eine Liste von Benutzern aus einer Datei im CSV-Format importiert werden.
- *Benutzer exportieren*: Mit dieser Aktion werden alle im System angelegten Benutzerkonten exportiert. Die Datei ist im CSV-Format aufgebaut. Dabei wird pro Benutzerkonto eine Zeile erzeugt. Die einzelnen Werte sind durch Komma getrennt. Die erste Zeile des Exports ist eine Musterzeile mit einer genauen Aufschlüsselung der einzelnen Felder.

4.6.4.2 *Benutzer bearbeiten*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Richtlinien – Benutzer*)

In diesem Dialog können die Einstellungen des Benutzerkontos bearbeitet werden.

Tab *Grundeinstellungen*, Abschnitt *Grundeinstellungen* Felder in diesem Abschnitt

- *Login-Name*: Der Login-Name des Benutzers wird zur Authentifizierung bei den verschiedenen Diensten des V-Cubes eingesetzt.

  Der Login-Name sollte in Kleinbuchstaben angegeben werden. Erlaubt sind nur die Buchstaben „a“ bis „z“ (keine Umlaute o. ä.), Ziffern, der Unterstrich „_“ sowie (nicht empfohlen) die Großbuchstaben „A“ bis „Z“. Der Login-Name darf nicht mit einer Ziffer beginnen.

  Das Eingabefeld erscheint nur, wenn ein neues Benutzerkonto angelegt wird.
- *Login-Name*: Hier wird der Login-Name des Benutzerkontos angezeigt. Wenn ein Benutzerkonto bearbeitet wird, kann der Name nicht geändert werden.
- *Account deaktiviert*: Mit dieser Option kann ein Benutzerkonto zeitweilig deaktiviert werden. Dem Benutzer werden dann alle Berechtigungen entzogen. Soll ein Benutzerkonto wieder Berechtigungen erhalten und im System verfügbar sein, kann das Benutzerkonto einfach wieder aktiviert werden.
- *Titel*: In diesem Feld kann der persönliche Titel des Benutzers (Dr., Dipl.-Ing. usw.) eingetragen werden. Diese Angabe erscheint dann im LDAP-Verzeichnis.
- *Vorname*: Der Vorname des Benutzers.
- *Nachname*: Der Nachname des Benutzers.

Abhängig von den SMTP-Einstellungen wird aus Vorname und Nachname des Benutzers die E-Mail-Adressierung erzeugt. Dabei werden nicht zulässige Zeichen automatisch konvertiert: Ein Leerzeichen wird zu einem Punkt, „ß“ wird zu „ss“. Umlaute werden in die Schreibweise mit folgenden „e“, z. B. „ä“ zu „ae“, und Zeichen mit Akzent werden zu Zeichen ohne Akzent umgewandelt.

- *Mail-Alias*: In diesem Eingabefeld können zusätzliche E-Mail-Adressen für den Benutzer angegeben werden, die als E-Mail-Alias angelegt werden. Wird dabei die Maildomain nicht angegeben, erhält der Benutzer den Alias in jeder der lokal verwalteten Maildomains, zu der er über die Gruppenberechtigung gehört. Wird die Adresse mit Maildomain angegeben, gilt der Alias nur in der angegebenen Domain.

  Pro Zeile wird eine Adresse eingegeben, ein Trennzeichen ist nicht erforderlich.

  Hinweis: Wird eine Adresse in einer Domain angegeben, die nicht zu einer der lokal verwalteten Maildomains des Systems gehört, erscheint die Adresse zwar im LDAP-Verzeichnis, E-Mails an diese Adresse werden jedoch nicht zugestellt.
- *E-Mail-Zustellung an*: In diesem Feld kann die E-Mail-Adresse eines lokalen Benutzers, eines Verteilers, ein Alias eines Benutzers oder eine externe E-Mail-Adresse angegeben werden. An die eingetragene Adresse werden alle E-Mails dieses Benutzers umgeleitet. Die E-Mails werden nicht im lokalen Postfach des Benutzers gespeichert. Normalerweise kann dieses Feld leerbleiben.
- *Primäre E-Mail-Adresse*: Wenn E-Mail-Clients verwendet werden, die eine Einstellung der Absenderadresse des Benutzers nicht zulassen, ist es sinnvoll diese Option auf Server-Seite zu setzen. Betreffende E-Mail-Clients können Web-Mailer und Clients, die sich mit einem MAPI-Server verbinden, sein. In das Feld soll eine

gültige lokale E-Mail-Adresse eingetragen werden. Diese Adresse wird als Absender in den versendeten E-Mails des Benutzers erscheinen.

Diese Option überschreibt den eingestellten Adressaufbau der Primär-Adresse im Formular *SMTP-Empfang*.

- *Tätigkeit*: Hier kann eine Beschreibung der Tätigkeit des Benutzers für das LDAP-Verzeichnis angegeben werden.
- *Telefon*: Hier können eine oder mehrere Telefonnummern für das LDAP-Verzeichnis angegeben werden. Mehrere Nummern müssen durch Komma getrennt eingetragen werden.
- *Mobiltelefon*: Hier können eine oder mehrere Mobilfunknummern für das LDAP-Verzeichnis angegeben werden. Mehrere Nummern müssen durch Komma getrennt eingetragen werden.
- *Fax*: Hier können eine oder mehrere Nummern von Faxanschlüssen für das LDAP-Verzeichnis angegeben werden. Mehrere Nummern müssen durch Komma getrennt eingetragen werden.

  Wird auf diesem System der Fax-Dienst genutzt und gehen Faxe auf einer der hier angegebenen Nummern ein, wird diesem Benutzer das Fax zugestellt.
- *Passwort*: Das Passwort des Benutzers.

  Hinweis: Bei einigen Sonderzeichen im Passwort kann es vorkommen, dass das Webmailinterface dieses nicht akzeptiert. Dann erhält der Benutzer beim Aufrufen des Webmailers eine Fehlermeldung, obwohl er sich zuvor an der Web-Access-Seite anmelden konnte.
- *Passwort (Wiederholung)*: Da das Passwort aus Sicherheitsgründen bei der Eingabe nicht angezeigt wird, muss es hier zur Kontrolle ein zweites Mal eingegeben werden.
- *Passwort-Richtlinie*: Dem Benutzer kann eine Passwort-Richtlinie zugewiessen werden, welcher er unterliegt. Wird das Feld leergelassen, oder auf Standard / Default gesetzt unterliegt der Benutzer der Standardrichtlinie.

Tab *Gruppenzugehörigkeit*, Abschnitt *Gruppenzugehörigkeit* Felder in diesem Abschnitt

- *Gruppen*: Hier kann konfiguriert werden, zu welchen Gruppen der Benutzer gehört. Es sind nur die Gruppen aufgeführt, die „in der Benutzerverwaltung sichtbar“ sind.

4.6.4.3 *Benutzer importieren*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Richtlinien – Benutzer*)

Felder in diesem Dialog

- *Benutzer importieren*: Mit diesem Dialog kann eine bestehende Liste von Benutzerkonten importiert werden. Diese müssen in einer Datei im CSV-Format gespeichert sein. Dabei wird pro Zeile ein Benutzerkonto angegeben, die einzelnen Werte sind in einer festgelegten Reihenfolge durch Kommas getrennt abgelegt.
- *CSV-Datei*: Hier wird die Datei mit den Benutzerkonten ausgewählt.
- *Ergebnis*: Nach dem Import wird hier das Ergebnis angezeigt.

Aktionen für diesen Dialog

- *Importieren*: Import der Benutzerliste starten.

4.6.5 *Administrative Rollen*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Umgebung – Administrative Rollen*)

In diesem Dialog werden die administrativen Rollen von Benutzern verwaltet.

4.6.5.1 *Administrative Rollen*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Umgebung – Administrative Rollen*)

In diesem Formular werden administrative Rollen für Benutzer angezeigt oder individuell definiert. Administrative Rollen sind Zugriffsberechtigungen von ausgewählten Benutzern auf entsprechende Formulare der Collax-Administrationsoberfläche. Sie können flexibel definiert werden, Zugriff auf nur ein einzelnes oder auf mehrere Formulare zu gewähren ist möglich.

Felder in diesem Formular

- *Name*: Hier wird der Name der Admin-Rolle angezeigt. Dieser wird frei definiert und erscheint auch im Formular der Gruppenberechtigungen zur Auswahl.
- *Kommentar*: Hier wird ein zusätzlicher Kommentar zur administrativen Rolle angezeigt.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion wird die gewählte Rolle bearbeitet.
- *Löschen*: Mit dieser Aktion wird die gewählte Rolle gelöscht. Sie

steht nachfolgend nicht mehr in den Gruppenberechtigungen zur Verfügung.

Aktionen für dieses Formular

- *Hinzufügen*: Mit dieser Aktion kann eine neue administrative Rolle für eine Benutzergruppe definiert werden.

4.6.5.2 *Berechtigung*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Umgebung – Administrative Rollen*)

Tab*Grundeinstellungen*, Abschnitt*Berechtigung*
Felder in diesem Abschnitt

- *Bezeichnung*: In dieses Feld wird die Namensbezeichnung der neuen Berechtigung eingegeben.
- *Beschreibung*: Hier wird eine spezifizierte Beschreibung der neuen Berechtigung eingegeben.

Tab*Formulare Zugewiesene Formulare*
Felder in diesem Abschnitt

- *Zugewiesene Formulare*: Hier werden die Formulare ausgewählt, die verwaltet werden dürfen.

Tab*Gruppen Zugewiesene Gruppen*
Felder in diesem Abschnitt

- *Zugewiesene Gruppen*: Hier werden die gewünschten Gruppen für die Berechtigung ausgewählt. Die Mitglieder der hier ausgewählten Gruppen dürfen die Funktionen der gewählten Formulare vollständig verwalten.

Aktionen für dieses Formular

- *Abbrechen*: Mit dieser Aktion wird die Bearbeitung beendet. Die Einstellungen werden nicht übernommen.
- *Speichern*: Mit dieser Aktion wird die Bearbeitung beendet. Die vorgenommenen Einstellungen werden übernommen.

4.6.6 *Zeiträume*

In diesem Dialog werden Zeiträume verwaltet. Auf diese Zeiträume wird in anderen Dialogen zurückgegriffen, etwa bei der Konfiguration von Filtern oder Mailabholaufträgen.

Vordefiniert ist der Zeitraum *always*, der rund um die Uhr gilt, also „24/7/365“. Weitere Zeiträume, etwa für die Arbeitszeiten, können angelegt werden.

4.6.6.1 *Zeitraum wählen*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Richtlinien – Zeiträume*)

In dieser Liste werden die definierten Zeiträume angezeigt.

Felder in diesem Dialog

- *Name*: Hier wird der Name des Zeitraumes angezeigt.
- *Kommentar*: Hier wird der Kommentartext zu dem Zeitraum angezeigt.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion kann der Zeitraum bearbeitet werden.
- *Löschen*: Diese Aktion löscht den gesamten Zeitraum.

Aktionen für diesen Dialog

- *Neuer Zeitraum*: Mit dieser Aktion wird ein neuer Zeitraum festgelegt.

4.6.6.2 *Zeitraum bearbeiten*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Richtlinien – Zeiträume*)

In diesem Dialog wird der Zeitraum bearbeitet. Ein Zeitraum besteht aus einem oder mehreren Zeitabschnitten, die wiederum aus einer Angabe für den Beginn und das Ende sowie einer Liste von Wochentagen bestehen.

Abschnitt *Name*

Hier wird der Name des Zeitraums festgelegt.

Felder in diesem Abschnitt

- *Bezeichnung*: Hier kann der Name des Zeitraums geändert werden.
- *Kommentar*: Hier kann ein kurzer Kommentartext zum Zeitraum angegeben werden.

Abschnitt *Zeitabschnitt*

Jeder Zeitraum kann mehrere Zeitabschnitte umfassen. Für jeden dieser Zeitabschnitte wird dieser Teildialog angezeigt.

Aktionen für diesen Dialog

- *Zeitabschnitt hinzufügen*: Mit dieser Aktion wird ein weiterer Zeitabschnitt zum Zeitraum hinzugefügt.

Spalten in der Tabelle

- *von*: Hier wird der Beginn des Zeitabschnitts angegeben.
- *bis*: Hier wird das Ende des Zeitabschnitts angegeben. Falls das Ende zeitlich vor dem Beginn liegt, wird dies als „endet am nächsten Tag um diese Zeit“ angenommen.
- *Wochentage*: Hier werden alle Wochentage aktiviert, an denen der Zeitabschnitt gelten soll. Die Tage beziehen sich jeweils auf die Anfangszeit (die Endzeit kann auf den Folgetag fallen).

Aktionen für jeden Tabelleneintrag

- *Löschen*: Hiermit wird der markierte Zeitabschnitt gelöscht.

4.7 GUI-Referenz: Umgebung

In diesem Abschnitt werden globale Einstellungen für den Administrator und den Standort des V-Cubes vorgenommen.

4.7.1 *Administrator*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Umgebung – Administrator*)

In diesem Dialog kann das Administrator-Passwort für die Oberfläche geändert und die E-Mail-Adresse für E-Mails des Systems selbst eingetragen werden.

4.7.1.1 Abschnitt *Angaben*

Felder in diesem Abschnitt

- *Passwort*: Hier kann ein neues Passwort für den Administrator gesetzt werden. Das Passwort wird nur geändert, wenn in diesem Feld ein neues Passwort eingegeben wird, das dann mit der Eingabe im Kontrollfeld übereinstimmt.
- *Passwort (Wiederholung)*: Da aus Sicherheitsgründen das Passwort während der Eingabe nicht angezeigt wird, muss es hier zur Kontrolle noch einmal eingegeben werden.
- *E-Mail-Adresse*: Hier wird die E-Mail-Adresse des Systemverantwortlichen angegeben. An diese Adresse werden Fehlermeldungen des Systems und ähnliches geschickt.

  Die Adresse kann entweder eine externe E-Mail-Adresse, das Login eines lokalen Benutzers oder die Adresse eines lokalen

Postfachs mit Angabe des kompletten Systemnamens als Domain (in der Form Login@FQDN) sein. Adressen aus einer der lokal verwalteten Maildomains und Adressen von Verteilern können hier nicht verwendet werden.

Wird hier nichts eingetragen, werden Meldungen des Systems verworfen.

4.7.1.2 Abschnitt *SSH*

Felder in diesem Abschnitt

- *Secure Shell aktivieren*: Mit dieser Option wird der SSH-Dienst auf dem System aktiviert. Welche Rechner und Netze eine SSH-Verbindung aufbauen dürfen, kann innerhalb der Gruppen in den Benutzungsrichtlinien konfiguriert werden.

4.7.1.3 Abschnitt *Administrations-Web-Server*

Felder in diesem Abschnitt

- *Serverzertifikat*: Für den verschlüsselten Zugriff auf die Web-Administration kann hier ein eigenes Zertifikat gewählt werden. Üblicherweise braucht kein Zertifikat gewählt werden, denn das System erzeugt dann ein auf den Server-Host-Namen abgestimmtes Zertifikat selbst. Das hat zur Folge, dass bei Änderung des Host-Namens ein neues Zertifikat mit geändertem Common Name erzeugt wird. Ist ein Zertifikat aus der Liste gewählt, wird dieses auch bei Änderung des FQDN weiter benutzt.

4.7.1.4 Abschnitt *Sitzungsverwaltung*

Felder in diesem Abschnitt

- *Automatische Abmeldung*: Aus Sicherheitsgründen werden Administrationssitzungen nach einer bestimmten Leerlaufzeit unterbrochen. Mit diesem Feld wird eingestellt, wie lange diese Leerlaufzeit dauern darf.

4.7.2 *Standort*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Umgebung – Standort*)

In diesem Dialog werden verschiedene Angaben zum Standort des Systems und des Unternehmens eingegeben.

Die Angaben hier dienen als Vorgabewerte für andere Stellen im System.

4.7.2.1 Abschnitt *Firma/Organisation*

Die Felder in diesem Abschnitt werden im LDAP-Verzeichnis eingetragen. Außerdem werden sie als Vorgabe beim Erstellen von Zertifikaten verwendet. Die meisten Felder sind optional, jedoch sollten mindestens der Name der Organisation sowie das Land angegeben werden.

Felder in diesem Abschnitt

- *Firma/Organisation*: Hier wird der Name des Unternehmens oder der Einrichtung angegeben.

- *Abteilung/Sektion*: Hier kann eine Abteilung oder Sektion angegeben werden.
- *Straße*: Hier wird die Straße des Unternehmens angegeben.
- *Postleitzahl*: Hier wird die Postleitzahl des Unternehmens angegeben.
- *Ort*: Hier wird der Ort des Unternehmens angegeben.
- *Bundesland/Region*: Hier wird das Bundesland oder die Provinz des Unternehmens angegeben.
- *Land*: Hier wird das Land des Unternehmens ausgewählt.

4.7.2.2 Abschnitt *Telefonie*

Die Angaben in diesem Abschnitt dienen dazu, Telefonnummern in eine einheitliche Form umzusetzen und später aus dieser Form die zu wählende Rufnummer zu ermitteln.

Felder in diesem Abschnitt

- *Landesvorwahl*: Hier wird die Landesvorwahl der eigenen Telefonnummer angegeben. Führende Nullen entfallen dabei. Für Deutschland ist dies z. B. „49“, für die Schweiz „41“ und für Österreich „43“.
- *Ortsnetz*: Hier wird die Ortskennzahl der eigenen Telefonnummer angegeben, ebenfalls ohne vorangestellte Null.
- *Anlagenrufnummer*: Hier wird die Rufnummer der Telefonanlage angegeben. Wird keine Telefonanlage verwendet und ist das System direkt an das öffentliche Telefonnetz angeschlossen, bleibt dieses Feld leer.
- *Amtsholung*: Ist das System an einer Nebenstellenanlage angeschlossen und bekommt beim Abnehmen nicht automatisch eine

Amtsleitung, muss hier die Kennzahl angegeben werden, mit der eine Amtleitung geschaltet wird. Dies ist meist eine Null.
- *Vorwahl für Fernverbindungen*: Hier wird die Vorwahl für nationale Verbindungen in andere Ortsnetze angegeben. Dies ist meist eine Null.
- *Vorwahl für internationale Verbindungen*: Hier wird die Vorwahl für internationale Fernverbindungen angegeben. Dies sind meist zwei Nullen.

4.7.3 GUI-Referenz: *Passwort-Richtlinien*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Authentifizierung – Passwort-Richtlinien*

Passwort-Richtlinien bestehen aus einer Liste von Regeln, die die Sicherheit auf dem Server und im Unternehmen erhöhen. Dies wird dadurch erreicht, dass Benutzer aufgefordert werden starke Passwörter im Unternehmen zu verwenden, oder dass Passwörter der Benutzer nur einen begrenzten Zeitraum gültig sind.

4.7.3.1 *Passwort-Richtlinie*

Felder in dieser Tabelle

- *Name*: Name der Passwortrichtlinie.
- *Kommentar*: Weitere Information über die Passwortrichtlinie.
- *Standard*: Zeigt an, ob die Richtlinie standardmäßig für die Benutzer gilt.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Diese Aktion öffnet den Dialog zum Bearbeiten einer Passwortrichtlinie. Die Richtlinie namens Default kann nicht bearbeitet werden, mit dieser Aktion können die Detaileinstellungen eingesehen werden.
- *Löschen*: Diese Aktion löscht die gewählte Richtlinie.
- *Als Standard setzen*: Mit dieser Aktion kann eine Richtlinie als Standardrichtlinie für die Benutzer gesetzt werden.

Aktionen für dieses Formular

- *Hinzufügen*: Diese Aktion öffnet den Dialog, um eine neue Richtlinie hinzuzufügen.

4.7.3.2 GUI-Referenz: *Passwort-Richtlinie editieren*

Tab *Allgemein*
Felder in diesem Abschnitt

- *Name*: Hier wird eine kurze Bezeichnung für die Richtlinie eingegeben oder angezeigt.
- *Kommentar*: Weitere Informationen können in diesem Feld eingegeben werden.
- *Passwort muss geändert werden nach (Tage)*: Die Zahl gibt an, nach wie viel Tagen der Benutzer sein Passwort ersetzen muss. Bei Angabe von 0 Tagen braucht das Passwort nie geändert werden.
- *Erlaubte Logins nach Ablauf*: Wenn das Passwort abgelaufen

ist, darf der Benutzer diese bestimmte Anzahl von Logins noch vornehmen, bevor der Zugang gesperrt wird.

- *Benutzer vor Ablauf per E-Mail informieren*: Hier wird angegeben, ob eine E-Mail an den Benutzer versendet wird, bevor das Passwort geändert werden muss.
- *Tage vor Ablauf*: Dieser Wert gibt den Zeitpunkt an, zu dem der Benutzer vor dem Ablauf informiert werden soll.
- *Anzahl alter zu speichernder Passwörter*: Gibt an, wie viele verwendete Passwörter gemerkt werden sollen, um eine Wiederverwendung zu verhindern.
- *Minimale Passwort Länge*: Das Passwort muss mindestens die hier angegebene Anzahl von Zeichen aufweisen.
- *Passwort-Qualität prüfen*: Durch diese Option können weitere Kriterien angegeben werden, welche bei der Definition eines neuen Passworts überprüft werden.
- *Standard*: Gibt an, ob diese Richtlinie standardmäßig für Benutzer angewendet werden soll.

Tab *Qualitätskriterien*, Abschnitt *Minimale Anzahl von Zeichen* Felder in diesem Abschnitt

- *Zahlen*: Diese Anzahl von Zahlen muss mindestens im neuen Passwort vorkommen.
- *Großbuchstaben*: Diese Anzahl von Großbuchstaben muss mindestens im neuen Passwort vorkommen.
- *Kleinbuchstaben*: Diese Anzahl von Kleinbuchstaben muss mindestens im neuen Passwort vorkommen.
- *Sonderzeichen*: Diese Anzahl von Sonderzeichen muss mindestens im neuen Passwort vorkommen.

Tab *Benutzer*

Felder in diesem Abschnitt

- *Benutzer*: Wenn die Passwort-Richtlinie nicht standardmäßig auf alle Benutzer angewendet wird, können hier die entsprechenden Benutzer gewählt werden. Diese Benutzer unterliegen noch keiner Passwort-Richtlinie.

Aktionen für dieses Formular

- *Als Standard setzen*: Diese Aktion setzt die gewählte Richtlinie als Standardrichtlinie, diese gilt dann für alle Benutzer, für die keine spezielle Richtlinie angegeben wurde.
- *Löschen*: Löscht die gewählte Richtlinie.
- *Abbrechen*: Beendet den Dialog, die Änderungen werden verworfen.
- *Speichern*: Beendet den Dialog, die Änderungen werden gespeichert.

5 Authentifizierung

5.1 LDAP

Das „Lightweight Directory Access Protocoll“ (kurz „LDAP“) ist ein Protokoll zum Zugriff auf Verzeichnisdienste. Solche Verzeichnisdienste enthalten Informationen über Benutzer, Rechner und weitere Resourcen in einem Netzwerk. Eine spezialisierte Form eines Verzeichnisdienstes ist „Active Directory“.

Im V-Cube wird „OpenLDAP“ eingesetzt, eine Implementierung von Version 3 des LDAP. Es wird genutzt, um Benutzer, deren Passwörter, Telefonnummer, Mailadressen usw. zu speichern. Dabei handelt es sich um Konfigurationseinstellungen, die von den verschiedenen beteiligten Diensten im V-Cube abgefragt werden. Das LDAP kann aber auch für die lokalen Anwender zugänglich gemacht und genutzt werden, um ein globales Adressbuch für den Mailclient aufzubauen.

Intern werden die Daten im LDAP in einer Baumstruktur abgelegt. Die Daten werden dabei als Objekte bezeichnet, die jeweils Attribute mit Einträgen haben. Durch die Baumstruktur ist etwa der Zugriff auf eine E-Mail-Adresse über folgenden Pfad möglich: Firma – Mitarbeiter – Abteilung – Person – E-Mail-Alias. Parallel zu Mitarbeiter könnte der Objektzweig „Server“ im LDAP-Baum existieren. Bei Abteilung wäre die Aufteilung in „Vertrieb“, „Entwicklung“ usw. denkbar.

Die Adressierung eines Objekts im LDAP erfolgt über den DN („Distinguished Name“). Jeder DN besteht seinerseits aus relativen Distinguished Names (RDN) (die den Ast im LDAP-Baum darstellen). Einzelne RDN-Attribute sind etwa:

- *uid:* Benutzername (User ID)
- *dc:* Domainnamen-Komponente
- *cn:* Name (Common Name)

- *l:* Ortangabe (Location)
- *st:* Bundesland (State)
- *o:* Organisation
- *ou:* Abteilung (Organisation Unit)

Wird bereits ein LDAP im Unternehmen eingesetzt, kann der V-Cube so konfiguriert werden, dass er auf dieses LDAP zugreift. Dann können vorhandene Benutzer und Gruppen verwendet werden. Voraussetzung dafür ist jedoch, dass die genutzten Objektklassendefinitionen kompatibel sind.

5.1.1 GUI-Referenz: *LDAP*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Authentifizierung – LDAP*)

In diesem Dialog werden die Einstellungen für das LDAP vorgenommen.

Hier kann angegeben werden, ob dieses System als Master arbeiten soll (also seinen eigenen LDAP-Datenbestand erzeugt), oder ob es nur Daten aus einem anderen LDAP-Verzeichnis importieren soll.

Damit dieses System der Master für ein LDAP-Verzeichnis auf einem anderen Rechner sein kann, müssen bestimmte Voraussetzungen an die Struktur des Verzeichnisses erfüllt sein.

5.1.1.1 Tab *Grundeinstellungen*

Felder in diesem Abschnitt

- *Arbeitsmodus*: Der Betrieb des LDAP-Servers kann in drei Modi erfolgen, wobei der Serverdienst in jedem Modus lokal gestartet wird. Es ändert sich lediglich die Art der Datenhaltung und die Art des Datenaustauschs.

Im Modus „Lokaler Master“ werden die Daten lokal im LDAP-Verzeichnis verwaltet. Durch entsprechende Gruppenberechtigungen können diese von einer LDAP-Replik oder von einem LDAP-Proxy benutzt werden.

Im Modus „Replik“ werden Daten durch den angegebenen LDAP-Server (Master) repliziert. Dies geschieht innerhalb einer andauernden Netzwerkverbindung zwischen Master und Replik. Ändern sich die Daten des Masters, werden diese sofort über die bestehende Verbindung an die Replik übermittelt und somit abgeglichen. Man spricht von „push-based synchronization“. Bei Dialup-Verbindungen kann dies nach einem definierten Zeitintervall geschehen, so dass Kosten reduziert werden können.

Der Modus „Proxy“ leitet LDAP-Anfragen prinzipiell an den LDAP-Server (Master) weiter, ohne dass Daten zwischengespeichert werden. Der Proxy nimmt Anfragen also stellvertretend entgegen und reicht diese weiter.

- *LDAP-Server*: In diesem Eingabefeld wird der Hostname des LDAP-Servers angegeben. Dieses Feld wird nur sichtbar, wenn der lokale LDAP-Server deaktiviert ist.
- *Port*: Üblicherweise läuft ein LDAP-Server auf Port 389. Hier kann ein davon abweichender Port angegeben werden.
- *Optimierung für Dialup-Verbindungen*: Sollen Daten eines entfernten LDAP-Verzeichnisses auf diesen Server repliziert werden, so kann hier auf die Synchronisation per Abholung umgestellt werden. Die Replik gleicht nach einem zu bestimmenden Zeitintervall Daten aus dem entfernten LDAP-Verzeichnis ab. Dies ist vor allem für Dialup-Verbindungen, zum Beispiel ISDN, geeignet.
- *Synchronisationsintervall*: Hier kann das Intervall angegeben werden, nach dem die Daten des LDAP-Servers mit der lokalen Replik sychronisiert werden.
- *Wurzel der Hierarchie*: Hier muss die Wurzel des Namensrau-

mes für das LDAP-Verzeichnis angegeben werden. Als Vorgabe erscheint die Umsetzung der DNS-Domain, die unter *Netzwerk – DNS* eingetragen ist. Die DNS-Domain muss jedoch nicht zwingend als Base-DN für das LDAP-Verzeichnis verwendet werden.

Wenn dieses System der Master für das Verzeichnis ist, werden die meisten Daten aus der lokalen Konfiguration erzeugt. Bestimmte Angaben (wie etwa Benutzerpasswörter) werden aber nur im LDAP-Verzeichnis abgelegt. Daher kann die Wurzel der Hierarchie nicht mehr nachträglich geändert werden.

- *Wurzel der Hierarchie (Base-DN/Suffix)*: Hier wird die Wurzel des Namensraumes für das LDAP-Verzeichnis angezeigt.
- *Bind-DN*: Der Bind-DN wird zum Anmelden am LDAP-Server verwendet und entspricht einem Login-Namen bei anderen Protokollen.

  Wenn ein lokales LDAP-Verzeichnis erstellt wird, wird dieser DN als „Root-DN“ eingesetzt. Ein Benutzer, der sich mit dem Root-DN angemeldet hat, unterliegt keinen administrativen Einschränkungen.

  Wird ein anderes System als LDAP-Server benutzt, muss der Account ausreichende Rechte besitzen.

  Wird das Feld leer gelassen, wurde die Vorgabe „cn=Manager, <Base-DN>“ verwendet.
- *Bind-Passwort*: Hier wird das Passwort für die Verbindung zum LDAP-Server eingetragen.

  Wird der lokale LDAP-Server verwendet, bestimmt diese Angabe das Passwort für den Root-DN (mit dem der administrative Zugriff erfolgt), andernfalls wird das Passwort für die Verbindung zum anderen Server verwendet.
- *Bind-Passwort (Wiederholung)*: Da das Passwort aus Sicherheitsgründen während der Eingabe nicht angezeigt wird, muss es hier noch einmal wiederholt werden.

- *Serverzertifikat*: Hier kann für den LDAP-Server ein Zertifikat ausgewählt werden. In der Liste sind alle installierten Zertifikate enthalten, die für den Server geeignet sind. Wird das LDAP nur innerhalb dieses Systems verwendet, ist kein Zertifikat notwendig.

5.1.1.2 Tab *Berechtigungen*

Felder in diesem Abschnitt

- *Zugang zu LDAP-Port erlauben für*: Alle Rechner und Netze, die zu einer der aktivierten Gruppen gehören, bekommen Zugriff auf den LDAP-Server. Benutzer sind von dieser Einstellung nicht betroffen.
- *Zugang zu LDAP-SSL-Port erlauben für*: Alle Rechner und Netze, die zu einer der aktivierten Gruppen gehören, bekommen verschlüsselten Zugriff via SSL auf den LDAP-Server. Benutzer sind von dieser Einstellung nicht betroffen.

  Hinweis: Um den Server mit SSL ansprechen zu können, muss in den Grundeinstellungen ein entsprechendes Zertifikat ausgewählt werden.
- *Zugriff auf das globale Adressbuch für*: Alle Benutzer, die zu einer der aktivierten Gruppen gehören, bekommen Lesezugriff auf das im LDAP-Server gespeicherte globale Adressbuch. Rechner und Netze sind von dieser Einstellung nicht betroffen.
- *Schreibzugriff auf globales Adressbuch*: Alle Benutzer, die zu einer der aktivierten Gruppen gehören, dürfen Änderungen im globalen Adressbuch vornehmen. Rechner und Netze sind von dieser Einstellung nicht betroffen.

5.2 Unterstützung von Windows-Domänen

In einer Windows-Domäne ist immer ein zentraler Server vorhanden: der „primäre Domänencontroller“ oder kurz „PDC“. An diesem erfolgt die Anmeldung der Benutzer, und die Benutzer können hier Daten ablegen (Homeverzeichnisse, Desktop-Profile usw.). In manchen Netzen wird der PDC durch einen oder mehrere Server ergänzt, die für Redundanz sorgen. Sie verfügen aber auch nur über die Konfigurationsinformationen des PDC, sie sind „Backup Domain Controller“ oder kurz „BDC“.

Der V-Cube kann auf vielfältige Weise an Windows-Domänen teilnehmen. Ist bereits ein Windows-Server vorhanden, der eine Domäne bereitstellt, kann der V-Cube ein Mitglied in dieser Domäne werden. Bei einem NT4-Server ist weitreichender Zugriff auf die Domäne möglich. Bei Servern auf der Basis von *Active Directory* (ADS) geht die Integration noch nicht ganz so weit. Aber auch bei ADS-Domänen kann auf die Benutzer- und Gruppenkonfiguration der Domäne zurückgegriffen werden, um Dienste bereitzustellen.

5.2.1 GUI-Referenz: SMB-/CIFS-Server

Auf dem V-Cube wird für die Netzwerkfunktionalität in Windows-Netzen das Softwarepaket „Samba“ verwendet. Dies wird oft als „SMB“ abgekürzt, wobei SMB eigentlich nur das Protokoll bezeichnet („Server Message Block"“).

Das „CIFS“ („Common Internet File System“) stellt eine erweiterte Version von SMB dar und wird ebenfalls vom V-Cube unterstützt.

5.2.1.1 *Windows-Support – Allgemein*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Windows-Support – Allgemein*)

In diesem Abschnitt wird die Unterstützung für Windows-Netzwerke konfiguriert. Wird diese eingeschaltet, erscheinen in anderen Dialogen zusätzliche Optionen.

In den Benutzungsrichtlinien kann im Dialog *PDC/ADS* die Authentifizierung an einer NT-Domäne aktiviert werden. Unter *Serverdienste* können im Dialog *File-Shares* Laufwerksfreigaben für Windows-Rechner angelegt werden.

Tab *Grundeinstellungen*
Felder in diesem Abschnitt

- *Aktivieren*: Hiermit wird die Unterstützung für Windows-Netzwerke aktiviert.

  Wird diese Option aktiviert, erscheint das System in der Netzwerkumgebung der Windows-Rechner.
- *Arbeitsgruppe oder Domäne*: Hier muss der Name der Arbeitsgruppe oder der Windows-Domäne angegeben werden.

  Aus verschiedenen Gründen sollte der Name der Arbeitsgruppe normalerweise mit dem ersten Abschnitt der DNS-Domain in Großbuchstaben übereinstimmen (für eine Domain „intern.example.com“ also die Arbeitsgruppe „INTERN“).

Tab *Berechtigungen*
Felder in diesem Abschnitt

- *Unterstützung für diese Gruppen*: Rechner und Netze, die zu einer aktivierten Gruppe gehören, erhalten Zugriff, damit sie sich an der Windows-Umgebung authentifizieren können.

Rechner und Netze, die eine Zugriffsberechtigung auf über SMB exportierte Freigaben haben, dürfen auf die Windows-Dienste dieses Systems ohnehin zugreifen.

Tab *Optionen*
Felder in diesem Abschnitt

- *Serverinformation*: Hier kann ein Kommentartext für den Server gesetzt werden. Dieser wird auf Windows-Systemen in der Netzwerkumgebung angezeigt.
- *Zeichenkodierung für Dateinamen*: Hier muss der Zeichensatz festgelegt werden, der für die Dateinamen verwendet wird, die über Windows-Filesharing auf diesem System abgelegt werden.

  Windows und Samba verwenden normalerweise *Unicode* (genauer die *UTF-8*-Kodierung). In dieser Kodierung lassen sich zwar die Schriftzeichen aller Sprachen darstellen, allerdings kann UTF-8 zu Problemen führen, wenn das Verzeichnis über andere Dienste exportiert wird. FTP-Client-Software erwartet beispielsweise meist keine UTF-8-Dateinamen und stellt Dateinamen daher nicht korrekt dar.

  Wird geplant, Verzeichnisse auch über andere Dienste zu exportieren, sollte hier eine andere Kodierung eingestellt werden. Im mitteleuropäischen Raum wird üblicherweise *ISO-8859-15* verwendet.

  Die Zeichenkodierung ist nur für solche Dateinamen relevant, die Zeichen enthalten, die nicht im *US-ASCII*-Zeichensatz vorkommen (Umlaute usw.).
- *WINS*: Wenn die Unterstützung für Windows-Netzwerke aktiviert ist, kann in dieser Liste eingestellt werden, wie sich das System gegenüber dem WINS (Windows Name Service) verhalten soll.

  Wird im Netzwerk kein WINS-Server betrieben und soll das Sy-

stem auch nicht als WINS-Server arbeiten, wird *Nein* eingestellt.

Wird ein WINS-Server im Netz betrieben, kann hier *Client* eingestellt und die IP-Adresse des WINS-Servers angegeben werden.

Wenn der V-Cube selbst als WINS-Server arbeiten soll, sollte hier *Server* eingestellt werden.

Mit der Einstellung *Proxy* ist es möglich, Anfragen von einem Subnetz an einen WINS-Server in einem anderen Netzwerksegment weiterzureichen. Die IP-Adresse des WINS-Servers muss dann im Folgenden Feld eingetragen werden.

- *WINS-Server*: Hier wird die IP-Adresse des WINS-Servers für die Arbeitsgruppe oder die Windows-Domäne angegeben.
- *Winbind-Cachezeit (in Sekunden)*: Winbind übernimmt die Namensauflösung im Windows-Netzwerk. Hier wird eingestellt, wie lange Namen im Cache behalten werden. Gültige Werte liegen zwischen 0 und 3600 Sekunden. Bei Eingabe von ungültigen Werten werden 300 Sekunden eingetragen.
- *Domänenseparator*: Bei Namen von Gruppen und Benutzern, die aus einer Windows-Domäne importiert werden, wird immer der Domänenname vorangestellt. Das hier ausgewählte Zeichen wird als Trennzeichen zwischen dem Domänennamen und dem Benutzer- bzw. Gruppennamen eingefügt.
- *Exportiere Heimatverzeichnisse der Benutzer*: Hier wird eingestellt, ob die Heimatverzeichnisse der eingerichteten Benutzer exportiert werden sollen.

5.2.1.2 *System für ADS-Domäne vorbereiten*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Windows-Support – Für ADS vorbereiten*)

Die *Vorbereitung für ADS-Domäne* soll helfen, die notwendigen Ein-

stellungen vorzunehmen und zu prüfen, damit das System erfolgreich in eine ADS-Domäne aufgenommen werden kann.

Dazu müssen verschiedene Dienste, zum Beispiel der DNS-Dienst oder das Authentifizierungs-Subsystem, korrekt konfiguriert sein; die notwendigen Einstellungen hierfür sind jedoch auf verschiedene Dialoge verteilt.

Hinweis: Durch diese Angaben werden Einstellungen in anderen Dialogen ohne weitere Warnung überschrieben. Davon betroffen sind die Einstellungen für Kerberos, DNS, Authentifizierung und Windows-Unterstützung. Angaben zu Netzwerken, Netzwerklinks oder Gruppen werden nicht geändert.

Nachdem die Konfiguration angepasst wurde, muss die neue Konfiguration aktiviert werden, bevor das System über den Dialog *Domänenbeitritt* in die Domäne aufgenommen werden kann.

Abschnitt *ADS-Einstellungen*

In diesem Abschnitt können die Einstellungen für die ADS-Domäne angegeben werden. Wenn das System noch nicht für ADS konfiguriert ist, versucht das System, diese Einstellungen automatisch zu ermitteln.

Felder in diesem Abschnitt

- *Name des Systems*: Hier wird der Name des Systems angegeben. Dieser Name wird zusammen mit der ADS-Domäne verwendet, um den FQDN des Systems festzulegen.
- *Domäne*: Hier wird die Domäne eingetragen. Diese Einstellung beeinflusst den Namen der DNS-Domäne, den FQDN dieses Systems, die Kerberos-Realm und den abgekürzten Namen der ADS-Domäne.

- *IP-Adresse des Domänencontrollers*: Hier wird die IP-Adresse des zu verwendenden Domänencontrollers angegeben. Diese Einstellung konfiguriert den DNS-Dienst.
- *IP-Adresse eines Backup-Domänencontrollers*: Hier kann ein weiterer Domänencontroller angegeben werden, der benutzt wird, wenn der primäre Domänencontroller nicht erreichbar ist.
- *DC ist WINS-Server*: Wird ein größeres Windows-Netzwerk betrieben, ist meist ein WINS-Server zur Namensauflösung im Einsatz. Durch das Aktivieren dieser Option wird der Domänencontroller als WINS-Server verwendet.

Abschnitt *Report*

In diesem Abschnitt werden die Ergebnisse der Überprüfung aller zur Integration in eine ADS-Umgebung relevanten Einstellungen des Systems angezeigt.

Felder in diesem Abschnitt

- *DNS-Server*: Der DNS-Server sollte aktiviert sein. Diese Anzeige gibt Auskunft über den aktuellen Status.
- *DNS-Suchliste*: Die ADS-Domäne sollte in der DNS-Suchliste aufgeführt sein.
- *DNS-Zone*: In der Regel verwaltet der AD-Server die DNS-Zone, die zur ADS-Domäne gehört. Auf dem V-Cube sollte eine Weiterleitung dieser DNS-Zone zum ADS-Controller eingerichtet sein.

  Hinweis: Eine Weiterleitung aller DNS-Anfragen an den ADS-Controller ist in den meisten Fällen nicht sinnvoll.
- *Systemname*: Diese Anzeige gibt Auskunft, ob der Name des Systems in der ADS-Domäne enthalten ist.
- *Windows-Unterstützung*: Hier wird angezeigt, ob die Unterstützung für Windows-Netzwerke grundsätzlich aktiviert ist.

- *WINS*: Dieses Feld zeigt, ob die Verwendung eines WINS-Servers für die Namensauflösung im Windows-Netzwerk aktiviert ist.
- *Arbeitsgruppe/Domäne*: Hier wird geprüft, ob die eingestellte Domäne als Abkürzung für die ADS-Domäne passt. Die Abkürzung sollte dem ersten Teil der ADS-Domäne entsprechen.
- *Kerberos-Server*: Der lokale Kerberos-Server muss deaktiviert sein. Hier wird geprüft, ob dies der Fall ist.
- *Kerberos-Realm*: Die eingestellte Kerberos-Realm muss dem Namen der ADS-Domäne in Großbuchstaben entsprechen. Dieses Feld enthält das Ergebnis der entsprechenden Prüfung.
- *ADS-Authentifizierung*: Gibt an, ob die Authentifizierung gegen ADS eingeschaltet ist.

5.2.1.3 *Windows-Gruppen Zuordnung*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Windows-Support – Windows-Gruppen Zuordnung*

Um Mitgliedern von Systemgruppen, die sich am lokalen PDC-Server anmelden, Windows-Berechtigungen zu vererben, kann hier die entsprechende Zuordnung vorgenommen werden. Sollen angemeldete Benutzer aus der lokalen Administrator-Gruppe ebenso Administrator-Rechte auf dem Microsoft Windows-PC erhalten, ist die Zuordnung „Domain-Admins“ zu „Administrators“ einzustellen.

Zuordnungstabelle

Diese Tabelle dient als Übersicht der zugeordneten Windows-Gruppen. Jeder Eintrag kann hier ebenso bearbeitet werden, eine Vererbung der Rechte findet nur dann statt, wenn der Collax-Server als PDC aktiviert ist.

Spalten in der Tabelle

- *Vordefinierte Windows-Gruppe*: In dieser Spalte werden die von Microsoft Windows vordefinierten NT-Domänengruppen angezeigt.
- *Lokale Gruppe*: Wenn eine Zuordnung für die Vererbung von Windows-Berechtigungen gesetzt ist, wird in dieser Spalte die entsprechende Berechtigungsgruppe des Collax Servers angezeigt. Ist keine Zuordnung gesetzt, bleibt die entsprechende Zeile leer.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion über das Kontextmenü (rechter Mausklick oder Doppelklick) kann die ausgewählte Zuordnung bearbeitet werden.

Zuordnung bearbeiten

Felder in diesem Formular

- *Vordefinierte Windows-Gruppe*: Hier wird die Windows-Gruppe angezeigt, deren Berechtigungen auf eine lokale Gruppe vererbt werden soll.
- *Lokale Gruppe*: In dieser Auswahl stehen alle bestehenden lokalen Gruppen für die Zuordnung zur Auswahl. Es kann nur eine Gruppe ausgewählt werden. Das Auswahlfeld kann auch leergelassen werden.

Aktionen für dieses Formular

- *Abbrechen*: Bearbeiten der Gruppenzuordnung beenden. Die Änderungen werden verworfen.
- *Speichern*: Bearbeiten der Gruppenzuordnung beenden. Die Änderungen werden gespeichert.

5.2.1.4 *Der Windows-Domäne beitreten*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Windows-Support – Domänenbeitritt*)

Hier kann das System bei einem Windows-Domänencontroller angemeldet und in die Domäne aufgenommen werden.

Felder in diesem Dialog

- *Benutzerdatenbank*: Hier wird angezeigt, ob die Benutzerdatenbank lokal oder auf einem PDC abgelegt ist.
- *Hinweis:* In diesem Feld erscheint ein Hinweis, wenn ein Domänenbeitritt nicht möglich ist. Meistens wurden in diesem Fall noch nicht alle Einstellungen passend vorgenommen. Im angezeigten Text finden sich weitere Hinweise dazu.
- *Domäne*: Hier wird die auf dem System eingestellte Domäne angezeigt.
- *Administrator-Account*: Hier muss der Benutzername eines Administrator-Accounts auf dem Domänencontroller angegeben werden. Das Feld kann leer bleiben, wenn auf dem DC bereits ein Maschinenaccount angelegt wurde.
- *Passwort*: Hier muss das Passwort für den Administrator-Account angegeben werden. Auch dieses Feld kann leer bleiben, wenn der Maschinenaccount bereits angelegt wurde.

Hinweis: Das Kennwort wird einzig für die Anmeldung des Systems beim Domänencontroller genutzt und nicht lokal gespeichert.

- *DC*: Hier ist der Hostname des Domänencontrollers anzugeben.

Aktionen für diesen Dialog

- *Anmelden*: Diese Aktion versucht, mit den eingestellten Werten eine Anmeldung am Domain-Controller durchzuführen.
- *Abmelden*: Diese Aktion meldet das System am Domänencontroller ab.

5.2.2 GUI-Referenz: *Kerberos*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Authentifizierung – Kerberos*)

Kerberos ist ein komplexes Verfahren zur Authentifizierung von Benutzern und Servern in einem ungesicherten TCP/IP-Netzwerk. Benutzer und Dienste werden mit Hilfe eines speziellen Netzwerkdienstes, des KDC (Key Distribution Center), authentifiziert. Der KDC stellt die vertrauenswürdige Instanz im Netz dar. Bei Kerberos werden keine Passwörter im Klartext über das Netzwerk übertragen.

Wenn eine *lokale* Benutzerdatenbank eingestellt wurde, kann zusätzlich der KDC auf dem System aktiviert werden. Die meisten Unix-Varianten (und auch Linux) können Kerberos zur Authentifizierung nutzen. Windows 2000 unterstützt ebenfalls Kerberos, benötigt jedoch eine manuelle Konfiguration.

Beim Aufbau einer Verbindung erfolgt eine Authentifizierung des Clients und des Servers gegen den KDC. Auch der KDC authentifiziert sich gegenüber Client und Server. Möchte der Client eine Verbindung

zum Server aufbauen, identifiziert er sich am KDC und erhält im Gegenzug ein „Ticket“, eine Art elektronische Eintrittskarte. Mit diesem kann er die Verbindung zum Server aufbauen. Dadurch ist ein „Single-Sign-On“ möglich, bei dem sich der Benutzer nur einmal innerhalb der Sitzung authentifiziert und dennoch verschiedene Dienste (Server) nutzen kann.

5.2.2.1 Tab *Grundeinstellungen*

Felder in diesem Abschnitt

- *Lokalen Server aktivieren*: Diese Option aktiviert den Kerberos-Dienst auf diesem System.
- *UDP verwenden*: Wenn diese Option aktiviert ist, werden bei der Authentifizierung UDP-Datenpakete anstelle von TCP-Paketen verwendet.

  Ist diese Option nicht aktiviert, werden TCP-Pakete genutzt, um mögliche Probleme mit bestimmten KDCs zu vermeiden, die zu große Antwortpakete verschicken. Dies kann zum Beispiel geschehen, wenn ein Windows ADS-Server Tickets für Benutzer herausgibt, die in sehr vielen Gruppen Mitglied sind.

  Da UDP in der Regel schneller als TCP ist, sollte diese Option aktiviert werden, wenn ein KDC ohne ADS verwendet wird oder wenn sich der ADS-Controller an einem entfernten Standort befindet und das angesprochene Problem nicht auftritt.
- *KDCs*: Hier kann eine Liste von KDCs für die Kerberos-Realm angegeben werden. Die einzelnen Einträge werden durch ein Komma oder Leerzeichen voneinander getrennt.

  Dieses Feld kann leer bleiben, wenn der oder die KDCs im DNS aufgeführt sind.
- *Kerberos-Realm*: Die Kerberos-Realm ist der Bereich, in dem eine

Authentifizierung gültig ist. Benutzer innerhalb eines Bereichs können sich gegenüber jedem Dienst auf einem Rechner in der Realm ausweisen.

Aus verschiedenen Gründen sollte der Name der Realm normalerweise mit der DNS-Domain in Großbuchstaben übereinstimmen (für die Domain „intern.example.com“ also die Realm „INTERN.EXAMPLE.COM“).

5.2.2.2 Tab *Berechtigungen*

Felder in diesem Abschnitt

- *Authentifizierung über KDC*: Alle Rechner und Netze, die zu einer der aktivierten Gruppen gehören, dürfen auf den KDC zugreifen. Benutzer sind von dieser Einstellung nicht betroffen.

  Diese Berechtigung ist die Voraussetzung dafür, dass sich Benutzer und Server gegenseitig authentifizieren können.

  Das Feld wird nur angezeigt, wenn auf diesem System ein KDC betrieben wird.
- *Administration Kerberos-Dienst*: Alle Rechner und Netze, die zu einer der aktivierten Gruppen gehören, bekommen Zugriff auf den Kerberos-Administrations-Dienst. Benutzer sind von dieser Einstellung nicht betroffen.

  Diese Berechtigung ist nur für solche Rechner notwendig, die in die Kerberos-Realm aufgenommen werden sollen.

  Das Feld wird nur angezeigt, wenn auf diesem System ein KDC betrieben wird.

5.2.3 GUI-Referenz: *PDC/ADS*

In diesem Dialog wird festgelegt, wo die Prüfung von Benutzerpasswörtern erfolgen soll. Die Voreinstellung sieht die Verwendung einer lokalen Benutzerdatenbank vor.

Alternativ können die Benutzer und deren Passwörter auf einem anderen System verwaltet und die Daten über ein entsprechendes Protokoll importiert werden.

5.2.3.1 *PDC/ADS*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Windows-Support – PDC/ADS*)

Felder in diesem Dialog

- *Benutzerdatenbank*: Zur Authentifizierung von Benutzern können verschiedene Server befragt werden.

  Mit der Einstellung *Lokal* wird die Benutzerdatenbank auf diesem System verwendet. Alle Benutzerinformationen sind im LDAP-Verzeichnis gespeichert.

  Mit der *NT-Domäne* muss dieses System in eine bestehende NT-Domäne aufgenommen werden. Danach kann die Authentifizierung gegen den primären Domänencontroller („PDC“) durchgeführt werden.

  Moderne Windows-Domänen verwenden *Active Directory Service* („ADS“) als interne Datenbank. Mit der Einstellung *ADS-Mitglied* kann dieses System den ADS befragen. Es muss dazu in die ADS-Domäne aufgenommen werden.
- *NT-/ADS-Domäne*: Hier wird die Windows-NT- oder ADS-Domäne

angezeigt, die in den Netzwerkeinstellungen konfiguriert wurde.

- *Benutzerabhängiges Anmeldeskript verwenden*: Diese Option darf nicht aktiviert werden, wenn bereits ein anderes System im Netzwerk als PDC betrieben wird. Andernfalls kann es dazu kommen, dass sich die Benutzer nicht mehr an der Domäne anmelden können.
- *Active Directory Server*: Wenn dieses System als Mitglied einer ADS-Domäne konfiguriert ist, wird die Authentifizierung ausschließlich am ADS-Server durchgeführt. In diesem Feld kann der Name des ADS-Servers eingegeben werden. Bleibt das Feld leer, wird der ADS-Server der Domäne automatisch gesucht.
- *PDC*: Hier wird der Name des PDC für die Domäne angegeben. Dieser wird für die Authentifizierung von Passwörtern kontaktiert. Bleibt das Feld leer, sucht das System automatisch nach einem PDC für die Domäne.

  Hinweis: In diesem Feld muss der *NetBIOS*-Name des PDC angegeben werden. Dieser ist nicht immer identisch mit dem DNS-Namen.
- *BDC*: Hier kann eine Liste von Backup-Domain-Controllern für die NT-Domäne angegeben werden. Die Angabe in diesem Feld kann IP-Adressen oder Namen der Server enthalten. Die Liste muss mit Komma und Leerzeichen getrennt werden: NT-BDC, NT-BDC1, NT-BDC2
- *Benutzer aus anderen Domänen zulassen*: Wird diese Option aktiviert, können sich Benutzer aus anderen Domänen am System anmelden. Voraussetzung ist, dass eine Vertrauensstellung zwischen den Domänen besteht.

  Durch das Aktivieren dieser Option wird der Domänencontroller der entfernten Domäne zur Authentifizierung kontaktiert. Dies kann bei großen Domänen und/oder langsamen Netzwerkverbindungen zu Problemen führen.

Aus Sicherheitsgründen sollte eine Aktivierung dieser Option gründlich geprüft werden.

- *Active Directory-Proxy aktivieren*: Ist ein V-Cube Mitglied eines Active Directory kann mit dieser Option die Funktion gestartet werden, um benutzerbezogene Daten aus dem Active Directory ins lokale Benutzerverzeichnis zu kopieren. Diese Daten aus dem Active Directory werden regelmäßig überprüft, und, falls erforderlich, werden Änderungen aus dem Active Directory lokal übernommen.

  Diese Funktion kann benutzt werden, falls für lokale Dienste bestimmte Benutzerdaten aus dem Active Directory ausgelesen werden müssen.

  Beim ersten Start des AD-Proxy kann, je nach Größe des AD-Verzeichnisses, das Synchronisieren der Benutzerdaten einige Minuten dauern.
- *Windows LDAP-Administrator*: Hier muss der Benutzer angegeben werden, der Leseberechtigung auf das Active Directory hat.
- *Passwort*: Hier wird das Passwort des Benutzers eingegeben.

6 Verschlüsselung

6.1 Einführung

Verschlüsselung dient der sicheren Übertragung von Information. Bereits im Altertum wurden erste Verschlüsselungsverfahren eingesetzt. Dabei wurden Ersetzungsvorschriften verwendet, die geheimgehalten werden mussten. Ende des 19. Jahrhunderts formulierte ein Wissenschaftler den Grundsatz, dass die Sicherheit eines kryptographischen Verfahrens allein auf dem Schlüssel basiert. Das Verfahren selbst kann offengelegt werden. In den letzten 60 Jahren machte die „Kryptographie“ durch zunehmend bessere technische Möglichkeiten rasante Fortschritte.

Heutzutage ist neben der Verschlüsselung zur Wahrung der „Vertraulichkeit“ auch die Sicherung der „Integrität“ wichtig. Beides schützt die Information vor unbefugtem Zugriff von außen, d. h. vor Einsichtnahme und vor Manipulation. Eine weitere wichtige Anforderung ist die „Authentizität“, d. h. die Gewissheit darüber, wirklich mit der richtigen Person Daten auszutauschen und nicht auf eine fingierte Information hereinzufallen.

Die ursprüngliche Information, die geschützt werden soll, wird als „Ursprungstext“ bezeichnet. Die verschlüsselte Information wird „Chiffriertext“ genannt. Die Transformation von Ursprungstext in Chiffriertext bezeichnet man als „Verschlüsselung“ oder „Chiffrierung“. Der Zurückwandlung vom Chiffriertext in den Ursprungstext ist die „Entschlüsselung“ oder „Dechiffrierung“. Dechiffrierung findet auch statt, wenn ein Angreifer mit eigenen Methoden eine Entschlüsselung vornehmen kann.

Zunächst wurden „symmetrische Verfahren“ entwickelt, bei denen

derselbe „Chiffrierschlüssel“ für die Verschlüsselung und später für die Entschlüsselung verwendet wird. Der offensichtliche Schwachpunkt dieses Verfahrens ist, dass der Austausch des Chiffrierschlüssels zum Kommunikationspartner gesichert erfolgen muss. Nachteilig ist zudem, dass mit jedem neuen Partner ein neuer Schlüssel ausgehandelt werden muss, was die Anzahl der Schlüssel schnell in die Höhe treibt. 1977 wurde mit „DES“ („Data Encryption Standard“) ein symmetrisches Verfahren als Standard für US-amerikanische Behörden eingeführt.

Diese Nachteile dieses Verfahrens werden durch „asymmetrische Verfahren“ umgangen; sie werden auch als „Public-Key-Kryptographie“ bezeichnet. Hierbei wird für jeden Teilnehmer ein „Schlüsselpaar“ erzeugt. Die eine Komponente ist der öffentliche Schlüssel („Public Key“), die andere der geheime, private Schlüssel („Private Key“). Entscheidend dabei ist, dass der zweite Schlüssel nicht einfach aus dem ersten Schlüssel errechnet werden kann. RSA ist ein verbreitetes asymmetrisches Verfahren.

Bei der Schlüsselerzeugung wird daher meist auf das Problem der Zerlegung einer natürlichen Zahl in ihre Primfaktoren zurückgegriffen: Die Zahl 2117 ist das Produkt der beiden Primzahlen 29 und 73. Die Zerlegung der Zahl 2117 in ihre Primfaktoren ist sehr aufwendig. Der umgekehrte Weg, zwei oder mehr Primzahlen auszuwählen und deren Produkt zu bilden, jedoch nicht. In der Praxis werden Primzahlen mit 300 und mehr Stellen verwendet, was auch für leistungsfähige Computersysteme eine deutliche Hürde darstellt (mit den heute bekannten Methoden wird die Dauer einer solchen Faktorisierung auf Millionen von Jahren geschätzt). Auf dieser Grundlage werden die beiden Schlüsselanteile aus einem gemeinsamen Satz an Primzahlen erzeugt. Dadurch, dass eine Zerlegung in die einzelnen Primbestandteile derzeit nicht möglich ist, kann der zugehörige zweite Schlüssel nicht berechnet werden.

Um zwischen zwei Teilnehmern eine Information verschlüsselt auszutauschen, benötigt der Absender den öffentlichen Schlüssel des Empfängers. Mit diesem verschlüsselt er den Ursprungstext und überträgt den Chiffretext an den Empfänger. Jeder, der diesen Chiffretext abfängt, sollte nur Zugriff auf den öffentlichen Schlüssel des Empfängers haben. Mit diesem ist eine Dechiffrierung jedoch nicht möglich. Nur der Empfänger verfügt über den passenden privaten Schlüssel, mit dem er die Information entschlüsseln kann.

Die Integrität der Information kann durch eine Prüfsumme garantiert werden. Dazu stehen verschiedene Algorithmen zur Verfügung, einer der bekanntesten ist MD5. Der Absender der Information berechnet dazu vor dem Versenden eine Prüfsumme über die Information. Diese Prüfsumme verschlüsselt er mit seinem privaten Schlüssel und fügt sie der Übertragung bei. Der Empfänger der Nachricht kann seinerseits eine Prüfsumme berechnen und mit Hilfe des öffentlichen Absenderschlüssels die Prüfsumme des Absenders entschlüsseln. Sind beide identisch, liegt die Originalinformation vor. Sind sie unterschiedlich, muss die Information auf dem Zwischenweg modifiziert worden sein.

Hier zeigt sich sehr deutlich das Zusammenspiel von Public und Private Key für Verschlüsselung und Integritätssicherung. Der Vorteil dieses Verfahrens ist der unkritische Schlüsselaustausch: Der Kommunikationspartner benötigt immer nur den eigenen öffentlichen Schlüssel. Dieser ist aber öffentlich, also nicht besonders schützenswert.

Nun muss als dritte Anforderung die Sicherung der Authentizität umgesetzt werden. Sind die beiden Kommunikationspartner miteinander bekannt, können sie die öffentlichen Schlüssel persönlich austauschen. So können sie sicher sein, wirklich mit der richtigen Gegenseite zu kommunizieren und nicht mit einem Angreifer, der seinen öffentlichen Schlüssel untergeschoben hat.

6.1.1 Zertifikate

Zertifikate sind in diesem Zusammenhang eine Art Transporthülle für asymmetrische Schlüssel und Informationen über den Besitzer des Schlüsselpaares. Beim Einlesen eines Zertifikats mit öffentlichem Schlüssel werden Name, Anschrift und weitere Informationen über den Inhaber des Zertifikats angezeigt. So kann sichergestellt werden, dass der Schlüssel des richtigen Kommunikationspartners verwendet wird.

Diese Informationen können jedoch auch gefälscht werden. Um diese Gefahr auszuschließen, kann jeder sein persönliches Zertifikat von einer Art elektronischem Notar „signieren“ lassen. Eine solche „Certificate Authority“ („CA“) prüft zunächst den Inhaber auf Echtheit (Lichtbildausweis, Handelsregisterauszug, usw.) und berechnet dann über den öffentlichen Schlüssel des Zertifikats eine Prüfsumme. Die Prüfsumme wird mit dem privaten Schlüssel der CA verschlüsselt und dem Zertifikat beigefügt.

Beim Verwenden eines auf diese Weise signierten Zertifikats muss wiederum die Prüfsumme ermittelt, die beigefügte Prüfsumme der CA mit dem öffentlichen Schlüssel der CA dechiffriert und beide miteinander verglichen werden. Sind sie identisch, ist garantiert, dass dieses Zertifikat tatsächlich dem angegebenen Inhaber zugeordnet ist.

Dieses Verfahren funktioniert nur, wenn die Signatur von einer vertrauenswürdigen CA ausgestellt wurde. Dies kann entweder eine eigene CA im Unternehmen oder eine externe sein, deren öffentlicher Schlüssel auf vertrauenswürdigem Wege besorgt werden kann. In modernen Webbrowsern beispielsweise sind die CA-Zertifikate der gängigen Anbieter solcher CA-Dienste hinterlegt. Damit ist der Anwender von der Beschäftigung mit Zertifikaten entbunden, üblicherweise schließt sich beim Aufbau einer verschlüsselten Verbindung

ein symbolisches Schloss. Achtung: In solchen Browsern können weitere CA-Zertifikate nachinstalliert werden. Der PC im Strandcafé von St. Tropez kann sich so schnell als falscher Freund erweisen.

Steht keine CA zur Verfügung, können auch „selbstsignierte“ Zertifikate erstellt werden. Auch solche Zertifikate können nicht automatisch auf ihre Vertrauenswürdigkeit hin überprüft werden.

Um den privaten Schlüssel eines Zertifikats zu schützen, kann dieser mit einer „Passphrase“ gesichert werden. Dieses Passwort muss dann jedes Mal, wenn mit dem privaten Schlüssel gearbeitet werden soll, eingegeben werden. Beim Einsatz eines Zertifikats für einen Server (Webserver o. ä.) darf keine Passphrase gesetzt sein. Ist dies doch der Fall, muss diese bei jedem Start des Servers eingegeben werden.

6.1.2 Aufbau eines X.509-Zertifikats

Ein häufig genutztes Format für Zertifikate ist der X.509-Standard.

```
Certificate:
    Data:
       Version: 3 (0x2)
       Serial Number: 1 (0x1)
       Signature Algorithm: md5WithRSAEncryption
       Issuer: CN=ca@untrustworthy.example.com, C=DE,
          ST=Bayern, L=Muenchen, O=Untrustworthy Ltd.,
          OU=Certificate Authority/emailAddress=
          ca@untrustworthy.example.com
       Validity
          Not Before: Nov 11 10:14:58 2005 GMT
          Not After : Apr 10 10:14:58 2007 GMT
       Subject: C=DE, ST=NRW, O=Elektro Britzel,
          OU=Netzwerk, CN=www.elektro-britzel.de
       Subject Public Key Info:
```

```
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
              Modulus (1024 bit):
                 00:c6:a5:4f:6b:cd:c3:b6:63:3f:6f:eb:a8:7c:13:
                 3f:25:7e:ce:a1:45:09:cb:3c:23:33:c6:0f:3c:b1:
                 7c:68:19:02:ab:80:7c:f9:e2:e4:fc:a1:1f:c5:ae:
                 6f:76:fe:f8:e7:90:16:4b:3a:ab:d4:24:16:18:24:
                 7a:bf:da:1f:45:d0:18:1a:1c:5e:b2:00:02:d2:e8:
                 77:2e:99:c9:01:b8:a0:33:ed:77:ed:6b:47:ad:97:
                 33:ae:97:18:f3:3e:cd:72:2b:bc:84:ad:cf:69:22:
                 d1:f8:15:11:f0:29:bc:c2:6d:20:5c:6c:fa:d3:c0:
                 79:7c:bd:4e:7c:df:d6:28:db
              Exponent: 65537 (0x10001)
          X509v3 extensions:
            Netscape Comment:
              Zertifikat fuer den Webserver der Firma Britzel
            X509v3 Basic Constraints:
              CA:FALSE
            X509v3 Key Usage:
              Digital Signature, Non Repudiation,
              Key Encipherment
            Netscape Cert Type:
              SSL Server
    Signature Algorithm: md5WithRSAEncryption
        3b:5d:ca:8a:01:14:e5:a4:7e:bb:12:e0:ff:7f:f6:7b:8f:5e:
        72:7d:eb:64:57:89:a1:97:2e:f8:58:ee:40:9e:7d:62:37:d5:
        1d:97:fb:43:70:37:26:24:09:15:59:50:2b:12:7b:ce:0f:e2:
        b5:d7:27:54:42:f0:c2:74:2e:14:5a:b2:5b:37:4c:cc:f7:4f:
        7e:95:b7:b1:04:20:f5:1b:d8:9e:f1:57:cd:b2:9c:ee:b4:5c:
        03:ff:36:0e:7c:60:ad:e2:a5:fa:96:c7:a1:f8:e0:61:5e:18:
        af:3f:ee:ee:0b:dd:2c:77:ce:40:15:34:b0:6c:a1:37:21:75:
        fc:8f
Certificate purposes:
SSL client : No
SSL client CA : No
SSL server : Yes
SSL server CA : No
Netscape SSL server : Yes
Netscape SSL server CA : No
```

```
S/MIME signing : No
S/MIME signing CA : No
S/MIME encryption : No
S/MIME encryption CA : No
CRL signing : No
CRL signing CA : No
Any Purpose : Yes
Any Purpose CA : Yes
OCSP helper : Yes
OCSP helper CA : No
```

Ein Zertifikat nach X.509 ist nach dem Schema Zertifikatsinhalt (Data), Signaturalgorithmus und Signatur aufgebaut.

- Version: Version des eingesetzten X.509-Standards. Üblicherweise heute Version 3.
- SerialNumber: Eine eindeutige Nummer des Zertifikats, die von der aussstellenden CA vergeben wird.
- Signature Algorithm: Algorithmus, mit dem der Signaturwert von der ausstellenden Instanz errechnet wurde. Dieser muss mit dem Signaturalgorithmus im Zertifikat übereinstimmen.
- Issuer: Die Zertifizierungsstelle, die die Authentizität der Person oder des Systems bestätigt.
- Validity: Gültigkeitszeitraum des Zertifikats.
- Subject: Informationen über die Person oder das System, für welche das Zertifikat erstellt wurde. Dabei enthält „C“ (Country) das Länderkürzel, „ST“ (State) das Bundesland, „O“ (Organisation) den Namen des Unternehmens oder der Einrichtung, „OU“ (Organisation Unit) die Abteilung und „CN“ (Common Name) den exakten Inhaber des Zertifikats. Für den Common Name wird üblicherweise bei einer Person die E-Mail-Adresse und bei einem Computersystem der FQDN eingesetzt. Nicht alle Felder müssen ausgefüllt sein, der CN sollte jedoch immer gesetzt sein.

- Subject Public Key Info: Der öffentliche Schlüssel. Der private Schlüssel ist in einem Serverzertifikat nicht enthalten.
- IssuerUniqueID: Ein optionaler, eindeutiger Identifikator des Zertifikatsausstellers, mit Version 2 eingeführt.
- SubjectUniqueID: Ein optionaler, eindeutiger Identifikator des Zertifikatsinhabers, mit Version 2 eingeführt.
- Extensions: Weitere Informationen, ab Version 3 nutzbar.

Im X.509-Standard ist ab Version 3 die Verwendung von Erweiterungen („Extensions“) definiert. Mit diesen lassen sich zusätzliche Informationen in einem Zertifikat abspeichern. Manche Erweiterungen sind im Standard festgelegt (etwa „KeyUsage“), es können aber auch private Erweiterungen definiert werden, die nur innerhalb einer bestimmten Nutzergruppe sinnvoll sind.

Folgende Erweiterungen gehören zum Standardumfang:

- AuthorityKeyIdentifier: Verfügt eine CA selbst über mehrere Zertifikate, gibt sie in diesem Feld an, mit welchem der Zertifikate das vorliegende signiert wurde. Dadurch kann zur Überprüfung der Prüfsumme der entsprechende Public Key der CA ausgewählt werden.
- SubjectKeyIdentifier: Falls der Inhaber des Zertifikats über mehrere Zertifikate verfügt, wird hier der genaue öffentliche Schlüssel angegeben. Handelt es sich beim Zertifikat um ein CA-Zertifikat, muss hier der Wert angegeben werden, den die CA beim Signieren ins Feld AuthorityKeyIdentifier schreibt. Bei Endbenutzerzertifikaten kann das Feld angegeben werden. Dies ist nützlich, falls das gleiche Ursprungszertifikat von mehreren CAs signiert wurde. Dann existieren mehrere Zertifikate mit gleichem Public Key, die über dieses Feld alle aufgefunden werden können.
- KeyUsage: Die Verwendung des Schlüssels kann hiermit beispielsweise nur auf die Überprüfung digitaler Signaturen oder zur verschlüsselten Datenübertragung eingeschränkt werden.

- ExtendedKeyUsage: Erweiterung zu „KeyUsage“, ist als Erweiterungsmöglichkeit für Einrichtungen gedacht, die weitere Einsatzzwecke zur Nutzung dieses öffentlichen Schlüssels angeben wollen.
- PrivateKeyUsagePeriod: Hiermit kann eine von der Gültigkeitsdauer des Zertifikats abweichende Gültigkeitsdauer für den privaten Schlüssel angegeben werden.
- CertificatePolicies: Gibt einen Indikator an, welcher auf die genauen Richtlinien verweist, unter deren Verwendung das Zertifikat erzeugt wurde. Die CA muss diese Richtlinien gesondert veröffentlichen. Es gibt auch die Möglichkeit, mit Verweis auf „any policy“ eine generische Richtlinie zu referenzieren. Dies wiederum kann über das Feld InhibitAnyPolicy auch gesperrt werden.
- PolicyMappings: Eine Auflistung von Zertifizierungsrichtlinien, die als gleichwertig zur verwendeten angesehen werden.
- SubjectAlternativeName: Hier können alternative Angaben über den Inhaber des Zertifikats gemacht werden. Bei einem Computersystem sind dies etwa weitere FQDNs oder die IP-Nummer.
- IssuerAlternativeName: Ein alternativer Name für die unterzeichnende CA. Hier wird oft eine Mailadresse angegeben.
- SubjectDirectoryAttributes: Weitere Angaben über den Zertifikatinhaber, etwa dessen Nationalität.
- BasicConstraints: Hier wird angegeben, ob das vorliegende Zertifikat selbst einen CA-Status hat, ob es also zum Signieren weiterer Zertifikate verwendet werden darf. Ist dies der Fall, kann zusätzlich der nachfolgende Zertifizierungspfad beschränkt werden.
- NameConstraints: Hiermit kann der Namespace, also etwa die im CN eingesetzten Domains, für nachfolgende Zertifikate beschränkt werden. Ein Unternehmen kann so etwa eine CA nur für die eigene Internetdomain betreiben.

- PolicyConstraints: Hier können Beschränkungen der Richtlinien für nachfolgende Zertifikate erwirkt werden.
- CrlDistributionPoints: Über dieses Feld wird angegeben, wo die Sperrlisten (CRLs) abgerufen werden können, die dieses Zertifikat für ungültig erklären können.
- FreshestCRL: Analog zu der Definition der Sperrlisten kann hier angegeben werden, wo die letzten Änderungen zu einer CRL abgerufen werden können.

6.1.3 Schlüssellänge

Die Sicherheit eines Schlüssels wird wesentlich durch die eingesetzte Schlüssellänge bestimmt. Bei einer Schlüssellänge von 2048 Bit werden Primzahlen von etwa 1024 Bit Länge benutzt. In diesem Bereich existieren etwa 10 hoch 305 verschiedene Primzahlen, mehr als es im gesamten Universum Atome gibt.

Man geht heute davon aus, dass Schlüssellängen von 2048 Bit bis etwa ins Jahre 2015 für Public-Key-Verfahren bei der Verwendung in Regierungseinrichtungen eine ausreichende Sicherheit gegen Angriffe bieten.

1024 Bit Schlüssellänge wurden im Jahre 2000 für Privatpersonen als ausreichend sicher angenommen. 1536 Bit gelten im Jahre 2006 als ausreichend für den Einsatz in Unternehmen.

Noch sicherer sind jeweils größere Schlüssellängen. Üblicherweise werden bis 4096 Bit unterstützt.

Bei symmetrischen Schlüsseln hingegen wird eine sichere Verschlüsselung ab ca. 100 Bit Schlüssellänge erreicht. Üblicherweise werden Schlüssellängen von 128 bis 256 Bit verwendet.

Der Faktor 10 in der Schlüssellänge gilt auch für den Aufwand zum (de-)chiffrieren. Auch mit immer leistungsfähigeren Computer-

systemen werden daher zum Austausch von Daten bevorzugt symmetrische Algorithmen wie AES eingesetzt. Asymmetrische Verfahren bieten hingegen eine höhere Sicherheit bezüglich des Schlüsselaustauschs. Sie werden daher eingesetzt, um beim Verbindungsbeginn eine gesicherte Übertragung aufzubauen. Dann wird ein zufällig generierter symmetrischer Schlüssel erzeugt und verschlüsselt zur Gegenseite übertragen. Dieser wird für die folgende Nutzdatenübertragung verwendet.

6.1.4 Laufzeit

Die Laufzeit jedes Zertifikats ist begrenzt. Üblicherweise werden Zertifikate mit einer Laufzeit von ein oder zwei Jahren erstellt. Diese Begrenzung sorgt im Fall des Verlusts eines Zertifikats für eine automatische Sperre nach Ablauf der Zeitspanne.

Bei einer CA sind alle abgeleiteten Zertifikate maximal so lange gültig wie die CA selbst. Hierbei sollte also eine längere Laufzeit (meist zehn Jahre) verwendet werden.

Zu beachten ist, dass Zertifikate nur für ein Zeitfenster gelten, also immer von einem Zeitpunkt bis zu einem anderen. Dies kann bei frisch erzeugten Zertifikaten auf zwei Systemen mit unterschiedlicher Uhrzeit zu Problemen führen.

6.1.5 Sperren eines Zertifikats

Es ist nie auszuschließen, dass ein vollständiger Schlüsselsatz aus Public und Private Key in falsche Hände gerät, etwa durch Diebstahl eines Notebooks. In diesem Fall muss der Inhaber des Schlüssels einen neuen Schlüsselsatz erstellen (lassen) und seinen

Public Key allen Kommunikationspartnern mitteilen. Der verlorene, kompromittierte Schlüssel existiert jedoch parallel weiter und scheint weiterhin gültig. Nach Ablauf der Laufzeit ist der kompromittierte Schlüssel irgendwann jedoch wertlos.

Bei der Nutzung einer CA bietet sich die Möglichkeit, einen kompromittierten Schlüssel noch vor Ablauf seiner eigentlichen Laufzeit zu sperren bzw. „zurückzuziehen". Dieser Vorgang kann ebenso wie die Signierung nur durch einen autorisierten Mitarbeiter der CA durchgeführt werden. Der zu sperrende Schlüssel wird widerrufen und in die sog. „Certificate Revocation List" CRL („Liste zurückgezogener Zertifikate") aufgenommen.

Problematisch dabei ist, dass jeder Teilnehmer unterhalb einer CA vor der Verwendung eines Schlüssels immer aktuell bei der CA anfragen muss, ob das zugehörige Zertifikat in der Sperrliste auftaucht. Auch wenn dies durch Software durchgeführt werden kann, geschieht es in der Praxis nur selten. Im V-Cube wird diese Überprüfung bei gleichzeitigem Einsatz als CA und als VPN-Einwahlpunkt immer durchgeführt.

6.1.6 Praktische Anwendung

Zertifikate können im V-Cube genutzt werden, um die Sicherheit von einigen Diensten im Internet zu verbessern. Das bekannteste Verfahren ist HTTPS zur verschlüsselten Übertragung von Webseiten. Damit dieses Verfahren angewendet werden kann, muss für den Webserver ein Zertifikat erstellt und eingebunden werden. Dies ist eine Voraussetzung zur Nutzung des User-Portal „Web-Access" im V-Cube.

Im E-Mail-Verkehr wird bei einigen Protokollen die Authentifizierung im Klartext übertragen (z. B. bei POP3). Mit Hilfe von

Verschlüsselung können diese Zugangsdaten sicher übermittelt werden. Auch hierfür muss für den Server ein Zertifikat erstellt und eingebunden werden. Solchen durch Verschlüsselung verbesserten Protokollen wird eine neue Bezeichnung zugewiesen (in diesem Beispiel POP3S). Achtung: Hier wird jeweils nur die Anmeldung am Server gesichert. Die E-Mail selbst wird weiter unverschlüsselt über das Internet übertragen.

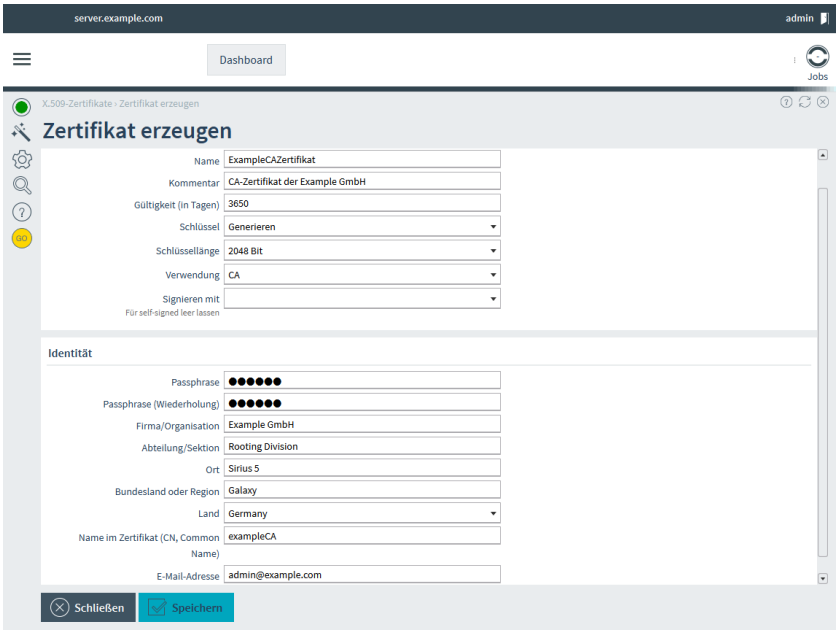
Natürlich lässt sich auch der Austausch von E-Mails zwischen zwei Personen durch Verschlüsselung schützen. Um den E-Mail-Verkehr zu verschlüsseln, müssen beide Beteiligte in ihrem Computer spezielle Software installieren (etwa PGP oder S/MIME), entsprechende Zertifikate für sich ausstellen lassen und die öffentlichen Schlüssel austauschen. Sie können dann Nachrichten verschicken. Hierbei wird der eigentliche Inhalt der E-Mail vor dem Versenden verschlüsselt und als „Buchstabensalat“ in einer normalen E-Mail übertragen. Die Mailserver, die die E-Mail übertragen, müssen also nicht speziell auf die Verschlüsselung abgestimmt werden. Virenscanner, die auf manchen Mailservern laufen, können jedoch den eigentlichen Inhalt der E-Mail ebenfalls nicht untersuchen. Der Inhalt kann erst auf dem Computer des Empfängers dechiffriert werden.

Für die sichere Datenübertragung zwischen zwei oder mehr Standorten über das Internet können VPN-Tunnel verwendet werden. In einem solchen Tunnel werden alle Daten durch Verschlüsselung gesichert. Über Zertifikate kann die Authentizität der Gegenstelle garantiert werden.

6.2 Schritt für Schritt: Erstellen eines Serverzertifikats

Um bestimmte Dienste durch Verschlüsselung abzusichern, muss für den V-Cube ein eigenes Zertifikat erzeugt werden. Dies geschieht in den *Benutzungsrichtlinien* unter *Zertifikate*. Hier können Zertifikate nach X.509-Standard und einfache RSA-Schlüssel verwaltet werden. Für die Serverdienste werden *X.509-Zertifikate* benötigt.

Zunächst wird eine eigene CA erstellt.

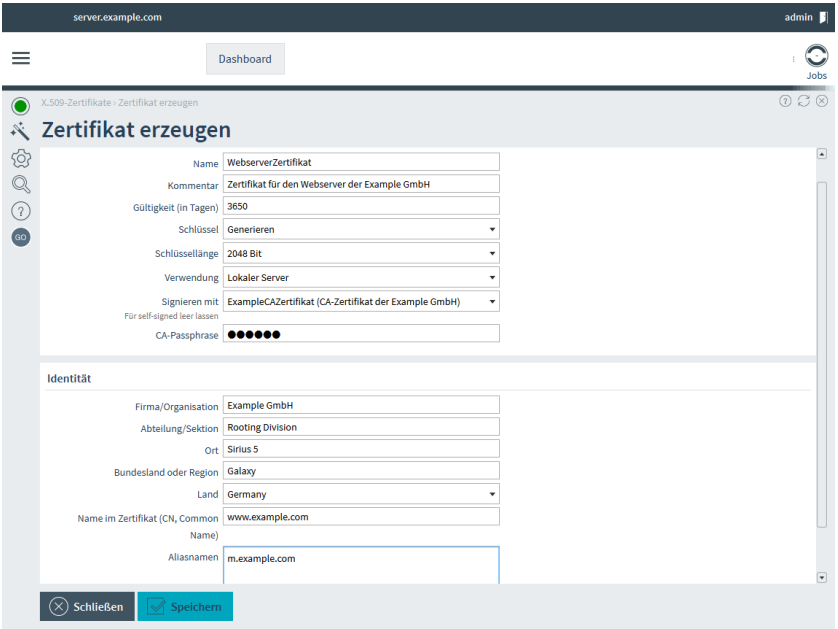


- Dazu wird mit *Zertifikat erstellen* ein Stammzertifikat erstellt. Mit diesem können dann weitere Zertifikate signiert werden.

- In den Feldern *Name* und *Kommentar* sollte ein möglichst sprechender Name eingegeben werden, da diese später nicht mehr geändert werden können.
- Unter *Gültigkeit* wird die Lebensdauer der CA festgelegt. Da alle mit dieser CA erzeugten Zertifikate maximal so lange wie die CA gültig sind, sollte hier eine ausreichene Zeitspanne gewählt werden.
- Wählen Sie unter *Verwendung* den Eintrag *CA* aus.
- Das CA-Zertifikat ist selbstsigniert (kein signierendes Zertifikat auswählen).
- Im Abschnitt *Identität* werden Informationen über den Inhaber des Zertifikats hinterlegt.
- Das unter *Passphrase* eingegebene Passwort sichert den privaten Schlüssel des Zertifikats. Es wird immer dann benötigt, wenn mit der CA signiert wird.

Nachdem das CA-Zertifikat erzeugt wurde, können mit diesem weitere Zertifikate signiert werden. Dazu wird jeweils ein neues Zertifikat angelegt.

- Wählen Sie unter *Verwendung* den Eintrag *lokaler Server* aus.
- Bei *Signieren mit* wird das erstellte CA-Zertifikat ausgewählt, dabei muss die hinterlegte *Passphrase* angegeben werden.
- Für den *Namen im Zertifikat* muss der FQDN eingetragen werden, sonst geben manche Clients später eine Fehlermeldung aus.



Ist das Zertifikat erzeugt, kann es in den Konfigurationsdialogen der jeweiligen Dienste zur Verschlüsselung ausgewählt werden, für den Webserver beispielsweise unter *Serverdienste – Webserver – Allgemein – Serverzertifikat*.

6.3 GUI-Referenz: *X.509-Zertifikate*

In diesen Dialogen werden im V-Cube Zertifikate nach dem X.509-Standard verwaltet. Es können neue Zertifikate erzeugt oder importiert werden. Ebenso ist der Aufbau und Betrieb einer Certificate Authority möglich.

6.3.1 *Vorhandene Zertifikate*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Zertifikate – X.509-Zertifikate*)

Hier sind alle Zertifikate aufgeführt, die auf diesem System erzeugt oder importiert wurden.

Unter *Zertifikate erstellen* können weitere Zertifikate hinzugefügt werden. Dabei können entweder neue Zertifikate generiert oder Zertifikate vom lokalen Rechner per Upload importiert werden.

Wenn ein eigenes CA-Zertifikat erzeugt wurde, werden alle von dieser CA signierten Zertifikate unterhalb des CA-Zertifikats angezeigt.

Bei einzelnen Zertifikaten aus der Liste besteht mit *Anzeigen* die Möglichkeit, das Zertifikat anzuzeigen, über einen Download zu exportieren und zu löschen.

Hinweis: Es ist nicht ausreichend, Zertifikate, die über eine CA erstellt wurden, zu löschen. Diese müssen vielmehr über *Anzeigen* zurückgezogen werden, damit sie ungültig werden. Werden CA-Zertifikate gelöscht, mit denen bereits Zertifikate signiert wurden, werden gleichzeitig die noch vorhandenen signierten Zertifikate gelöscht. Bei einem CA-Zertifikat kann zudem die Certificate Revocation List (CRL) exportiert werden.

6.3.1.1 Spalten in der Tabelle

- *Typ*: In dieser Spalte werden die Typen der Zertifikate angezeigt.
- *Key*: In dieser Spalte wird angezeigt ob der private Key im Zertifikat enthalten ist.
- *Gültig*: In dieser Spalte wird angezeigt ob das Zertifikat noch Gültig ist.
- *Name*: In dieser Spalte werden die Namen der Zertifikate angezeigt.
- *CA*: In dieser Spalte wird angezeigt mit welcher CA das Zertifikat signiert ist.
- *Gültigkeit (in Tagen)*: In dieser Spalte wird die Gültigkeit eines Zertifikates angezeigt.
- *Kommentar*: In dieser Spalte werden die Kommentare der Zertifikate angezeigt.

6.3.1.2 Aktionen für jeden Tabelleneintrag

- *Anzeigen*: Diese Aktion zeigt das Zertifikat in Textdarstellung an.
- *Zertifikat exportieren*: Mit dieser Aktion kann das Zertifikat über einen Download auf ein Computersystem exportiert werden. Dort kann es entweder direkt verwendet, archiviert oder weiter transferiert werden.
- *Zurückziehen*: Mit dieser Aktion wird ein Zertifikat zurückgezogen. Das Zertifikat wird gelöscht und in die CRL (Certificate Revocation List) für die CA eingetragen. Ab diesem Zeitpunkt ist das Zertifikat auf dem V-Cube gesperrt.

  Es können nur solche Zertifikate zurückgezogen werden, die mit einer lokalen CA signiert wurden. Dies sind nur die Zertifikate, die auf diesem System erzeugt wurden.

- *CRL*: Bei einem CA-Zertifikat selbst kann mit dieser Aktion die Certificate Revocation List (CRL) über einen Download auf das zur Administration genutzte System exportiert werden. Zudem bietet diese Aktion die Möglichkeit, eine CRL zu erzeugen.
- *Löschen*: Mit dieser Aktion wird das Zertifikat gelöscht. Es können jedoch keine Zertifikate gelöscht werden, die von einer CA signiert wurden.

  Hinweis: Zum Sperren eines Zertifikats, das über eine CA erzeugt wurde, muss dieses Zertifikat *zurückgezogen* werden.

6.3.1.3 Aktionen für diesen Dialog

- *Zertifikat importieren*: Mit dieser Aktion kann ein Zertifikat auf das System importiert werden. Das Zertifikat kann dabei nur aus einem Public Key bestehen, aber auch ein vollständiges Zertifikat bilden.
- *Zertifikat erstellen*: Mit dieser Aktion wird ein neues Zertifikat angelegt. Dazu öffnet sich ein neuer Dialog, über den die Informationen über den Zertifikatsinhaber abgefragt werden.

6.3.2 *Zertifikat anzeigen*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Zertifikate – X.509-Zertifikate*)

In diesem Dialog wird der Inhalt des Zertifikats angezeigt.

6.3.2.1 Tab *Zertifikat*
Felder in diesem Abschnitt

- *Name des Zertifikats*: Hier wird der Name angezeigt, unter dem das Zertifikat im V-Cube abgelegt ist. Dabei handelt es sich meist nicht um den Common Name, der im Zertifikat selbst gespeichert ist.
- *Inhalt*: Hier wird der Inhalt des Zertifikats angezeigt. Dabei wird die X.509-Textdarstellung verwendet.

6.3.2.2 RSA Public Key

- *RSA Public Key (HEX):* In diesem Textfeld wird der Public Key im RSA-Format in hexadezimaler Schreibweise angezeigt. Er kann hier markiert und über die Zwischenablage gespeichert werden.
- *RSA Public Key (Base64):* In diesem Textfeld wird der Public Key im RSA-Format in Base64-Kodierung angezeigt. Er kann hier markiert und über die Zwischenablage gespeichert werden.

6.3.3 *Zertifikat erzeugen*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Zertifikate – X.509-Zertifikate*)

In diesem Dialog wird ein neues Zertifikat erstellt. Solch ein Zertifikat kann verwendet werden, um verschiedenen Diensten auf dem System die Möglichkeit zur Verschlüsselung zu geben.

Je nach der Art der Anwendung kann es sinnvoll sein, ein Zertifikat zu installieren, welches von einer offiziellen CA signiert wurde (etwa

beim Einsatz eines offiziellen Webservers mit Verschlüsselung). Außenstehende Personen werden selbst erzeugten Zertifikaten meist nicht vertrauen. Innerhalb der eigenen Organisation können selbst erstellte Zertifikate jedoch problemlos verwendet werden (etwa für eine sichere Anmeldung am eigenen Mailserver).

Wenn eigene Zertifikate erstellt werden, ist es meist sinnvoll, zunächst ein eigenes CA-Zertifikat anzulegen. Mit diesem werden dann die weiteren Zertifikate für die einzelnen Dienste oder Mitarbeiter signiert.

6.3.3.1 Abschnitt *Zertifikat erzeugen*
Felder in diesem Abschnitt

- *Name des Zertifikats*: Unter diesem Namen wird das Zertifikat im System abgelegt. Er dient dazu, das Zertifikat in der Administrationsoberfläche aufzufinden. Der Name wird nicht in die Inhaberinformation im Zertifikat aufgenommen. Es sollte ein möglichst aussagekräftiger Name für den späteren Einsatzzweck des Zertifikats gewählt werden.
- *Ausgabe*: In diesem Fenster werden während der späteren Erzeugung die Ausgaben der beteiligten Programme angezeigt. Ansonsten ist das Fenster nicht sichtbar.
- *Kommentar*: Mit diesem Kommentartext kann das Zertifikat genauer beschrieben werden. Der Inhalt dieses Feldes wird auch als Kommentar in das Zertifikat kopiert und ist für jeden sichtbar.
- *Gültigkeit (in Tagen)*: Jedes Zertifikat hat eine begrenzte Gültigkeitsdauer und kann danach nicht mehr benutzt werden. In diesem Feld wird diese Dauer in Tagen ab heute angegeben.

  Für ein CA-Zertifikat sollte ein langer Zeitraum gewählt werden (z. B. 5 Jahre), da nach Ablauf des CA-Zertifikats auch alle damit signierten Zertifikate ungültig werden.

- *Schlüssel*: Hier kann gewählt werden, ob ein neues Schlüsselpaar für das Zertifikat generiert oder ein vorhandener Schlüsselsatz in das Zertifikat importiert werden soll.
- *Schlüssellänge*: Die gewünschte Schlüssellänge wird hier vorgegeben. Die Sicherheit des Schlüssels ist von seiner Länge abhängig. Es ist ratsam, möglichst lange Schlüssel zu verwenden. Schlüssel mit weniger als 1024 Bit gelten als unsicher. 1024-Bit-Schlüssel sind möglicherweise ebenfalls nicht mehr sicher, allerdings können manche Clients nicht mit längeren Schlüsseln umgehen.

  Wird ein CA-Zertifikat erzeugt, sollte ein möglichst langer Schlüssel verwendet werden.
- *Datei*: Hier kann der zu importierende Schlüssel ausgewählt und hochgeladen werden. Momentan werden hier nur „ipsec.secrets"-Dateien von *FreeSWAN* aus Kompatibilitätsgründen akzeptiert.

  Im Normalfall wird ein neuer Schlüssel erzeugt. Diese Importfunktion wird nur in besonderen Fällen benötigt.
- *Verwendung*: Hier wird der Verwendungszweck für den Schlüssel gewählt. Wenn ein CA-Schlüssel erzeugt werden soll, muss hier *CA* gewählt werden. In den meisten anderen Fällen wird *lokaler Server* eingestellt. Das Feld kann auch leer bleiben, dann wird ein Schlüssel mit einem breiten Verwendungsspektrum erzeugt.
- *Signieren mit*: Hier muss das Zertifikat der CA ausgewählt werden, mit der das neue Zertifikat signiert werden soll. Wird ein neues CA-Zertifikat erzeugt, braucht kein weiteres Zertifikat ausgewählt werden. Das neue CA-Zertifikat signiert sich dann selbst. Dies ist grundsätzlich auch für einfache Zertifikate möglich.
- *CA-Passphrase*: Um zum Signieren den privaten Schlüssel des CA-Zertifikats nutzen zu können, muss hier die Passphrase der CA angegeben werden.

6.3.3.2 Abschnitt *Identität*

In diesem Abschnitt werden Angaben zur Identität des Inhabers für das Zertifikat gemacht.

Felder in diesem Abschnitt

- *Passphrase*: Hier kann eine Passphrase angegeben werden, mit der der private Schlüssel des Zertifikats gesichert wird. Dies ist nützlich, wenn ein Clientzertifikat erzeugt wird, bei dessen späterer Benutzung jedes Mal die Passphrase abgefragt werden soll.

  Für Serverzertifikate, die für Dienste auf diesem System verwendet werden sollen, darf keine Passphrase gesetzt werden. Die Passphrase würde beim Start der Netzwerkdienste auf der Systemkonsole abgefragt und der Startvorgang des Systems bis zur Eingabe unterbrochen werden. Bei der Erstellung eines Zertifikats für *lokale Server* ist das Feld daher auch nicht sichtbar.

  Die Passphrase wird nicht im System gespeichert. Sie wird immer wieder benötigt, wenn der private Schlüssel des Zertifikats benutzt werden soll. Bei einem CA-Zertifikat ist dies etwa beim Signieren oder Sperren weiterer Zertifikate der Fall.
- *Passphrase (Wiederholung)*: Um zu verhindern, dass eine dritte Person die Eingabe der Passphrase mitlesen kann, wird diese nicht im Klartext angezeigt. Um Fehleingaben zu vermeiden, muss sie daher ein zweites Mal eingegeben werden.
- *Firma/Organisation*: Hier wird der Name der Organisation oder der Firma angegeben, für die das Zertifikat ausgestellt werden soll.

  Hinweis: Da Zertifikate international eingesetzt werden, sollten in den folgenden Textfeldern keine Umlaute und andere

Sonderzeichen aus speziellen Zeichensätzen verwendet werden.

- *Abteilung/Sektion*: Hier kann innerhalb der Einrichtung genauer spezifiziert werden, für welche Abteilung oder Sektion das Zertifikat erzeugt wird.
- *Ort*: Hier wird der Ort angegeben, an dem das Unternehmen bzw. die Organisation den Sitz hat.
- *Bundesland oder Region*: Hier wird das Bundesland oder die Provinz innerhalb des Landes angegeben.
- *Land*: Hier wird das Land ausgewählt.
- *Name im Zertifikat (CN, Common Name)*: Hier wird der Name der Person oder des Systems angegeben, für die das Zertifikat erzeugt werden soll. Diese Name muss eindeutig den Inhaber des Zertifikats beschreiben. Bei E-Mail-Zertifikaten sollte der Name oder die Mailadresse der Person, auf die das Zertifikat ausgestellt wird, benutzt werden. Bei Serverzertifikaten empfiehlt sich die Angabe des FQDNs des Rechners.

  Wird ein Zertifikat für einen Webserver erstellt, sollte hier der exakte FQDN verwendet werden, unter dem das System später von außen angesprochen wird. Manche Webbrowser nehmen eine Überprüfung vor, ob der Zertifikatsname mit dem Servernamen identisch ist.
- *Mail-Alias*: Wird ein Zertifikat für einen Benutzer angelegt, sollte hier die E-Mail-Adresse dieses Benutzers angeben werden.
- *Aliasnamen*: Wird ein Serverzertifikat erzeugt, können hier zusätzliche Namen angegeben werden, unter denen der Server erreichbar ist.
- *E-Mail-Adresse*: Hier wird die E-Mail-Adresse angegeben, die zur CA gehört, z. B. die Adresse des Administrators.

6.3.3.3 Aktionen für diesen Dialog

- *Erzeugen*: Diese Aktion startet die Erzeugung des Zertifikats.

6.3.4 *Zertifikat exportieren*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Zertifikate – X.509-Zertifikate*)

Damit Zertifikate auch für Clients oder VPN-Verbindungen genutzt werden können, müssen sie vom V-Cube heruntergeladen werden. Dazu stehen verschiedene Exportformate zur Verfügung.

6.3.4.1 Felder in diesem Dialog

- *Zertifikat*: In diesem Feld wird der Name des Zertifikats angezeigt.
- *Format*: Hier wird das Format gewählt, in dem das Zertifikat gespeichert wird. Welches Format benötigt wird, richtet sich danach, welche Formate die Gegenseite bzw. der Client einlesen können. In den Formaten PEM, PKCS12 und DER wird der private Schlüssel des Zertifikats exportiert.

  PEM ist ein Base64-kodiertes Standardformat zum Zertifikatsaustausch mit anderen Linux-/Unix-Servern. Wird dieses Format gewählt, kann noch festgelegt werden, ob der private Schlüssel mit exportiert wird oder nicht. Der private Schlüssel der eigenen Zertifikate darf unter keinen Umständen an andere Personen weitergegeben werden.

  Das gepackte Zertifikat enthält auch den Public Key der CA, die das Zertifikat signiert hat. Nicht alle VPN-Produkte können eine solche Kombination einlesen. In diesem Fall muss der CA-

Schlüssel getrennt exportiert und auf der Gegenseite eingelesen werden.

PKCS12-Zertifikate werden von einigen Webbrowsern und Mailprogrammen verwendet (Netscape/Mozilla, Internet Explorer, Outlook). Dieses Format kann nur gewählt werden, wenn ein privater Schlüssel zum Zertifikat existiert. Der private Schlüssel wird in jedem Fall mit exportiert. Der private Schlüssel der eigenen Zertifikate darf unter keinen Umständen an andere Personen weitergegeben werden.

In diesem Format kann auf die Exportdatei eine Passphrase gelegt werden. Nur mit der Kenntnis dieser Passphrase kann das Zertifikat auf einem anderen System eingelesen bzw. verwendet werden.

DER-Zertifikate werden von einigen PDAs verwendet, um gesicherte Verbindungen aufzubauen. In einer DER-Datei können private Keys, Public Keys oder Zertifikate enthalten sein. DER-Zertifikate stellen das Standard-Format für die meisten Web-Browser dar.

- *Mit privatem Schlüssel*: Ist diese Option aktiviert, wird der private Schlüssel mit in den Export aufgenommen.

  Die Option steht zur Verfügung, wenn das Zertifikat im *PEM*- oder im *DER*-Format exportiert wird.

  Diese Option sollte nur dann aktiviert werden, wenn ein Clientzertifikat auf diesem System erzeugt wurde und dieses nun für den Client exportiert werden soll.
- *CA-Zertifikat*: Ist das Zertifikat von einer CA signiert worden, ist es sinnvoll, das CA-Zertifikat zusätzlich mit in die exportierte Datei aufzunehmen. Über dieses CA-Zertifikat wird das eigentliche Zertifikat gültig erklärt (vorausgesetzt, dem CA-Zertifikat wird vertraut).
- *Passphrase*: Ist der private Schlüssel des Zertifikats mit einer Pas-

sphrase gesichert, muss hier zum Exportieren diese Passphrase angeben werden.

- *Exportpasswort*: Wird ein Zertifikat im PKCS#12-Format exportiert, muss hier ein Passwort angegeben werden. Mit diesem wird die Exportdatei verschlüsselt. Das Passwort wird später beim Importieren des Zertifikats auf den Client wieder benötigt.
- *Exportpasswort (Wiederholung)*: Da das Exportpasswort bei der Eingabe aus Sicherheitsgründen nicht sichtbar ist, muss es hier zur Sicherheit nochmals eingegeben werden.

6.3.4.2 Aktionen für diesen Dialog

- *Download*: Mit dieser Aktion wird der Download des Zertifikats gestartet. Nach kurzer Zeit sollte im Browser ein *Speichern-unter*-Dialog geöffnet werden. Ist dies nicht der Fall, wurde im Browser eventuell eine automatische Speicherung in ein bestimmtes Verzeichnis aktiviert.

6.3.5 *Zertifikat importieren*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Zertifikate – X.509-Zertifikate*)

Über diesen Dialog kann ein Zertifikat auf das System importiert werden.

Ein Zertifikat besteht in der Regel aus drei Teilen: Dem von der CA signierten öffentlichen Schlüssel, dem privaten Schlüssel und dem Zertifikat der CA. Nicht alle drei Teile sind immer notwendig.

Manche Dateiformate für Zertifikate (PKCS#12 und PEM) können alle drei Teile in einer Datei enthalten. Liegt das Zertifikat aber nur

im DER-Format vor, müssen die einzelnen Teile separat angegeben werden.

Das Zertifikat einer CA muss nur einmal auf dem System installiert werden. Wurde bereits ein Zertifikat installiert, das von der gleichen CA unterschrieben wurde, muss das CA-Zertifikat nicht nochmals installiert werden.

Der private Schlüssel zum Zertifikat wird nur dann benötigt, wenn das Zertifikat für das System selbst verwendet werden soll, etwa für einen Serverdienst oder als VPN-Endpunkt. In allen anderen Fällen muss der private Schlüssel nicht auf dem System installiert werden.

6.3.5.1 Felder in diesem Dialog

- *Name für das Zertifikat*: Unter diesem Namen wird das Zertifikat im System abgelegt. Er dient dazu, das Zertifikat in der Administrationsoberfläche aufzufinden. Der Name muss nicht mit den Inhaberinformationen im Zertifikat identisch sein. Es sollte jedoch ein möglichst aussagekräftiger Name für den Einsatzzweck des Zertifikats gewählt werden.
- *Kommentar*: In diesem Kommentartext kann eine ausführlichere Information zum Zertifikat angegeben werden.
- *Ausgabe*: Während des Imports erscheint ein Fenster mit der Ausgabe des Installationsprozesses.
- *Passwort*: PKCS#12-Zertifikate und der private Schlüssel in PEM-Zertifikaten sind meist während des Transports mit einem Passwort geschützt. Dieses muss hier eingegeben werden, um auf das Zertifikat zugreifen zu können.
- *Zertifikat*: Mit diesem Dialog kann die Datei mit dem Zertifikat auf dem Computer ausgewählt werden, von dem aus gerade die Administration erfolgt.

- *Privater Schlüssel*: Wird das Zertifikat für einen Serverdienst oder für ein VPN verwendet, kann hier eine Datei ausgewählt werden, die den privaten Schlüssel für das Zertifikat enthält.

  Ist das Zertifikat im PKCS#12-Format oder als kombiniertes PEM-Zertifikat gespeichert, bleibt dieses Feld leer.
- *CA-Zertifikat*: Hier wird die Datei mit dem Zertifikat der CA ausgewählt, die das zu installierende Zertifikat unterschrieben hat.

  Dieses Feld bleibt leer, wenn das CA-Zertifikat bereits installiert wurde oder wenn das Zertifikat in einem Format vorliegt, das diese Information bereits enthält (PKCS12 oder kombiniertes PEM).

6.3.5.2 Aktionen für diesen Dialog

- *Upload*: Mit dieser Aktion wird der Import des Zertifikats gestartet. Nach erfolgreichem Import sollte das Zertifikat unter dem beim Import angegebenen Namen in der Zertifikatsübersicht aufgeführt sein.

6.3.6 *Zertifikat zurückziehen*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Zertifikate – X.509-Zertifikate*)

In diesem Dialog kann ein Zertifikat zurückgezogen werden. Dieses Sperren ist nur für Zertifikate möglich, die von einer auf dem System betriebenen CA signiert wurden. Die Sperre kann nicht wieder aufgehoben werden. In diesem Fall muss ein neues Zertifikat erstellt werden.

Die Laufzeit eines Zertifikats wird normalerweise bei seiner Erzeu-

gung festgelegt. Wird ein CA-signiertes Zertifikat zur Authentifizierung (z. B. für VPN-Einwahl) benutzt, ist es nicht ausreichend, das Zertifikat zu löschen. Über die CA-Signatur und seine Restlaufzeit ist es weiterhin gültig.

Um Zertifikate vor Ablauf des Verfallsdatums für ungültig zu erklären, werden diese in eine Liste (die Certificate Revocation List CRL) eingetragen. Dienste, die mit Zertifikaten arbeiten, können in dieser Liste abfragen, ob ein Zertifikat für ungültig erklärt wurde.

6.3.6.1 Felder in diesem Dialog

- *Name für das Zertifikat*: Hier wird der Name des Zertifikats angezeigt, das gesperrt werden soll.
- *Kommentar*: Hier wird der Kommentartext angezeigt, der beim Erstellen oder Importieren des Zertifikats angegeben wurde.
- *CA-Passwort*: Um das Zertifikat zurückzuziehen, muss das Passwort der CA angegeben werden. Es muss die CA verwendet werden, mit der das Zertifikat bei der Erstellung signiert wurde.

  Das Feld wird nur dann angezeigt, wenn für die Verwendung des privaten Schlüssels der CA ein Passwort benötigt wird.
- *Log*: Während des Vorgangs erscheint ein Fenster mit der Ausgabe der aufgerufenen Programme.

6.3.6.2 Aktionen für diesen Dialog

- *Zurückziehen*: Hiermit wird der Sperrvorgang ausgelöst. Das Zertifikat wird widerrufen und danach gelöscht.

6.3.7 *CRL verwalten*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Zertifikate – X.509-Zertifikate*)

Eine CRL (Certificate Revocation List) ist eine Sperrliste von Zertifikaten, die von einer CA unterschrieben wurden, aber vor Ende der Laufzeit zurückgezogen wurden.

Für eine CA, die auf diesem System verwaltet wird, kann die CRL mit diesem Dialog erzeugt werden. Die CRL wird dann von allen lokalen Diensten automatisch verwendet. Diese CRL kann exportiert werden.

Wird auf einem anderen System eine CA betrieben, von der auf dem lokalen System Zertifikate eingesetzt werden, kann die CRL auf dem anderen System exportiert und ins lokale System importiert werden. Dieser Vorgang sollte spätestens nach jeder Sperrung eines Zertifikats durchgeführt werden.

6.3.7.1 Felder in diesem Dialog

- *Name der CA*: Hier wird der Name der CA angezeigt, für die die CRL verwaltet wird.
- *Kommentar*: Hier wird der Kommentartext angezeigt, der beim Erstellen oder Importieren der CA angegeben wurde.
- *CA-Passwort*: Um ein Zertifikat zurückzuziehen, muss das Passwort der CA angegeben werden. Dabei handelt es sich um die CA, die das Zertifikat ausgestellt hat.

  Dieses Feld wird nur dann angezeigt, wenn für die lokale CA ein Passwort benötigt wird.
- *Datei*: Wird eine CA auf einem anderen System verwaltet, kann die CRL der CA über dieses Feld in dieses System importiert

werden. Zertifikate können nur auf dem System mit der CA gesperrt werden. Um andere Systeme über diese Sperrungen zu informieren, muss die CRL exportiert und auf den beteiligten Systemen importiert werden.

- *Log*: Während des Vorgangs erscheint ein Fenster mit der Ausgabe der aufgerufenen Programme.

6.3.7.2 Aktionen für diesen Dialog

- *CRL erstellen*: Mit dieser Aktion wird die CRL erstellt.
- *Importieren*: Mit dieser Aktion wird der Upload der CRL gestartet.
- *Exportieren*: Mit dieser Aktion wird der Download der CRL gestartet. Nach kurzer Zeit sollte im Browser ein *Speichern-unter*-Dialog geöffnet werden. Ist dies nicht der Fall, wurde im Browser eventuell eine automatische Speicherung in ein bestimmtes Verzeichnis aktiviert.

6.4 GUI-Referenz: *Certificate Signing Requests (CSR)*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Zertifikate – Certificate Signing Requests*

6.4.1 *Certificate Signing Request wählen*

6.4.1.1 Spalten in der Tabelle

- *Name*: Hier wird der Name eines erstellten CSR angezeigt.
- *Distinguished Name (DN)*: Zeigt den DN des erstellten CSR an.

6.4.1.2 Aktionen für jeden Tabelleneintrag

- *Anzeigen*: Mit dieser Aktion werden Details des CSR angezeigt.
- *Löschen*: Mit dieser Aktion kann das gewählte CSR gelöscht werden.
- *Exportieren*: Durch diese Aktion öffnet sich ein Dialog, um das CSR zu exportieren.

6.4.1.3 Aktionen für dieses Formular

- *CSR erstellen*: Mit dieser Aktion kann ein neuer CSR erstellt werden.

6.4.2 GUI-Referenz: *CSR erzeugen*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Zertifikate – Certificate Signing Requests*)

6.4.2.1 Abschnitt *CSR erzeugen* Felder in diesem Abschnitt

- *Name des Zertifikats*: Unter diesem Namen wird das Zertifikat im System abgelegt. Er dient dazu, das Zertifikat in der Administrationsoberfläche aufzufinden. Der Name muss nicht mit den Inhaberinformationen im Zertifikat identisch sein. Es sollte jedoch ein möglichst aussagekräftiger Name für den Einsatzzweck des Zertifikats gewählt werden.
- *Kommentar*: In diesem Kommentartext kann eine ausführlichere Information zum Zertifikat angegeben werden.
- *Schlüssellänge*: Die gewünschte Schlüssellänge wird hier vorgegeben. Die Sicherheit des Schlüssels ist von seiner Länge abhängig. Es ist ratsam, möglichst lange Schlüssel zu verwenden. Schlüssel mit weniger als 1024 Bit gelten als unsicher. 1024-Bit-Schlüssel sind möglicherweise ebenfalls nicht mehr sicher, allerdings können manche Clients nicht mit längeren Schlüsseln umgehen.

  Wird ein CA-Zertifikat erzeugt, sollte ein möglichst langer Schlüssel verwendet werden.
- *Verwendung*: Hier wird der Verwendungszweck für den Schlüssel gewählt. Wenn ein CA-Schlüssel erzeugt werden soll, muss hier *CA* gewählt werden. In den meisten anderen Fällen wird *lokaler Server* eingestellt. Das Feld kann auch leer bleiben, dann wird ein Schlüssel mit einem breiten Verwendungsspektrum erzeugt.
- *Ausgabe*: Während des Imports erscheint ein Fenster mit der Ausgabe des Installationsprozesses.

6.4.2.2 Abschnitt *Identität*
Felder in diesem Abschnitt

- *Passphrase (privater Schlüssel)*: Hier kann eine Passphrase angegeben werden, mit der der private Schlüssel des Zertifikats gesichert wird. Dies ist nützlich, wenn ein Clientzertifikat erzeugt wird, bei dessen späterer Benutzung jedes Mal die Passphrase abgefragt werden soll.

  Für Serverzertifikate, die für Dienste auf diesem System verwendet werden sollen, darf keine Passphrase gesetzt werden. Die Passphrase würde beim Start der Netzwerkdienste auf der Systemkonsole abgefragt und der Startvorgang des Systems bis zur Eingabe unterbrochen werden. Bei der Erstellung eines Zertifikats für *lokale Server* ist das Feld daher auch nicht sichtbar.

  Die Passphrase wird nicht im System gespeichert. Sie wird immer wieder benötigt, wenn der private Schlüssel des Zertifikats benutzt werden soll. Bei einem CA-Zertifikat ist dies etwa beim Signieren oder Sperren weiterer Zertifikate der Fall.
- *Passphrase (Wiederholung)*: Um zu verhindern, dass eine dritte Person die Eingabe der Passphrase mitlesen kann, wird diese nicht im Klartext angezeigt. Um Fehleingaben zu vermeiden, muss sie daher ein zweites Mal eingegeben werden.
- *Firma/Organisation*: Hier wird der Name der Organisation oder der Firma angegeben, für die das Zertifikat ausgestellt werden soll.

  Hinweis: Da Zertifikate international eingesetzt werden, sollten in den folgenden Textfeldern keine Umlaute und andere Sonderzeichen aus speziellen Zeichensätzen verwendet werden.
- *Abteilung/Sektion*: Hier kann innerhalb der Einrichtung genauer spezifiziert werden, für welche Abteilung oder Sektion das Zertifikat erzeugt wird.

- *Ort*: Hier wird der Ort angegeben, an dem das Unternehmen bzw. die Organisation den Sitz hat.
- *Bundesland oder Region*: Hier wird das Bundesland oder die Provinz innerhalb des Landes angegeben.
- *Land*: Hier wird das Land ausgewählt.
- *Name im Zertifikat (CN, Common Name)*: Hier wird der Name der Person oder des Systems angegeben, für die das Zertifikat erzeugt werden soll. Diese Name muss eindeutig den Inhaber des Zertifikats beschreiben. Bei E-Mail-Zertifikaten sollte der Name oder die Mailadresse der Person, auf die das Zertifikat ausgestellt wird, benutzt werden. Bei Serverzertifikaten empfiehlt sich die Angabe des FQDNs des Rechners.

  Wird ein Zertifikat für einen Webserver erstellt, sollte hier der exakte FQDN verwendet werden, unter dem das System später von außen angesprochen wird. Manche Webbrowser nehmen eine Überprüfung vor, ob der Zertifikatsname mit dem Servernamen identisch ist.
- *Mail-Alias*: Wird ein Zertifikat für einen Benutzer angelegt, sollte hier die E-Mail-Adresse dieses Benutzers angeben werden.
- *Aliasnamen*: Wird ein Serverzertifikat erzeugt, können hier zusätzliche Namen angegeben werden, unter denen der Server erreichbar ist.
- *E-Mail-Adresse*: Hier wird die E-Mail-Adresse angegeben, die zur CA gehört, z. B. die Adresse des Administrators.

6.4.2.3 Abschnitt *Extra Attribute*

Felder in diesem Abschnitt

- *Optionaler Firmenname*: Hier kann ein optionaler Firmenname angegeben werden. Erkundigen Sie sich jedoch vorher bei Ihrer Zertifizierungsstelle, ob diese Angabe möglich ist.

- *Challenge Passwort (CSR)*: Hier kann ein optionales Challenge Passwort angegeben werden. Erkundigen Sie sich jedoch vorher bei Ihrer Zertifizierungsstelle, ob diese Angabe möglich ist.

6.4.2.4 Aktionen für dieses Formular

- *Zurück*: Diese Aktion führt zurück in die Zertifikatsübersicht.
- *Erzeugen*: Diese Aktion startet die Erzeugung des Zertifikats.

6.4.3 GUI-Referenz: *CSR anzeigen*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Zertifikate – Certificate Signing Requests*)

6.4.3.1 Tab *CSR Information*
Felder in diesem Abschnitt

- *Name des CSR*: Hier wird der Name des CSR angezeigt.
- *Inhalt*: Hier wird der Inhalt des CSR angezeigt. Dabei wird die X.509-Textdarstellung verwendet.

6.4.3.2 Tab *CSR*
Felder in diesem Abschnitt

- *CSR-Quelltext*: Hier wird der Quelltext des CSR angezeigt.

6.4.3.3 Aktionen für dieses Formular

- *Zurück*: Diese Aktion führt zurück in die Zertifikatsübersicht.
- *Download*: Mit dieser Aktion können Sie den CSR herunterladen.

7 Netzwerke

7.1 Einführung

Computer müssen ein gemeinsames Protokoll verwenden, um miteinander kommunizieren zu können. In der Vergangenheit kamen verschiedene, teils herstellerspezifische Protokolle zum Einsatz. Heutzutage setzt der Großteil der Systeme auf TCP/IP.

Grundlage ist das „Internet Protocol“ IP, auf dem weitere Protokolle basieren. Jedes dieser weiteren Protokolle ist für bestimmte Daten besonders geeignet. Eines dieser Protokolle ist das „Transmission Control Protocol“ TCP. Es ist so bedeutend, dass seine Abkürzung mit zur offiziellen Bezeichnung der Protokollfamilie TCP/IP beiträgt.

7.1.1 Adressierung von Computersystemen

Zur Kommunikation im Internet erhält jedes System eine 32 Bit breite „IP-Nummer“ als Adresse. Als übliche Schreibweise hat sich die Aufteilung in vier Oktette in dezimaler Darstellung durchgesetzt, z. B. 192.168.9.9. Diese Schreibweise wird auch als „Dotted Decimal Notation“ bezeichnet.

Diese IP-Adresse stammt aus dem Adressbereich von Version 4 des IP-Protokolls („IPv4“). Insgesamt lassen sich damit etwa 4 Milliarden unterschiedliche Adressen bilden. In diesem Handbuch ist immer IPv4 gemeint, wenn nicht ausdrücklich etwas anderes angegeben wird (wie im Folgenden Absatz).

Für die Zukunft ist IPv4 nicht ausreichend, da immer mehr Geräte eine IP-Adresse benötigen und die vorhandenen IP-Adressen etwas

ungleich verteilt sind (in Asien besteht großer Bedarf, aber die Mehrheit der IP-Adressen sind Europa und Nordamerika zugeordnet). Daher steht als Nachfolger bereits Version 6 („IPv6“) bereit, hier werden Adressen einer Größe von 128 Bit verwendet. Daraus ergeben sich Billiarden von IP-Nummern pro Quadratmillimeter Erdoberfläche, was nach heutigem Ermessen eine ganze Zeit ausreichen wird.

7.1.2 Adressierung von Computerdiensten

Auf einem Computersystem laufen unterschiedliche Programme, meist als eigenständige Prozesse, etwa Webserver, POP3-Server, IMAP-Server usw. Über die IP-Adresse wird das System selbst angesprochen. Die Zuordnung auf die einzelnen Dienste erfolgt über die Angabe einer Portadresse. Dabei handelt es sich um eine 16-Bit-Adresse, hinter der ein Dienst oder eine Applikation Verbindungen annimmt. Sie stellt bildlich betrachtet die Zimmernummer in dem großen Computerhaus dar. Dabei werden die Portnummern bis 1024 weitgehend für Systemdienste genutzt.

Die Portadresse muss entweder vor dem Verbindungsaufbau abgesprochen werden, oder es wird eine festgelegte Nummer verwendet, etwa Port 80 für HTTP/Webserver. Die Liste der offiziell zugewiesenen Portnummern wird von der „Internet Assigned Numbers Authority“ (IANA) verwaltet.

Die Portadresse des Absenders (in diesem Beispiel des Webbrowsers) wird vom Betriebssystem im Moment des Verbindungsaufbaus zufällig vergeben.

Gängige Portnummern

Dienst	Protokoll	Port
Webadmin	TCP	8001
DNS	UDP und TCP	53
HTTP-Webserver	TCP	80
HTTPS-Webserver	TCP	443
HylaFax-Dienst	TCP	4559
MySQL-Dienst	TCP	3306
Squid-Webproxy	TCP	3128
SMTP-Mailserver	TCP	25
POP3-Mailserver	TCP	110
POP3S-Mailserver	TCP	995
SSH	TCP	22

7.1.3 Protokolle

Für den Austausch von Daten über IP sind verschiedene Unterprotokolle definiert. ICMP („Internet Control Message Protocol“) ist ein Protokoll zum Betrieb des eigentlichen Netzwerkes. Computer tauschen darüber Informationen über Laufzeiten und Erreichbarkeitsprobleme im Netz aus.

Eines der einfachsten Protokolle zur Nutzdatenübertragung ist das „User Datagram Protocol“ UDP. Neben Absender- und Ziel-IP-Adresse werden die Nutzdaten, die Absender- und Zielportadresse sowie eine optionale Prüfsumme in einem Datenpaket übertragen. Es gibt keinerlei Rückmeldung, ob ein UDP-Paket beim Empfänger angekommen ist; es könnte also unterwegs verloren gehen. Ebenso ist es möglich, dass mehrere abgeschickte Pakete in unterschiedlicher Reihenfolge ankommen oder dass einzelne Pakete mehrfach ankommen. UDP ist durch den fehlenden Verbindungsaufbau sehr schnell und wird daher für DNS-Anfragen, NFS, Onlinespiele und VoIP-Verbindungen eingesetzt.

Das „Transmission Control Protocol“ TCP ist im Gegensatz zu UDP ein verbindungsorientiertes Protokoll. Zwischen den beiden beteiligten Systemen wird mittels eines Drei-Wege-Handshakes eine Verbindung aufgebaut. Gelingt dies, ist die Verbindung etabliert („established“). In diesem Zustand werden alle gesendeten Datenpakete durchnummeriert. Durch diese „Sequenznummer“ können verlorene Pakete erkannt und neu angefordert oder in unterschiedlicher Reihenfolge eingetroffene Pakete korrekt eingeordnet werden. Analog zum Aufbau muss die Verbindung wieder abgebaut werden.

Eine DNS-Anfrage über TCP würde drei Pakete für den Verbindungsaufbau, drei Pakete für die eigentliche Datenübertragung inkl. Bestätigungen sowie drei Pakete zum Abbau der Verbindung benötigen. Mittels UDP ist dasselbe mit insgesamt zwei Paketen erreichbar.

7.1.4 Paketzustellung

Das Versenden von Datenpaketen im lokalen Netzwerk – auch als „Local Area Network“ LAN bezeichnet – ist noch recht einfach. Ein Computersystem „fragt“ im LAN nach, welcher andere Computer die Ziel-IP-Adresse hat. Sobald dieser die Anfrage beantwortet, kann die Übertragung gestartet werden. Antwortet niemand, läuft die Anfrage in einen Timeout, und es gibt nach einiger Zeit eine entsprechende Fehlermeldung.

Liegt die Ziel-IP-Nummer dagegen außerhalb des lokalen Netzes in einem anderen Gebäude oder einer anderen Stadt, ist eine direkte Adressierung nicht möglich. Hier müssen „Router“ oder „Gateways“ verwendet werden. Üblicherweise ist ein Computer so eingestellt, dass er IP-Nummern aus dem eigenen lokalen Netzbereich direkt im lokalen Netz anfragt und alle Pakete zu fremden IP-Nummern zu einem „Default-Gateway“ im lokalen Netz sendet.

Dieses Gateway ist normalerweise das System mit der Internetverbindung und schickt die Datenpakete weiter zu seinem Default-Gateway beim Provider. Von dort aus läuft das Datenpaket über weitere Gateways und Router bis zum Zielsystem. Das Antwortpaket läuft den umgekehrten Weg zurück – es kann auch einen anderen Weg nehmen, da der genaue Weg im Internet nicht festgelegt ist und auch abhängig von Last und Ausfällen umgeschaltet wird. Dieser ganze Mechanismus der Paketzustellung wird als „Routing“ bezeichnet.

Um festzulegen, ob ein Paket für das lokale Netz bestimmt ist oder zum Default-Gateway gesendet werden muss, wird der „Adressbereich“ des lokalen Netzes benötigt. Dieser Adressbereich beinhaltet alle im lokalen Netz verwendeten IP-Nummern und besteht aus der „Netzwerkadresse“ und der „Netzmaske“.

Die Netzwerkadresse ist die erste IP-Adresse des Adressbereichs und wird nicht an Computer vergeben. Die Netzmaske legt die Größe des Adressbereichs fest und bestimmt damit die letzte IP-Adresse des Bereichs. Diese letzte Adresse ist die „Broadcastadresse“. Alle an diese Adresse geschickten Datenpakete werden von allen Computern im Adressbereich angenommen. Die Broadcastadresse sollte daher auch nicht für einen einzelnen Computer genutzt werden.

Der gesamte „IP-Adressraum“ von 0.0.0.0 bis 255.255.255.255 wurde anfangs in fünf Klassen unterteilt, um damit im Internet das Routing durchzuführen.

Für das Routing ist prinzipiell auf jedem zentralen Backbone-Router für jede IP-Nummer ein Eintrag notwendig, der klärt, wo diese IP-Nummer erreichbar ist. Um diese „Routingtabellen“ überschaubar zu halten, werden IP-Nummern zu IP-Netzen zusammengefasst. Damit sind in den Routingtabellen nur Einträge für Netze notwendig. Eine IP-Nummer kann in ihren Netzwerkanteil und den Hostanteil zerlegt werden. Dabei muss festgelegt werden, wie viele Bits (von links) innerhalb der IP-Adresse den Netzwerkanteil bilden.

Das Herausfiltern des Netzwerkanteils geschieht mit Hilfe der Netzmaske über eine logische UND-Verknüpfung. Dabei werden alle in der Netzmaske gesetzten Bits „stehen“ gelassen. Da der Netzanteil links und der Hostanteil rechts notiert ist, kann der Netzanteil (von links) 8 Bit, 9 Bit, 10 Bit, 11 Bit bis 32 Bit betragen. Daraus ergibt sich die heute verbreitete Schreibweise „/24“ für einen 24 Bit breiten Netzwerkanteil. Diese Schreibweise ist äquivalent zur Angabe der Netzmaske in der Form „255.255.255.0“.

Bei Class-A-Netzen ist der Netzwerkanteil 8 Bit groß. Die drei folgenden Oktette sind Hostnummern und können vom Inhaber des jeweiligen Class-A-Netzes beliebig in seinem Netzwerk verteilt werden. Weltweit gibt es 126 Class-A Netze mit jeweils über 16 Millionen Hosts.

Class-B-Netze haben einen 16 Bit großen Netzwerkanteil, 16 Bit bleiben für die (über 65000) Hosts übrig.

Bei Class-C-Netzen beträgt der Netzwerkanteil 24 Bit. Ihre Netzmaske ist die bekannte „255.255.255.0“. Weltweit gibt es knapp zwei Millionen Netze mit je 254 Hosts.

Ursprünglich konnte anhand der Netzklasse die Netzmaske für das Routing identifiziert werden. Heute wird dieses starre Schema nicht mehr angewandt, um mehr Flexibilität bei der Zuweisung von IP-Adressen zu erhalten. Der Adressraum ist damit „klassenlos“. Für die einzelnen Netze werden in den Internetroutern jeweils Einträge (mit den entsprechenden Netzmasken) vorgenommen. Diese gesamte Technik wird als „Classless Inter Domain Routing“ CIDR bezeichnet.

IP-Adressräume

Netzwerkadresse	Bit	Netzmaske	Verwendung
10.0.0.0	8	255.0.0.0	Für den privaten Gebrauch reservierter Block, darf im Internet nicht geroutet werden.
14.0.0.0	8	255.0.0.0	Für „Public Data Networks“ reservierter Block.
24.0.0.0	8	255.0.0.0	1996 für Kabelmodem-Anbieter reservierter Block, inzwischen freigegeben.
39.0.0.0	8	255.0.0.0	1995 für das „Klasse-A-Subnetz-Experiment“ reservierter Block, inzwischen freigegeben.
127.0.0.0	8	255.0.0.0	Als „Internet Host Loopback“ zur Kommunikation innerhalb eines Systems genutzter Block, darf nicht im Internet geroutet werden.
128.0.0.0	16	255.255.0.0	Ursprünglich von IANA reserviert, inzwischen freigegeben.
169.254.0.0	16	255.255.0.0	Systeme, die ihre IP-Adresse per DHCP beziehen, weisen sich aus diesem „Link Local“-Block eine Adresse zu, wenn kein DHCP-Server erreichbar ist.
172.16.0.0	12	255.240.0.0	Für den privaten Gebrauch reservierter Block, darf nicht im Internet geroutet werden.
192.255.0.0	16	255.255.0.0	Ursprünglich von IANA reserviert, inzwischen freigegeben.

192.0.0.0	24	255.255.255.0	Ursprünglich von IANA reserviert, inzwischen freigegeben.
192.0.2.0	24	255.255.255.0	„Test Netz“ zur Verwendung in Dokumentationen und Beispielen, darf im Internet nicht geroutet werden.
192.88.99.0	24	255.255.255.0	Reserviert für „6to4-Anycast-Adressen“ (siehe RFC3068).
192.168.0.0	24	255.255.255.0	Für den privaten Gebrauch reservierter Block, darf nicht im Internet geroutet werden.
192.18.0.0	15	255.254.0.0	Reserviert für Benchmark-Tests (siehe RFC2544).
223.255.255.0	24	255.255.255.0	Ursprünglich von IANA reserviert, inzwischen freigegeben.
224.0.0.0	4	240.0.0.0	Ehemaliger Klasse-D-Adressraum, reserviert für „IPv4-Multicast-Adresszuweisungen“.
240.0.0.0	4	240.0.0.0	Ehemaliger Klasse-E-Adressraum. Reserviert für zukünftige Freigabe, darf nicht geroutet werden.

Mit NAT („Network Address Translation“) wird der Vorgang bezeichnet, wenn in IP-Paketen die Quell- bzw. Ziel-Adresse ausgetauscht wird. Abhängig von der modifizierten Adresse werden SNAT („Source NAT“) und DNAT („Destination NAT“) unterschieden. Im V-Cube ist es auch möglich, NAT für ganze Netze durchzuführen („Netmap“). Dabei wird nur der Netzanteil ersetzt, der Hostanteil der IP-Adresse bleibt unverändert. Die Möglichkeiten der praktischen Anwendung sind in einfachen Netzwerkinstallationen begrenzt, da bei NAT eine

Eins-zu-Eins-Umsetzung von Adressen erfolgt. Beispielsweise muss der Provider vier öffentliche IP-Adressen bereitstellen, damit diese auf vier interne, private IP-Adressen umgesetzt werden können.

Da die Menge an IP-Nummern begrenzt ist und ein Administrator nicht immer genügend öffentliche IP-Nummern für alle Systeme in seinem Netz bekommen kann, wird das sogenannte „Masquerading“ eingesetzt. Dabei ersetzt das Gateway in den IP-Paketen jeweils die Absender-IP-Adresse (aus dem lokalen Netz) durch seine eigene IP-Nummer im Internet. Zusätzlich wird der Absendeport durch eine neue Portnummer ersetzt. Das Paket gelangt zum Zielrechner, der ein Antwortpaket an die vermeintliche Absenderadresse zurückschickt. Dadurch gelangt das Paket zum Gateway, und dieses kann anhand der Portnummer die ursprüngliche Absender-IP-Adresse sowie die Portnummer als neue Ziel-Adresse eintragen. Durch diesen Mechanismus wird das gesamte lokale Netz versteckt bzw. maskiert.

Masquerading ist ein Sonderfall von DNAT, da hier neben den IP-Adressen auch die Portadressen modifiziert werden. Durch dieses Verfahren können viele Rechner aus dem LAN ins Internet zugreifen und sich eine IP-Adresse „teilen“. Es ist jedoch kein Rechner aus dem LAN-Bereich im Internet sichtbar und von dort für den Aufbau einer neuen Verbindung erreichbar.

Für diesen Zweck ist die Verwendung von „privaten Netzen“ im lokalen Netz wichtig. Dies sind spezielle IP-Bereiche, die nicht im Internet geroutet werden. Würden willkürlich IP-Nummern für das lokale Netz verwendet, die an anderer Stelle im Internet vergeben sind, können diese Systeme im Internet nicht erreicht werden, da der Zielhost im lokalen Netz gesucht und u. U. gefunden wird.

Folgende Netze sind für private Verwendung freigegeben:

- 10.0.0.0/8 (von 10.0.0.0 bis 10.255.255.255)
- 172.16.0.0/12 (von 172.16.0.0 bis 172.31.255.255)
- 192.168.0.0/16 (von 192.168.0.0 bis 192.168.255.255)

Um bei Verwendung privater Adressen von außen auf einzelne Systeme im lokalen Netz zugreifen zu können, kann „Portforwarding“ genutzt werden. Dabei wird auf dem Gateway eine Portadresse festgelegt, bei deren Adressierung die Datenpakete zu einem anderen System weitergeleitet werden. Die Portadresse auf dem Zielsystem kann dabei ebenfalls festgelegt werden. So ist es beispielsweise möglich, unter der Portnummer 2403 des Gateways auf einen internen HTTPS-Webserver (Port 443) zuzugreifen.

7.1.5 Links

Ein „Netzwerklink“ stellt im einfachsten Fall eine Verbindung zwischen zwei Computern dar. Im V-Cube ist das Konzept der Links auf grundsätzlich jede Netzwerkverbindung ausgeweitet. So kann ein Link auch zwei oder mehr Netze miteinander verbinden.

In jedem Fall stellt ein Link eine Netzwerkverbindung dar. Dabei kann es sich um die Konfiguration einer konkreten Netzwerkschnittstelle handeln, aber auch um mehr abstrakte Konfigurationen wie der einer Route oder eines Tunnels.

Bei allen Linktypen können die erreichbaren Netze angegeben werden. Damit wird eine Routing-Entscheidung vorgenommen, d. h., diese Netze werden auf den Link geroutet.

Im klassischen Modell kann ein Netz nur über einen Link erreichbar sein. V-Cube geht einen Schritt weiter. Hier kann ein und dasselbe Netz auf mehreren Links als erreichbar angegeben werden. Dies ist möglich, da intern „Policy-Routing“ verwendet wird. Die einzelnen Links zu einem Netz werden priorisiert, und der Link mit der höchsten Priorität wird verwendet. Mittels Link-Überwachung schaltet der V-Cube im Fehlerfall selbständig zwischen den einzelnen Links um.

Auf einem Link kann „Masquerading“ aktiviert werden. Dabei

werden die zum Maskieren ausgewählten Netze aus der Quell-IP-Adresse der Pakete entfernt und durch die eigene IP-Adresse des V-Cubes auf dem jeweiligen Link ersetzt.

Auf einem Link können ein oder mehrere Port-Weiterleitungen eingerichtet werden. Dabei wird als Port jeweils ein angelegter *Dienst* ausgewählt. Die Adresse, auf der dieser Port angenommen und umgeleitet wird, ist die Adresse auf dem Link selbst. Die Zieladresse (IP-Nummer und Port) für die Umleitung kann frei vergeben werden. Auf dem Zielsystem muss der V-Cube als Standard-Gateway eingetragen sein, damit Antwortpakete den Weg zurück finden.

7.1.5.1 Ethernet

TCP/IP spezifiziert Protokolle, Adressen und Ports, macht aber keinerlei Angaben über das eigentliche Übertragungsmedium. Der Transport der Daten ist Aufgabe eines untergeordneten Mediums. Dabei handelt es sich im LAN meist um „Ethernet“, dem wichtigsten Typ eines Links.

Ethernet ist eine Vernetzungstechnologie, bei der alle Teilnehmer analog zum Funkverkehr jederzeit zu senden anfangen können (daher auch der Name „Äthernetz“). Praktisch darf zu einem Zeitpunkt immer nur eine Station senden, sonst kommt es im Netz zu Kollisionen. Daher wartet jedes System zunächst, bis das Medium frei ist, und beginnt dann die Übertragung. Der Algorithmus „Carrier Sense Multiple Access with Collision Detection“ CSMA/CD sorgt dafür, dass Kollisionen durch mehrere gleichzeitig sendende Stationen erkannt werden. Diese Stationen warten dann jeweils eine zufällige, sehr kurze Zeitspanne und senden erneut. Damit dieser Mechanismus sicher funktioniert, müssen die Datenpakete eine Mindestgröße haben (so dass die Übertragung eine minimale „Sendezeit“ nicht unterschreitet).

Diese Betriebsart wird Halbduplex genannt, d. h., bei der Übertragung zwischen zwei Stationen kann nur eine Station senden. Bei Vollduplex hingegen können beide beteiligten Stationen gleichzeitig senden und empfangen, was den Datendurchsatz erhöht.

Thin-Wire-Ethernet

Bei Thin-Wire-Ethernet (10Base2, Standard IEEE 802.3a) wird Koaxialkabel mit einem Wellenwiderstand von 50 Ohm (RG58-Kabel) in Kombination mit BNC-Steckverbindern eingesetzt. Alle angeschlossenen Systeme werden jeweils mit einem T-Stück wie auf einer Perlenkette zu einem Segment miteinander verbunden. Ein solches Segment darf insgesamt bis zu 185 m lang sein und wird an beiden Enden jeweils mit einem Abschlusswiderstand terminiert. Auf Thin-Wire-Ethernet sind Datenraten von 10 MBit/s möglich, die allerdings bei vielen Teilnehmern durch zunehmende Kollisionen nie erreicht werden. Zudem ist es sehr fehleranfällig, da eine einzelne Störung (defektes T-Stück o. ä.) bereits das gesamte Segment lahmlegen kann. Da es mit geringem Aufwand zu installieren ist und außer Netzwerkkarten keine weiteren Komponenten benötigt, war Thin-Wire-Ethernet bis vor wenigen Jahren sehr beliebt.

Twisted-Pair-Ethernet

Bei Twisted-Pair-Ethernet wird Kabel mit acht Adern eingesetzt, von denen je zwei zu einem Paar verdrillt sind. Als Steckverbinder werden RJ45-Stecker genutzt. Im Gegensatz zu Thin-Wire-Ethernet ist bei TP eine Sternverkabelung notwendig, d. h., ein Hub oder Switch bildet das Zentrum des TP-Ethernets.

Die Kabel werden entsprechend ihrer Qualität und Abschirmung in verschiedene Kategorien unterteilt. Anfangs wurden von den vier

Aderpaaren nur zwei zur Übertragung genutzt, zunächst wurden mit CAT-3-Kabeln Datenraten von 10 MBit/s erreicht (10Base-T), später auf CAT-5-Kabeln 100 MBit/s (100-Base-T) und heute ist 1 GBit/s möglich (dann werden allerdings vier Adernpaare genutzt). Varianten mit 10 GBit/s sind in Entwicklung und haben derzeit auf Kupferkabeln eine Reichweite von etwa 15 m.

Durch das zentrale Element ist TP-Ethernet wesentlich unanfälliger für Störungen, da durch Ausfall eines Kabels nur die Verbindung zu einem System unterbrochen ist.

Ein Hub dupliziert alle auf einer Schnittstelle ankommenden Datenpakete auf alle Schnittstellen, daher kann hier das Netzwerk nur im Halbduplex-Betrieb laufen. Jedes System sieht den gesamten Datenverkehr im Netzwerk. Dies ist gleichzeitig gut (für den Einsatz von IDS-Sensoren, die Angriffsmuster erkennen) und schlecht (Passwortsniffer).

Ein Switch ist ein intelligenter Ersatz für den Hub. Er erkennt anhand der MAC-Adresse, welches System an welchem Anschluss erreichbar ist. So schaltet er eingehende Pakete für ein System nur zu dessen Anschluss durch (es sind jedoch Angriffe möglich, um Pakete für andere Systeme auf den eigenen Anschluss geschaltet zu bekommen). Das Netzwerk kann auch im Vollduplex-Modus betrieben werden.

Größere Switches sind "managebar", d. h., sie können über eine Oberfläche verwaltet werden. So lassen sich einzelne Ports sperren, Datenvolumen können protokolliert werden, der gesamte Netzwerkverkehr kann auf einen Monitorport dupliziert werden (etwa für IDS-Sensoren) und vieles weitere mehr.

Glasfaser

Glasfaserkabel oder Lichtwellenleiter (LWL) sind flexible Kabel, deren Kern aus Glasfasern besteht. Diese sind jeweils mit einem Glas mit niedrigem Brechungsindex ummantelt. An der Grenzfläche zwischen Mantel und Faser kommt es zur Totalreflexion des Lichts. Eingespeistes Licht kann daher nahezu verlustfrei über große Entfernungen übertragen werden und ermöglicht gleichzeitig hohe Übertragungsraten bis in den Terabit-Bereich. Glasfaserverbindungen sind unempfindlich gegen elektromagnetische Störungen wie Übersprechen, technische Geräte und Gewitter.

Ethernet-Arten

Physical Layer	Kabelart	Geschwindigkeit	Reichweite	Topologie
10base-5	Koaxial (dick)	10 MBit/s halb-duplex	500 m	Ring
10base-T	Twisted Pair, CAT4, 2 Paare	10 MBit/s halb-duplex	100 m	Stern
100base-T	Twisted Pair, CAT5, 2 Paare	100 MBit/s halb-/vollduplex	100 m	Stern
100baseT4	Twisted Pair, CAT3, 4 Paare	100 MBit/s halb-/vollduplex	100 m	Stern
100baseFX	Glasfaser	100 MBit/s vollduplex	412 m	Point-to-Point, Stern
1000baseT	Twisted Pair, CAT5/6, 4 Paare	1000 Mit/s halb-/vollduplex	100 m	Point-to-Point, Stern
1000baseSX/LX	Glasfaser (short/long laser)	1000 MBit/s vollduplex	550 m/5000 m	Point-to-Point, Stern
10GBase-T	Twisted Pair, CAT 6a/7, 4 Paare	10000 MBit/s vollduplex	100 m	Point-to-Point, Stern

LAN-Adressierung

Neben den eingesetzten Kabeltypen definiert Ethernet auch Zugriffsprotokolle auf diese Medien. Zur Adressierung der einzelnen

Systeme werden „MAC-Adressen“ (Media Access Control) verwendet. Dabei handelt es sich um eine 48 Bit lange Hardwareadresse, die pro Netzwerkschnittstelle weltweit eindeutig sein sollte. Sie kann mit geringem Aufwand auf andere Werte gesetzt werden, ist also nicht fälschungssicher.

Meist wird die MAC-Adresse in der Form 00:D0:59:13:7C:e8 geschrieben. In Ethernet-Paketen taucht sie als Absender- wie auch als Empfängeradresse auf. MAC-Adressen sind nur innerhalb eines Netzwerksegments sichtbar.

Bevor die Kommunikation zwischen zwei Systemen beginnen kann, muss die Adresse des Partners ermittelt werden. Dazu wird das „Address Resolution Protocol“ (ARP) verwendet. Das sendende System fragt ins Netzwerk, welche MAC-Adresse einer bestimmte IP-Nummer entspricht:

```
arp who-has 192.0.2.9 tell 192.0.2.4
```

Das Zielsystem muss auf die IP-Nummer reagieren und seine MAC-Adresse mitteilen:

```
arp reply 192.0.2.9 is-at 00:50:c2:20:e0:8a
```

Hier findet das Zusammenspiel von TCP/IP und Ethernet statt. Aufgelöste MAC-Adressen werden von den Systemen eine Zeit lang im ARP-Cache zwischengespeichert, ein Switch kann anhand seiner ARP-Tabelle die Pakete an die entsprechenden Ports weitergeben.

Konfiguration

Im V-Cube bleiben all diese technischen Details verborgen, da sie von der Netzwerkkarte entsprechend umgesetzt werden. Sobald die Netzwerkkarte vom V-Cube mit einem Treiber unterstützt wird, steht die Schnittstelle in der Weboberfläche zur weiteren Konfiguration zur Verfügung.

Auf einem Ethernet-Link wird die IP-Adresse gesetzt, die der V-

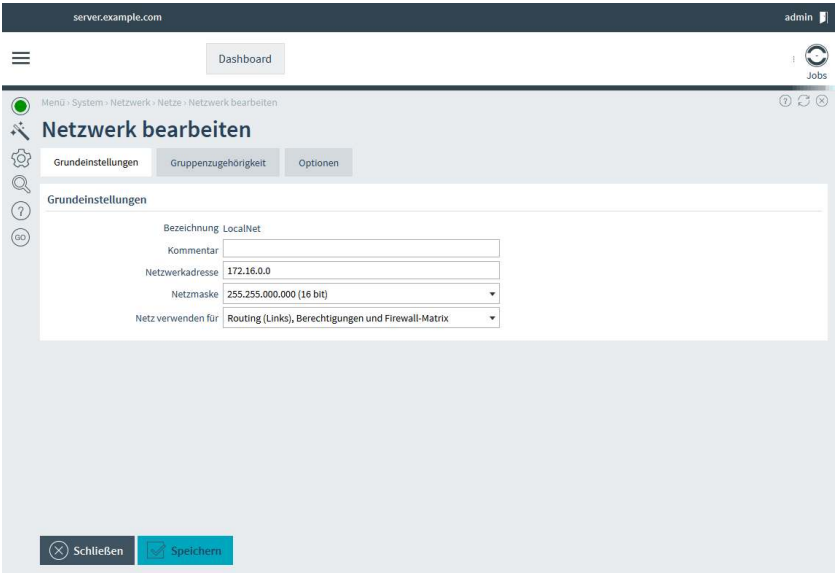
Cube bekommen soll. Bleibt das Feld leer, wird er versuchen eine Adresse per DHCP zu beziehen. Dazu werden die erreichbaren Netze angegeben, meist die Bereiche, aus denen seine eigene IP-Adresse stammt.

7.1.5.2 Datenverkehr ins Internet

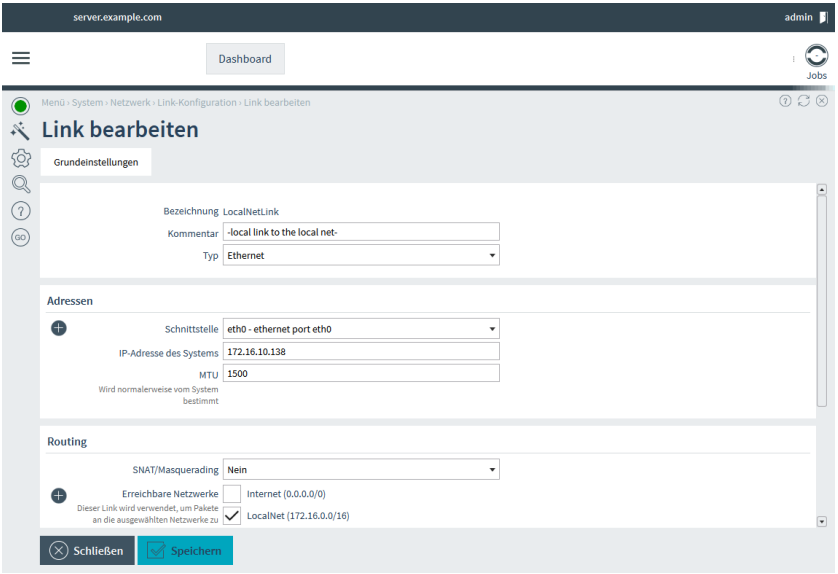
Die Verbindung zum Internet (manchmal auch als „Uplink“ bezeichnet) kann über verschiedene Medien und Protokolle hergestellt werden. Dabei hat sich der Begriff des „Wide Area Network“ WAN eingebürgert.

7.2 Schritt für Schritt: Einrichten des lokalen Netzes

Einer der ersten Schritte bei der Konfiguration des V-Cubes ist das Einrichten des lokalen Netzwerks. Dazu gehören der IP-Bereich und die IP-Adresse des V-Cubes in diesem Netz.



- Wechseln Sie zu *Netzwerk – Netze – Konfiguration*.
- Bearbeiten Sie das *LocalNet*, welches bereits in der Grundeinstellung vorhanden ist.
- Tragen Sie unter *Netzwerkadresse* die Basisadresse Ihres lokalen IP-Bereichs ein. Dies ist nicht die IP-Adresse, die der V-Cube später verwenden wird.
- Prüfen Sie die *Netzwerkmaske*.
- Speichern Sie das geänderte Netzwerk.



- Unter *Netzwerk – Links – Konfiguration* sind alle angelegten Links aufgelistet.
- Bearbeiten Sie den *LocalNetLink*, der ebenfalls in der Grundeinstellung vorhanden ist.
- Unter *Typ* legen Sie fest, welcher Art der Link ist. Mit dem lokalen Netz wird der V-Cube üblicherweise über ein Netzwerkkabel verbunden, die entsprechende Einstellung ist daher *Ethernet*.
- Die IP-Adresse des V-Cubes tragen Sie unter *IP-Adresse des Systems* ein. Diese IP-Adresse muss unbedingt zu dem Netzwerkbereich des *LocalNets* gehören.
- Unter *Schnittstelle* legen Sie die Netzwerkkarte fest, an der das lokale Netz angeschlossen ist. Üblicherweise wird dazu die erste Netzwerkkarte im System verwendet, also *eth0*.
- Unter *Erreichbare Netzwerke* legen Sie fest, welche Netze (IP-Bereiche) auf diesen Link geroutet werden. Hier wird nur das

LocalNet markiert, das *Internet* ist auf dem Netzwerkkabel an *eth0* nicht erreichbar.
- Speichern Sie Ihre Änderungen.

7.3 GUI-Referenz: *Netze*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Richtlinien – Netze* sowie unter *Netzwerk – Netze*)

In diesem Dialog werden alle angelegten Netzwerke angezeigt. Ein Netzwerk umfasst einen IP-Bereich, der in den Dialogen zu den *Links* auf Interfaces oder Routen geschaltet werden kann.

In diesem Dialog können weitere Netzwerke angelegt bzw. vorhandene Netze bearbeitet oder gelöscht werden.

Hinweis: Das vordefinierte Netzwerk *Internet* umfasst alle IP-Nummern dieser Welt außer denen, die in anderen hier angelegten Netzwerken spezifiziert sind. Dieses Netzwerk wird zum Routen ins Internet benötigt. Es kann daher nicht bearbeitet werden.

7.3.1 *Netzwerk wählen*

In diesem Dialog können ein Netzwerk zum Bearbeiten oder Löschen ausgewählt und weitere Netzwerke anlegt werden.

7.3.1.1 Felder in diesem Dialog

- *Bezeichnung*: Hier wird die Bezeichnung des Netzwerks angezeigt.
- *Netzwerkadresse*: In diesem Feld wird die zugehörige Netzwerkadresse angezeigt.

- *Netzmaske*: Über die hier angezeigte Netzmaske ergibt sich die Größe des Netzwerkbereichs.

7.3.1.2 Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion können die Einstellungen für ein Netzwerk geändert werden.
- *Löschen*: Mit dieser Aktion wird das angezeigte Netzwerk gelöscht.

7.3.1.3 Aktionen für diesen Dialog

- *Netzwerk anlegen*: Mit dieser Schaltfläche wird der Dialog zum Anlegen eines neuen Netzwerks geöffnet.

7.3.2 *Netzwerk bearbeiten*

In diesem Dialog werden für ein Netzwerk die Netzwerkadresse und die Netzmaske festgelegt und eine Bezeichnung vergeben.

Hinweis: Wird die Netzwerkadresse oder die Netzmaske eines Netzes geändert, kann es geschehen, dass eine IP-Adresse eines dem Netz zugeordneten Links außerhalb des Netzwerkes liegt. Solche Links werden nicht automatisch aus dem Netz entfernt oder einem anderen Netz zugeordnet. Als Folge ist das System eventuell nicht mehr erreichbar.

In solchen Fällen wird eine Warnung ausgegeben. Die Einstellungen werden dennoch gespeichert.

7.3.2.1 Tab *Grundeinstellungen*, Abschnitt *Grundeinstellungen* Felder in diesem Abschnitt

- *Bezeichnung des Netzwerks*: Hier wird die Bezeichnung für das Netzwerk angegeben. Unter diesem Namen wird das Netzwerk in verschiedenen anderen Dialogen zur Auswahl angeboten.

  Diese Bezeichnung kann nachträglich nicht mehr geändert werden.
- *Bezeichnung*: Wird ein bereits angelegtes Netzwerk bearbeitet, wird das Feld *Bezeichnung* nur angezeigt, es kann nicht geändert werden.
- *Netzwerkadresse*: In diesem Feld wird die Adresse des Netzwerks festgelegt.
- *Netzmaske*: In diesem Feld wird die zugehörige Netzmaske für das Netzwerk eingestellt. Dabei können beide Schreibweisen (*255.255.255.0* und */24*) ausgewählt werden.
- *Netz verwenden für*: Ein Netzwerk kann für entweder für die lokalen Benutzungsrichtlinien und in den Regeln der Firewall-Matrix, oder für lokales Routing, lokale Benutzungsrichtlinien und Regeln der Firewall-Matrix verwendet werden. Wird es für lokales Routing verwendet, kann das Netzwerk nicht nur als Element für Gruppenberechtigungen oder Firewall-Regeln verwendet werden, sondern es kann auch über die Link-Konfiguration als erreichbares Netzwerk geroutet werden.
- *Link*: Für neu angelegte Netzwerke kann bereits ein Link ausgewählt werden, auf dem das Netzwerk *erreichbar* ist. Es ist nur möglich, einen einzelnen Link auszuwählen. Weitere Einstellungen können in der „Link-Konfiguration“ vorgenommen werden.

7.3.2.2 Tab *Gruppenzugehörigkeit*, Abschnitt *Gruppenzugehörigkeit* Felder in diesem Abschnitt

- *Einstellungen*: Das bearbeitete Netz ist Mitglied in allen aktivierten Gruppen. Über die Gruppen werden in den *Benutzungsrichtlinien* Berechtigungen für Systeme aus den einzelnen Netzwerkbereichen vergeben.

7.3.2.3 Tab *Optionen*, Abschnitt *Optionen* Felder in diesem Abschnitt

- *Proxy-ARP aktivieren*: Normalerweise sind Systeme innerhalb eines Netzwerkbereichs in einem Netzwerksegment angeschlossen. Sie kommunizieren direkt über das ARP-Protokoll auf Ethernet-Ebene miteinander.

  In bestimmten Konfigurationen ist es sinnvoll, einzelne Rechner in anderen Segmenten anzuschließen, etwa ein Server in eine DMZ. Wird seine IP-Adresse dabei nicht geändert, ist er für die anderen Systeme „unsichtbar“ (da Ethernet-Pakete nicht über Router weitergeleitet werden).

  Durch das Aktivieren von Proxy-ARP erkennt der V-Cube ARP-Anfragen auf einem Segment für ein System, welches auf einem anderen Segment angeschlossen ist, und beantwortet diese. Dadurch erhält er selbst das Paket und kann es auf das richtige Netzwerksegment weiterleiten. Eine solche Konfiguration wird manchmal als „Pseudo Bridging“ bezeichnet.

  Hinweis: Falsch eingesetzt kann ein aktiviertes Proxy-ARP zu erheblichen Störungen im Netzwerk führen.
- *Schnittstellen für Proxy-ARP*: Hier wird die Schnittstellen ausgewählt, auf denen ARP-Anfragen beantwortet werden sollen. Die

Liste enthält nur die Ethernet-Schnittstellen, die durch einen Link vom Typ *Ethernet* in Verwendung sind.

7.4 GUI-Referenz: Links

Im Gegensatz zu den Netzen behandeln Links eine konkrete Schnittstellenkonfiguration und dienen der Einrichtung des Routings. Links können für verschiedenste Anwendungen eingerichtet werden. Der einfachste Fall ist die Einrichtung einer Netzwerkschnittstelle mit dem Setzen der IP-Adresse des V-Cubes.

Genauso ist es über Links möglich, Routen zu setzen, eine Internet-Einwahl über DSL einzurichten oder Datentunnel aufzubauen.

7.4.1 *Links – Allgemein*

(Diese Option befindet sich im Zusatzmodul *Collax Gatekeeper*)

(Dieser Dialog befindet sich unter *Netzwerk – Links – Allgemein*)

In diesem Dialog werden allgemeine Einstellungen für die Links vorgenommen.

7.4.1.1 Abschnitt *VPN*

In diesem Abschnitt werden globale VPN-Optionen konfiguriert.

Felder in diesem Abschnitt

- *NAT-Traversal aktivieren*: NAT-Traversal ist eine Technik, mit der ein VPN-Client hinter einem maskierenden Router einen VPN-Tunnel aufbauen kann. Dazu werden die IPsec-Pakete in UDP-Pakete eingepackt, die gefahrlos maskiert werden können. Dies ist eine globale Option, die bei ihrer Aktivierung für jeden Verbindungsaufbau einzeln geprüft und ggf. verwendet wird.
- *Standard-Proposal*: Hier wird ein definiertes IPsec-Proposal als Standard definiert.

7.4.2 *Link-Konfiguration*

In diesen Dialogen werden die Netzwerkverbindungen des V-Cubes konfiguriert. Solche Verbindungen werden als *Links* bezeichnet.

7.4.2.1 *Link wählen*

(Dieser Dialog befindet sich unter *Netzwerk – Links – Link*)

In dieser Übersicht werden alle vorhandenen Links angezeigt. Hier können weitere Links angelegt oder vorhandene Links bearbeitet oder gelöscht werden.

Felder in diesem Dialog

- *Bezeichnung*: Hier wird die Bezeichnung des Links angezeigt. Unter diesem Namen wird der Link in weiteren Dialogen verwendet.
- *Typ*: Hier wird der Typ des Links angezeigt.
- *Kommentar*: Hier wird ein Kommentartext zum Link angezeigt.

Aktionen für jeden Tabelleneintrag

- *Link bearbeiten*: Mit dieser Aktion können die Einstellungen eines Links bearbeitet werden.
- *Löschen*: Diese Aktion löscht den Link.

Aktionen für diesen Dialog

- *Link hinzufügen*: Mit dieser Aktion wird ein neuer Link hinzugefügt.

7.4.2.2 *Link bearbeiten*

(Dieser Dialog befindet sich unter *Netzwerk – Links – Link*)

In diesem Dialog werden die Einstellungen eines Links geändert.

In diesem Dialog werden die Konfigurationseinstellungen zu einem Link angegeben.

Abhängig von der unter *Typ* eingestellten Art des Links werden verschiedene Optionen ein- und ausgeblendet. Im folgenden werden die unterschiedlichen Linktypen mit ihren jeweiligen Optionen vorgestellt.

Felder in diesem Dialog für Typ *Ethernet*

- *Bezeichnung*: Hier muss eine eindeutige Bezeichnung für den Link angegeben werden. Unter diesem Namen steht der Link in verschiedenen anderen Dialogen zur Verfügung.
- *Kommentar*: Hier kann ein Kommentartext zu diesem Link angegeben werden.
- *Typ*: Hier wird der genaue Typ des Links angegeben. Abhängig

davon werden weitere Felder in diesem Dialog sichtbar bzw. unsichtbar.

- *IP-Adresse des Systems*: Hier wird die lokale IP-Adresse für den Link angegeben. Bleibt das Feld leer, versucht das System, eine dynamische IP-Adresse per PPP oder DHCP zu beziehen. Sollen mehrere IP-Adressen auf einen Netzwerkanschluss zugewiesen werden (IP-Alias), muss für jede IP-Adresse ein eigener Link angelegt werden. Dabei wird jedes Mal die gleiche Schnittstelle angegeben.
- *MTU*: Hier kann die maximale Paketgröße auf diesem Link eingestellt werden.

  Große Werte für die MTU verbessern den Durchsatz, da weniger Verwaltungsdaten übertragen werden. Kleine Werte für die MTU hingegen verbessern die Antwortzeiten für interaktive Anwendungen und Echtzeitdatenübertragung (etwa VoIP).

  Wird hier kein Wert eingetragen, wird abhängig von der Art des Links ein geeigneter Wert gewählt. Für Ethernet-Verbindungen wird typischerweise eine MTU von 1500 Byte verwendet.
- *Schnittstelle*: Wird für den Link eine Schnittstelle benötigt, kann diese hier eingestellt werden.
- *SNAT/Masquerading*: SNAT und Masquerading dienen dazu, ganze Netzwerke hinter einer einzelnen IP-Adresse zu „verstecken“. Wird diese Option aktiviert, scheinen alle abgehenden Verbindungen von diesem System zu stammen und nicht vom wirklichen Absender.

  Diese Option muss aktiviert werden, wenn auf dem Internet-Link vom Provider nur eine einzelne IP-Adresse bereitgestellt wird und wenn Systeme aus dem lokalen Netz IP-Verbindungen aufbauen müssen.

  Die Unterscheidung zwischen SNAT und Masquerading erfolgt automatisch, abhängig davon, ob eine IP-Adresse für den Link angegeben wurde oder nicht.

Hinweis: SNAT/Masquerading für Routen und VPN-Netze funktioniert nur, wenn auf dem unterliegenden Link kein Masquerading aktiviert ist.

- *Zu maskierende Netzwerke*: Wird Masquerading für *spezielle Netze* aktiviert, können in dieser Liste aus allen angelegten Netzwerken diejenigen ausgewählt werden, die maskiert werden müssen.

  Hinweis: Alle Subnetze eines ausgewählten Netzwerks werden ebenfalls maskiert.

  Wird ein Netzwerk aus der Liste ausgewählt, bedeutet das nicht automatisch, dass Daten aus diesem Netzwerk über diesen Link versendet werden können.
- *Erreichbare Netzwerke*: Hier können aus der Liste aller angelegten Netzwerken diejenigen ausgewählt werden, die über diesen Link erreichbar sind. Für jedes ausgewählte Netz wird ein Eintrag unter *Zuordnungen* angelegt.

  Bei VPN-Verbindungen muss das lokale Netz der Gegenstelle innerhalb einem der hier angegebenen Netze liegen.
- *Verifikation von MAC-Adressen*: Für Ethernet-Links kann der Zugriff auf das System auf bekannte und verifizierte Hosts beschränkt werden. Pakete von fremden Systemen werden dann verworfen. Zwei verschiedene Arten der Adressverifikation sind möglich:

  IP+MAC-Verifikation nimmt nur Pakete an, wenn die Absender-IP-Adresse von einem bestätigten, bekannten Host kommt und die MAC-Adresse mit der Adresse in der Hosts-Konfiguration übereinstimmt.

  Bei der *MAC*-Verifikation werden nur Pakete angenommen, deren Absender-MAC-Adresse einem bekannten und bestätigten Host gehört. Es wird nicht überprüft, ob die MAC-Adresse zu der entsprechenden IP-Adresse gehört. Diese Option wird genutzt, wenn DHCP verwendet wird.

  Hinweis: Vor dem Aktivieren dieser Option müssen die Syste-

me im lokalen Netz und allen anderen direkt angeschlossenen Ethernet-Segmenten im V-Cube angelegt und bestätigt werden. Zudem ist der Sicherheitsgewinn nicht sehr groß, da eine MAC-Adresse ohne großen Aufwand per Software geändert werden kann.

Felder in diesem Dialog für Typ *Route*

- *Bezeichnung*: Hier muss eine eindeutige Bezeichnung für den Link angegeben werden. Unter diesem Namen steht der Link in verschiedenen anderen Dialogen zur Verfügung.
- *Kommentar*: Hier kann ein Kommentartext zu diesem Link angegeben werden.
- *Typ*: Hier wird der genaue Typ des Links angegeben. Abhängig davon werden weitere Felder in diesem Dialog sichtbar bzw. unsichtbar.
- *IP-Adresse der Gegenstelle*: Hier wird die IP-Adresse der Gegenstelle angegeben. Bleibt das Feld leer, versucht das System, die Adresse der Gegenstelle automatisch zu bestimmen.
- *MTU*: Hier kann die maximale Paketgröße auf diesem Link eingestellt werden.

  Große Werte für die MTU verbessern den Durchsatz, da weniger Verwaltungsdaten übertragen werden. Kleine Werte für die MTU hingegen verbessern die Antwortzeiten für interaktive Anwendungen und Echtzeitdatenübertragung (etwa VoIP).

  Wird hier kein Wert eingetragen, wird abhängig von der Art des Links ein geeigneter Wert gewählt. Für Ethernet-Verbindungen wird typischerweise eine MTU von 1500 Byte verwendet.
- *SNAT/Masquerading*: SNAT und Masquerading dienen dazu, ganze Netzwerke hinter einer einzelnen IP-Adresse zu „verstecken“. Wird diese Option aktiviert, scheinen alle abgehenden Verbindungen

von diesem System zu stammen und nicht vom wirklichen Absender.

Diese Option muss aktiviert werden, wenn auf dem Internet-Link vom Provider nur eine einzelne IP-Adresse bereitgestellt wird und wenn Systeme aus dem lokalen Netz IP-Verbindungen aufbauen müssen.

Die Unterscheidung zwischen SNAT und Masquerading erfolgt automatisch, abhängig davon, ob eine IP-Adresse für den Link angegeben wurde oder nicht.

Hinweis: SNAT/Masquerading für Routen und VPN-Netze funktioniert nur, wenn auf dem unterliegenden Link kein Masquerading aktiviert ist.

- *Zu maskierende Netzwerke*: Wird Masquerading für *spezielle Netze* aktiviert, können in dieser Liste aus allen angelegten Netzwerken diejenigen ausgewählt werden, die maskiert werden müssen.

  Hinweis: Alle Subnetze eines ausgewählten Netzwerks werden ebenfalls maskiert.

  Wird ein Netzwerk aus der Liste ausgewählt, bedeutet das nicht automatisch, dass Daten aus diesem Netzwerk über diesen Link versendet werden können.
- *Erreichbare Netzwerke*: Hier können aus der Liste aller angelegten Netzwerken diejenigen ausgewählt werden, die über diesen Link erreichbar sind. Für jedes ausgewählte Netz wird ein Eintrag unter *Zuordnungen* angelegt.

  Bei VPN-Verbindungen muss das lokale Netz der Gegenstelle innerhalb einem der hier angegebenen Netze liegen.

Felder in diesem Dialog für Typ *Analoges Modem*

(Diese Option befindet sich im Zusatzmodul *Collax Gatekeeper*)

- *Bezeichnung*: Hier muss eine eindeutige Bezeichnung für den

Link angegeben werden. Unter diesem Namen steht der Link in verschiedenen anderen Dialogen zur Verfügung.

- *Kommentar*: Hier kann ein Kommentartext zu diesem Link angegeben werden.
- *Typ*: Hier wird der genaue Typ des Links angegeben. Abhängig davon werden weitere Felder in diesem Dialog sichtbar bzw. unsichtbar.
- *Verbindungsaufbau*: Bei Verbindungen, für die eine Einwahl stattfindet oder die eine Einwahl annehmen können, wird in diesem Feld ausgewählt, wie genau die Einwahl erfolgen soll:

  Immer bedeutet, dass der Link beim Aktivieren der Konfiguration bzw. beim (Neu-)Start des Systems sofort versuchen wird, sich auf der Gegenstelle einzuwählen. Die Verbindung besteht also quasi permanent.

  Bei Bedarf wartet mit dem Einwahlvorgang, bis wirklich Pakete vom lokalen System oder aus dem lokalen Netz zur Gegenseite übertragen werden sollen.

  Auf Einwahl warten baut selbst keine Verbindung auf, sondern wartet darauf, dass eine Gegenstelle die Verbindung aufbaut. Dies kann beispielsweise die Einwahl eines Außendienstmitarbeiters über ISDN oder über VPN sein.
- *Neustart erzwingen*: Diese Option ermöglicht einen gezielten Neustart der Verbindung, um u. U. die Erreichbarkeit des Servers zu erhöhen.
- *Uhrzeit*: Der Zeitpunkt, zu dem die entsprechende Verbindung neu gestartet wird.
- *IP-Adresse des Systems*: Hier wird die lokale IP-Adresse für den Link angegeben. Bleibt das Feld leer, versucht das System, eine dynamische IP-Adresse per PPP oder DHCP zu beziehen. Sollen mehrere IP-Adressen auf einen Netzwerkanschluss zugewiesen werden (IP-Alias), muss für jede IP-Adresse ein eigener Link

angelegt werden. Dabei wird jedes Mal die gleiche Schnittstelle angegeben.

Ist der Link vom Typ *auf Einwahl warten* und bleibt das Feld leer, wird eine zufällig ausgewählte IP-Adresse als lokale IP-Adresse verwendet. Andernfalls wird die eingetragene IP-Adresse als lokale IP-Adresse genutzt.

- *IP-Adresse der Gegenstelle*: Hier wird die IP-Adresse der Gegenstelle angegeben. Bleibt das Feld leer, versucht das System, die Adresse der Gegenstelle automatisch zu bestimmen.
- *Benutzername*: Hier wird das Login angegeben, mit dem sich das System bei der Einwahl an der Gegenstelle authentifizieren soll.
- *Passwort*: Hier wird das zugehörige Passwort angegeben.
- *Zusätzliche Hayes-Befehle*: Bei einem Link vom Typ *Modem* können hier zusätzliche Hayes-Kommandos eingegeben werden, die bei der Initialisierung an das Modem geschickt werden. Oft müssen spezielle Optionen gesetzt werden, um ein Modem an einer Telefonanlage zu betreiben.
- *Rufnummer der Gegenstelle*: Hier wird die Telefonnummer der Gegenstelle angegeben. Eine Rufnummer im Ortsnetz sollte ohne Vorwahl eingegeben werden. Die Vorwahl wird automatisch übernommen, wenn unter *Konfiguration – Hardware* die entsprechende Option aktiviert ist.
- *MTU*: Hier kann die maximale Paketgröße auf diesem Link eingestellt werden.

  Große Werte für die MTU verbessern den Durchsatz, da weniger Verwaltungsdaten übertragen werden. Kleine Werte für die MTU hingegen verbessern die Antwortzeiten für interaktive Anwendungen und Echtzeitdatenübertragung (etwa VoIP).

  Wird hier kein Wert eingetragen, wird abhängig von der Art des Links ein geeigneter Wert gewählt. Für Ethernet-Verbindungen wird typischerweise eine MTU von 1500 Byte verwendet.

- *Schnittstelle*: Wird für den Link eine Schnittstelle benötigt, kann diese hier eingestellt werden.
- *SNAT/Masquerading*: SNAT und Masquerading dienen dazu, ganze Netzwerke hinter einer einzelnen IP-Adresse zu „verstecken“. Wird diese Option aktiviert, scheinen alle abgehenden Verbindungen von diesem System zu stammen und nicht vom wirklichen Absender.

  Diese Option muss aktiviert werden, wenn auf dem Internet-Link vom Provider nur eine einzelne IP-Adresse bereitgestellt wird und wenn Systeme aus dem lokalen Netz IP-Verbindungen aufbauen müssen.

  Die Unterscheidung zwischen SNAT und Masquerading erfolgt automatisch, abhängig davon, ob eine IP-Adresse für den Link angegeben wurde oder nicht.

  Hinweis: SNAT/Masquerading für Routen und VPN-Netze funktioniert nur, wenn auf dem unterliegenden Link kein Masquerading aktiviert ist.
- *Zu maskierende Netzwerke*: Wird Masquerading für *spezielle Netze* aktiviert, können in dieser Liste aus allen angelegten Netzwerken diejenigen ausgewählt werden, die maskiert werden müssen.

  Hinweis: Alle Subnetze eines ausgewählten Netzwerks werden ebenfalls maskiert.

  Wird ein Netzwerk aus der Liste ausgewählt, bedeutet das nicht automatisch, dass Daten aus diesem Netzwerk über diesen Link versendet werden können.
- *Erreichbare Netzwerke*: Hier können aus der Liste aller angelegten Netzwerken diejenigen ausgewählt werden, die über diesen Link erreichbar sind. Für jedes ausgewählte Netz wird ein Eintrag unter *Zuordnungen* angelegt.

  Bei VPN-Verbindungen muss das lokale Netz der Gegenstelle innerhalb einem der hier angegebenen Netze liegen.

Felder in diesem Dialog für Typ *ISDN synchron*

(Diese Option befindet sich im Zusatzmodul *Collax Gatekeeper*)

- *Bezeichnung*: Hier muss eine eindeutige Bezeichnung für den Link angegeben werden. Unter diesem Namen steht der Link in verschiedenen anderen Dialogen zur Verfügung.
- *Kommentar*: Hier kann ein Kommentartext zu diesem Link angegeben werden.
- *Typ*: Hier wird der genaue Typ des Links angegeben. Abhängig davon werden weitere Felder in diesem Dialog sichtbar bzw. unsichtbar.
- *Verbindungsaufbau*: Bei Verbindungen, für die eine Einwahl stattfindet oder die eine Einwahl annehmen können, wird in diesem Feld ausgewählt, wie genau die Einwahl erfolgen soll:

  Immer bedeutet, dass der Link beim Aktivieren der Konfiguration bzw. beim (Neu-)Start des Systems sofort versuchen wird, sich auf der Gegenstelle einzuwählen. Die Verbindung besteht also quasi permanent.

  Bei Bedarf wartet mit dem Einwahlvorgang, bis wirklich Pakete vom lokalen System oder aus dem lokalen Netz zur Gegenseite übertragen werden sollen.

  Auf Einwahl warten baut selbst keine Verbindung auf, sondern wartet darauf, dass eine Gegenstelle die Verbindung aufbaut. Dies kann beispielsweise die Einwahl eines Außendienstmitarbeiters über ISDN oder über VPN sein.
- *Neustart erzwingen*: Diese Option ermöglicht einen gezielten Neustart der Verbindung, um u. U. die Erreichbarkeit des Servers zu erhöhen.
- *Uhrzeit*: Der Zeitpunkt, zu dem die entsprechende Verbindung neu gestartet wird.
- *IP-Adresse des Systems*: Hier wird die lokale IP-Adresse für den

Link angegeben. Bleibt das Feld leer, versucht das System, eine dynamische IP-Adresse per PPP oder DHCP zu beziehen. Sollen mehrere IP-Adressen auf einen Netzwerkanschluss zugewiesen werden (IP-Alias), muss für jede IP-Adresse ein eigener Link angelegt werden. Dabei wird jedes Mal die gleiche Schnittstelle angegeben.

Ist der Link vom Typ *auf Einwahl warten* und bleibt das Feld leer, wird eine zufällig ausgewählte IP-Adresse als lokale IP-Adresse verwendet. Andernfalls wird die eingetragene IP-Adresse als lokale IP-Adresse genutzt.

- *IP-Adresse der Gegenstelle*: Hier wird die IP-Adresse der Gegenstelle angegeben. Bleibt das Feld leer, versucht das System, die Adresse der Gegenstelle automatisch zu bestimmen.
- *Benutzername*: Hier wird das Login angegeben, mit dem sich das System bei der Einwahl an der Gegenstelle authentifizieren soll.
- *Passwort*: Hier wird das zugehörige Passwort angegeben.
- *Rufnummer der Gegenstelle*: Hier wird die Telefonnummer der Gegenstelle angegeben. Eine Rufnummer im Ortsnetz sollte ohne Vorwahl eingegeben werden. Die Vorwahl wird automatisch übernommen, wenn unter *Konfiguration – Hardware* die entsprechende Option aktiviert ist.
- *MSN*: Wenn der Link ein ISDN-Interface benutzt, muss aus dieser Liste eine MSN ausgewählt werden. Die gewählte MSN wird als abgehende Rufnummer verwendet.
- *Secure MSN*: Wird auf dem Link eine Einwahl über ISDN angenommen, kann über Einträge in diesem Feld die Annahme von Verbindungen auf bestimmte Rufnummern beschränkt werden. In dem Feld können durch Leerzeichen getrennt auch mehrere MSNs eingegeben werden. Nur bei Anrufen von diesen MSNs aus wird eine Verbindung angenommen. Bleibt das Feld leer, werden alle Anrufe angenommen.

Um diese Funktion nutzen zu können, muss das anrufende System seine Rufnummer übermitteln. Um die exakt übermittelte Rufnummer zu ermitteln, kann in den Logdateien nach Einträgen gemäß folgendem Muster gesucht werden:

```
kernel: ipppX: call from 8793787 - > 12345 ignored
```

IpppX ist dabei das Interface, auf dem der Anruf einging (mit X der entsprechenden Nummer der Schnittstelle). Die Rufnummer (MSN) des Anrufers ist in diesem Beispiel 8793787, die angerufene Nummer die 12345. In diesem Fall wurde der Anruf nicht angenommen (*ignored*), eine angenommene Verbindung wird als *accepted* angezeigt.

- *Callback aktivieren*: *Callback* ist ein spezielles Verfahren, welches bei Fernwartung bzw. Remotezugriff allgemein eine höhere Sicherheit bietet. Bei Callback signalisiert das anrufende System nur seine Rufnummer, eine Verbindung wird nicht aufgebaut. Stattdessen baut nun das angerufene System seinerseits eine Verbindung zum eigentlichen Anrufer auf.

  Bei abgehenden Verbindungen wird die Gegenstelle dazu aufgefordert, zurückzurufen. Bei ankommenden Verbindungen wird hingegen die Gegenstelle zurückgerufen.
- *Callbacknummer*: Hier muss die Rufnummer hinterlegt werden, die zurückgerufen werden soll.
- *MTU*: Hier kann die maximale Paketgröße auf diesem Link eingestellt werden.

  Große Werte für die MTU verbessern den Durchsatz, da weniger Verwaltungsdaten übertragen werden. Kleine Werte für die MTU hingegen verbessern die Antwortzeiten für interaktive Anwendungen und Echtzeitdatenübertragung (etwa VoIP).

  Wird hier kein Wert eingetragen, wird abhängig von der Art des Links ein geeigneter Wert gewählt. Für Ethernet-Verbindungen wird typischerweise eine MTU von 1500 Byte verwendet.

- *SNAT/Masquerading*: SNAT und Masquerading dienen dazu, ganze Netzwerke hinter einer einzelnen IP-Adresse zu „verstecken“. Wird diese Option aktiviert, scheinen alle abgehenden Verbindungen von diesem System zu stammen und nicht vom wirklichen Absender.

  Diese Option muss aktiviert werden, wenn auf dem Internet-Link vom Provider nur eine einzelne IP-Adresse bereitgestellt wird und wenn Systeme aus dem lokalen Netz IP-Verbindungen aufbauen müssen.

  Die Unterscheidung zwischen SNAT und Masquerading erfolgt automatisch, abhängig davon, ob eine IP-Adresse für den Link angegeben wurde oder nicht.

  Hinweis: SNAT/Masquerading für Routen und VPN-Netze funktioniert nur, wenn auf dem unterliegenden Link kein Masquerading aktiviert ist.
- *Zu maskierende Netzwerke*: Wird Masquerading für *spezielle Netze* aktiviert, können in dieser Liste aus allen angelegten Netzwerken diejenigen ausgewählt werden, die maskiert werden müssen.

  Hinweis: Alle Subnetze eines ausgewählten Netzwerks werden ebenfalls maskiert.

  Wird ein Netzwerk aus der Liste ausgewählt, bedeutet das nicht automatisch, dass Daten aus diesem Netzwerk über diesen Link versendet werden können.
- *Erreichbare Netzwerke*: Hier können aus der Liste aller angelegten Netzwerken diejenigen ausgewählt werden, die über diesen Link erreichbar sind. Für jedes ausgewählte Netz wird ein Eintrag unter *Zuordnungen* angelegt.

  Bei VPN-Verbindungen muss das lokale Netz der Gegenstelle innerhalb einem der hier angegebenen Netze liegen.

Felder in diesem Dialog für Typ *DSL mit PPPoE*

(Diese Option befindet sich im Zusatzmodul *Collax Gatekeeper*)

- *Bezeichnung*: Hier muss eine eindeutige Bezeichnung für den Link angegeben werden. Unter diesem Namen steht der Link in verschiedenen anderen Dialogen zur Verfügung.
- *Kommentar*: Hier kann ein Kommentartext zu diesem Link angegeben werden.
- *Typ*: Hier wird der genaue Typ des Links angegeben. Abhängig davon werden weitere Felder in diesem Dialog sichtbar bzw. unsichtbar.
- *Verbindungsaufbau*: Bei Verbindungen, für die eine Einwahl stattfindet oder die eine Einwahl annehmen können, wird in diesem Feld ausgewählt, wie genau die Einwahl erfolgen soll:

  Immer bedeutet, dass der Link beim Aktivieren der Konfiguration bzw. beim (Neu-)Start des Systems sofort versuchen wird, sich auf der Gegenstelle einzuwählen. Die Verbindung besteht also quasi permanent.

  Bei Bedarf wartet mit dem Einwahlvorgang, bis wirklich Pakete vom lokalen System oder aus dem lokalen Netz zur Gegenseite übertragen werden sollen.
- *Neustart erzwingen*: Diese Option ermöglicht einen gezielten Neustart der Verbindung, um u. U. die Erreichbarkeit des Servers zu erhöhen. DSL-Verbindungen werden teilweise von Providerseite nach einem bestimmten Zeitintervall getrennt. Diese Option kann benutzt werden, um den Zeitpunkt der Trennung zu verschieben.
- *Uhrzeit*: Der Zeitpunkt, zu dem die entsprechende Verbindung neu gestartet wird.

7.4.3 *Zuordnung*

Unter *Zuordnung* wird die „Routingtabelle“ des V-Cubes angezeigt. Da intern Policy-Routing genutzt wird, existiert keine starre Routingtabelle. Vielmehr können zu einem Zielnetz alternative Wege (Links) bestehen, die über Prioritäten gesteuert werden.

Hinweis: Bei der Zuordnung von Links zu den Netzwerken ist zu beachten, dass auch Konfigurationen möglich sind, die ohne spezielle Einstellungen an anderen Routern im Netzwerk nicht funktionieren.

7.4.3.1 *Prioritäten*

(Dieser Dialog befindet sich unter *Netzwerk – Links – Zuordnung*)

In diesem Dialog wird die Zuordnung von Links und den jeweils erreichbaren Netzen dargestellt. Über einstellbare Prioritäten kann das Routing gesteuert werden. In diesem Dialog können neue Zuordnungen angelegt und vorhandene gelöscht werden.

Felder in diesem Dialog

- *Priorität*: In diesem Feld wird die Priorität angezeigt. Existieren zu einem Zielnetz alternative Wege, unterscheiden sich diese durch die Priorität. Dabei wird zunächst der Weg mit der höchstmöglichen Priorität verwendet. Der Vorgabewert ist 1 (höchste Priorität).
- *Netz*: Hier wird der Name des Netzwerks angezeigt.
- *Link*: Hier wird der Link angezeigt, auf dem das Netz als *erreichbar* markiert ist.
- *Typ*: Hier wird der Typ des Links angezeigt.

Aktionen für jeden Tabelleneintrag

- *Höher*: Mit dieser Aktion wird die Priorität des Links erhöht.
- *Niedriger*: Mit dieser Aktion wird die Priorität des Links verringert.
- *Löschen*: Mit dieser Aktion wird die Zuordnung gelöscht. Das Netz wird auf dem zugehörigen Link aus der Liste der *erreichbaren Netze* entfernt.

Aktionen für diesen Dialog

- *Anlegen*: Mit dieser Aktion wird eine neue Zuordnung angelegt.

7.4.3.2 *Neue Zuordnung*

(Dieser Dialog befindet sich unter *Netzwerk – Links – Zuordnung*)

Felder in diesem Dialog

- *Netzwerk*: Hier wird das Netzwerk ausgewählt, für das ein neuer Eintrag angelegt werden soll.
- *Link*: Hier wird der zugehörige Link ausgewählt, über den das Netzwerk erreichbar sein soll.

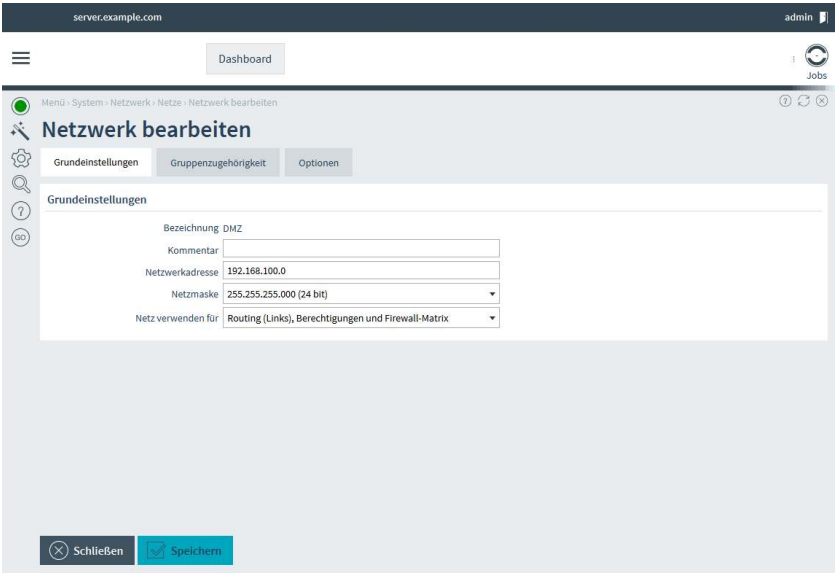
7.5 Schritt für Schritt: Internetzugang einrichten

Abhängig von der Leitungsart kann die Verbindung zum Internet auf verschiedenen Wegen erfolgen. In diesem Abschnitt werden die gängigsten Verbindungen vorgestellt.

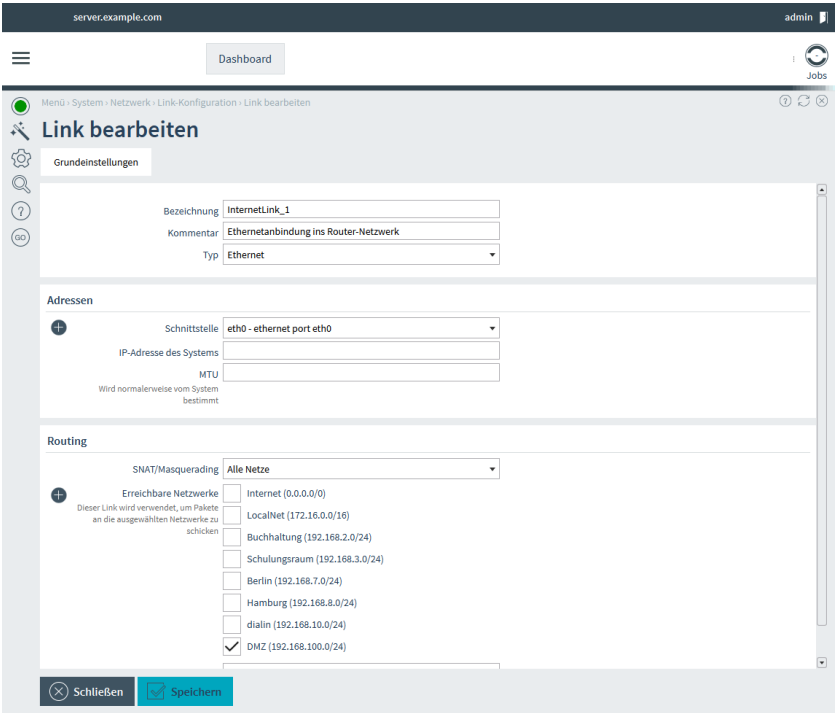
7.5.1 Zugang über einen Router

Wird vom Provider ein Router für die Internetverbindung bereitgestellt, ist die Einrichtung etwas aufwendiger. Damit der V-Cube als Trennstelle zwischen lokalem Netz und dem Internet fungieren kann, müssen beide Bereiche auf eigenen Netzwerkschnittstellen angeschlossen sein. Zunächst müssen Sie daher das Netzwerk und einen entsprechenden Link für die Verbindung zum Router anlegen. Darüber können Sie dann die Internetverbindung leiten.

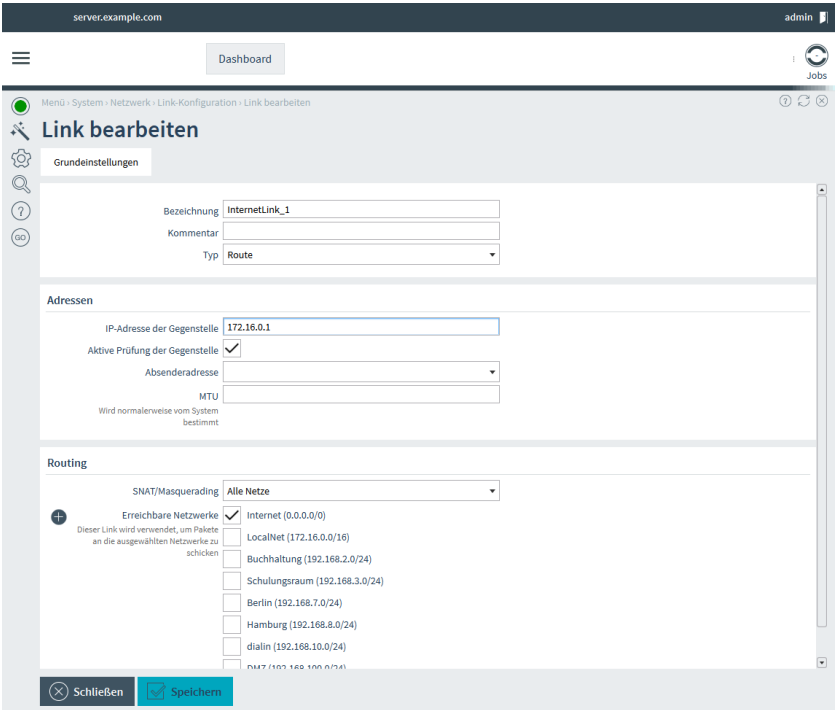
Existiert bereits eine Firewall im Netz und soll der V-Cube nur für spezielle Serverdienste (PDC, Fileserver usw.) verwendet werden, müssen Sie weder das Netz noch einen Link für einen Router anlegen. Diese Firewall stellt dann das Gateway zum Internet dar und hat eine IP-Adresse im *LocalNet*. Sie ist dadurch über den *LocalNetLink* für den V-Cube erreichbar. In diesem Fall müssen nur der *InternetLink* modifiziert und die IP-Adresse der Firewall als *Gegenstelle* eingetragen werden.



- Wechseln Sie zu *Netzwerk – Netze – Konfiguration* und legen Sie ein neues *RouterNetz* an.
- Verwenden Sie den IP-Bereich und die Netzmaske, die Ihr Provider Ihnen mitgeteilt hat.
- Speichern Sie das neu erstellte Netz.



- Wechseln Sie zu *Netzwerk – Links – Konfiguration* und legen Sie einen neuen *RouterLink* an.
- Setzen Sie den *Typ* auf Ethernet.
- Tragen Sie unter *IP-Adresse* die IP-Nummer für Ihren V-Cube ein. Diese muss zum IP-Bereich des Routernetzes gehören. Soll der V-Cube eine IP-Adresse per DHCP beziehen, lassen Sie das Feld leer.
- Wählen Sie unter *Schnittstelle* das Netzwerkinterface aus, an dem der Router angeschlossen ist.
- *SNAT/Masquerading* kann deaktiviert bleiben, da nur der V-Cube selbst Datenpakete zum Router schicken wird.
- Unter *Erreichbare Netze* wählen Sie das *RouterNetz* aus.
- Speichern Sie das neu erstellte Netz.



- Bearbeiten Sie unter *Netzwerk – Links – Konfiguration* den aus der Grundeinstellung vorhandenen *InternetLink*.
- Ändern Sie die Einstellung von *Typ* auf *Route*.
- Unter *IP-Adresse der Gegenstelle* geben Sie die IP-Adresse des Routers ein.
- Die *MTU* kann auf 1500 eingestellt bleiben.
- Ändern Sie die Einstellung von *SNAT/Masquerading* auf *Alle Netze*, wenn Sie im lokalen Netz private IP-Adressen verwenden und von dort auf das Internet zugreifen möchten.
- Unter *Erreichbare Netze* wählen Sie das *Internet* aus. Nur dieses Netz befindet sich hinter dem Router.
- Speichern Sie Ihre Änderungen.

8 Hardwarekonfiguration

8.1 Grundlagen

In diesem Kapitel werden Schnittstellen des V-Cubes behandelt, über die Verbindungen zur Außenwelt hergestellt werden können. Zu diesem Zweck können serielle Schnittstellen, ISDN-Karten und Netzwerkschnittstellen konfiguriert werden.

Das Linux-System zählt Schnittstellen beginnend mit Null. Daher wird bei seriellen Schnitstellen „COM 1“ als „ttyS0“, bei mehreren ISDN- oder Netzwerkkarten die jeweils erste Schnittstelle mit Null bezeichnet: „isdn0“ bzw. „eth0“.

8.1.1 Netzwerk-Bridges

Durch eine Bridge werden mehrere Ethernet-Ports zu einer Art Switch zusammengeschaltet. Dadurch erscheinen sie nach außen wie ein einziges Netzwerksegment (eine so genannte „Broadcast-Domain“). Dabei werden nur diejenigen Pakete auf einen Port der Bridge kopiert, deren Ziel-Adresse an diesem Port erreichbar ist.

Eine Bridge lernt die MAC-Adressen innerhalb eines jeden Teilnetzes, indem sie diese intern in einer Tabelle speichert. Anhand dieser Tabelle werden die Datenpakete in das entsprechende Ziel-Netzwerksegment weitergeleitet. Wird ein System auf ein anderes Netzwerksegment umgesteckt, dauert es eine gewisse Zeit, bis die Bridge den Umzug erkennt und die Adresse „neu lernt“.

Durch die Verwendung von Switches und Bridges kann nicht grundsätzlich ausgeschlossen werden, dass eine Verbindungsleitung

redundant geschaltet wird, so dass eine Schleife entsteht. Dies führt zu duplizierten Datenpaketen und damit zu Fehlfunktionen und Geschwindigkeitseinbußen im Netzwerk. Um dennoch solche Redundanz für eine höhere Funktionssicherheit nutzen zu können, wird das „Spanning Tree Protocol“ (STP) benötigt.

Bei aktiviertem STP ermitteln innerhalb einer Netzwerkumgebung alle Bridges abhängig von ihrer Priorität und der jeweiligen Mac-Adresse eine „Root-Bridge“. Diese Root-Bridge prüft nun, welche weiteren Bridges vorhanden sind und ob es redundante Pfade gibt. Letztere werden eliminiert, indem die entsprechenden Ports an den betroffenen Bridges deaktiviert werden. Auf diese Weise wird ist ein störungsfreier Betrieb des Netzwerks möglich.

Im laufenden Betrieb werden von der Root-Bridge aus Pakete zur Überwachung ins Netz geschickt, die von untergeordneten Bridges dupliziert werden. Dadurch können Störungen bzw. Änderungen im Netzwerk erkannt werden. In solchen Fällen findet eine Reorganisation des Netzes statt. In dieser Zeit sind im gesamten Netz nur noch STP-Pakete zulässig, jeder andere Netzwerkverkehr wird unterbunden.

Im V-Cube können mehrere Netzwerkschnittstellen zu einer Bridge zusammengefasst werden. Zwischen diesen Schnittstellen verhält sich der V-Cube transparant, d. h., es werden keine Firewallregeln angewendet.

8.1.2 VLAN-Routing

Mit VLANs (Virtual Local Area Networks) lässt sich ein lokales Netzwerk in mehrere virtuelle, voneinander getrennte Netze unterteilen. VLAN ist teilweise als IEEE 802.1q standardisiert.

Damit VLAN eingesetzt werden kann, muss ein Switch mit ent-

sprechender Unterstützung vorhanden sein. Jedem VLAN wird eine eigene Nummer zugewiesen, die den Headern der Datenpakete hinzugefügt wird. Derart markierte Datenpakete werden von einem entsprechenden Switch nur auf die Ports weitergeleitet, die dem VLAN zugeordnet sind. Ist am Zielport ein Endgerät angeschlossen, wird die VLAN-Markierung entfernt. Die Teilnehmer eines VLANs sind so an einem eigenen, virtuellen Switch angeschlossen. Broadcast-Pakete werden vom Switch nicht in andere VLANs weitergeleitet.

Um mehrere Switches miteinander zu verbinden, wird am Switch der Uplink-Port als „Trunked Port“ eingestellt. Auf solchen Ports werden ausgehenden Paketen entsprechende VLAN-Markierungen hinzugefügt. Werden derart markierte Pakete über einen Switch ohne VLAN-Unterstützung an ein Endgerät zugestellt, enthält der Paketheader noch die VLAN-Information. Ein Endgerät ohne VLAN-Unterstützung erkennt das Paket als ungültig und verwirft es.

Der V-Cube unterstützt VLAN-Technik. Mit einem entsprechenden Switch können mehrere virtuelle Netzwerksegmente angesteuert werden.

8.1.3 Schnittstellen-Bonding

Durch das Zusammenschalten von mehreren Ethernet-Verbindungen können Zuverlässigkeit und Durchsatz des Systems erhöht werden. Dazu ist jedoch die Unterstützung durch den eingesetzten Switch erforderlich. Der Switch muss „Bonding“, „EtherChannel“ bzw. „Trunking“ unterstützen.

Eine (unvollständige) Liste von Switches mit der erforderlichen Unterstützung:

- Bay Networks
- Cabletron SmartSwitch
- Cisco Catalyst 5000 series

- Extreme Summit Switches
- Foundry FastIron Switches
- HP Advancestack Switch 800T
- Plaintree WaveSwitch
- Prominet P550 Cajun Switch

Je nach Switch und Einstellung werden entweder mehrere Leitungen gebündelt verwendet („Load Balancing“), oder es wird nur eine genutzt, die dann im Fehlerfall umgeschaltet wird („Failover“).

Folgende Einstellungen werden vom V-Cube unterstützt:

- *Round Robin* – Es wird immer die nächste verfügbare physikalische Schnittstelle benutzt. Diese Arbeitsweise erreicht den höchsten Durchsatz, erfordert aber die Unterstützung des Switches.
- *XOR* – Jede Gegenstelle wird immer über dieselbe physikalische Schnittstelle angesprochen. Einige Switches verwenden dieses Verfahren, es wird aber nur ein geringer Durchsatz erreicht. Es ist nicht erforderlich, zur Kommunikation mit diesen Switches auch XOR zu benutzen, jedoch ist auch für diese Arbeitsweise die Unterstützung des Switches erforderlich.
- *Active Backup* – Diese Arbeitsweise erfordert keine Unterstützung durch die Gegenstelle. Es wird aber kein erhöhter Durchsatz, sondern nur erhöhte Zuverlässigkeit erreicht. Zu jedem Zeitpunkt ist nur ein Link aktiv. Zusätzlich zur MII-Link-Status-Überwachung kann in diesem Modus auch eine aktive Überprüfung des Links durch ARP-Anfragen erfolgen.
- *Broadcast* – In dieser Arbeitsweise werden alle Pakete auf allen Schnittstellen gesendet. Dieser Modus zielt auf Fehlertoleranz, kann aber auch z. B. für den Einsatz eines IDS nützlich sein.

8.2 GUI-Referenz: *Hardware*

(Dieser Dialog befindet sich unter *Hardware – Systemgeräte & Komponenten*)

In diesen Dialogen werden die Hardware-Ressourcen des Systems angezeigt. Einzelne Komponenten können bearbeitet werden.

Einige der angezeigten Ressourcen können nicht verändert werden, z. B. die vorhandenen Ethernet-Ports. Alle Hardwarekomponenten werden beim Starten des Systems erkannt und in die Oberfläche eingefügt. Dies gilt auch für „hotplug-fähige“ Komponenten wie USB-ISDN-Adapter.

Andere Ressourcen wie etwa VLANs oder MSNs müssen hingegen manuell eingerichtet werden. Hier ist keine automatische Erkennung möglich.

8.2.1 *Systemgeräte & Komponenten*

In diesem Dialog werden alle relevanten Komponenten des Systems angezeigt.

8.2.1.1 Tab *System*, Abschnitt *CPU*

In diesem Abschnitt werden Informationen über den Prozessor des Systems angezeigt.

Felder in diesem Abschnitt

- *Hersteller*: Hier wird der Code des CPU-Herstellers angezeigt.
- *Modell*: Hier wird die Modellbezeichnung der CPU angezeigt.
- *Geschwindigkeit*: Hier wird die ermittelte Taktrate der CPU angezeigt.
- *Cachegröße*: Hier wird Größe des Cachespeichers der CPU angezeigt.

8.2.1.2 Tab *RAM*, Abschnitt *RAM*

Felder in diesem Abschnitt

- *RAM gesamt*: Hier wird die Gesamtgröße des erkannten Hauptspeichers (RAM) angezeigt.
- *RAM frei*: Hier wird die Größe des aktuell verfügbaren freien Hauptspeichers angezeigt.
- *Swap gesamt*: Hier wird die Gesamtgröße des Auslagerungsspeichers angezeigt.
- *Swap frei*: Hier wird die Größe des aktuell verfügbaren freien Auslagerungsspeichers angezeigt.

8.2.1.3 Tab *Serielle Schnittstellen*

Spalten in der Tabelle

- *Art*: Die Art der Schnittstelle.
- *Name*: Der Name der Schnittstelle.
- *Kommentar*: Ein Kommentar zu dieser Schnittstelle.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion wird die Konfiguration der seriellen Schnittstelle bearbeitet.

8.2.1.4 Tab *IPMI*

IPMI ist eine integrierte Management-Technik, mit der die Stromversorgung und der Status eines Systems kontrolliert werden können. Damit IPMI auf einem V-Cube genutzt werden kann, muss entsprechende Hardware vorhanden sein.

Spalten in der Tabelle

- *Art*: Die Art der Schnittstelle.
- *Name*: Der Name der Schnittstelle.
- *Kommentar*: Ein Kommentar zu dieser Schnittstelle.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion wird die Funktion der Schnittstelle festgelegt.

8.2.2 *Serielle Schnittstelle bearbeiten*

(Dieser Dialog befindet sich unter *Hardware – Systemgeräte & Komponenten*)

In diesem Dialog werden die seriellen Schnittstellen konfiguriert.

Um die Änderungen vollständig zu aktivieren, muss ein Reboot des Systems durchgeführt werden.

8.2.2.1 Felder in diesem Dialog

- *Schnittstelle*: In diesem Feld wird der Name der Schnittstelle angezeigt. Die interne Nummerierung beginnt bei Null, d. h., die Schnittstelle *ttyS0* entspricht *COM 1*.
- *Verwendung*: Hier wird eingestellt, zu welchem Zweck die Schnittstelle verwendet werden soll.

  Bei der Auswahl von *serielle Konsole* wird auf der seriellen Schnittstelle eine Konsole bereitgestellt. Mit Hilfe eines Terminalprogramms kann dann auch ohne Netzwerk oder Bildschirm / Tastatur auf das System zugegriffen werden.

  Mit der Einstellung *Modem* müssen verschiedene Modem-Parameter gesetzt werden. Dann steht ein analoges Modem zur Einwahl bzw. zum Faxbetrieb zur Verfügung.

  Mit der Einstellung *Sonstiges* wird keine Konfiguration der Schnittstelle durchgeführt. Die Schnittstelle steht dann für andere Programme zur Verfügung, die die Konfiguration vornehmen (z. B. für den USV-Dienst oder einen Zeitsignalempfänger).

  Hinweis: Wird keine serielle Schnittstelle auf *Sonstiges* eingestellt, kann bei der USV-Konfiguration usw. keine Schnittstelle ausgewählt werden.
- *Übertragungsrate*: Hier wird die Übertragungsgeschwindigkeit für die Schnittstelle eingestellt. Wird an diesem Port ein Modem angeschlossen, sollte hier ein Wert eingestellt werden, der mindestens so hoch wie die maximale Übertragungsrate des Modems ist. Normalerweise wird ein Wert eingestellt, der doppelt so groß ist, damit der Datenpuffer im Modem immer gefüllt ist.
- *Bits*: Hier wird die Anzahl der zur Datenübertragung genutzten Bits angegeben. Üblich ist der Wert 8, spezielle Gegenstellen könnten den Wert 7 benötigen.
- *Parität*: Hier wird angegeben, ob *Gerade* (even) oder *Ungerade*

Parität (odd parity) genutzt wird. Dabei handelt es sich um einfache Verfahren zur Erkennung von Übertragungsfehlern. Abhängig von der Einstellung wird im Paritätsbit signalisiert, ob die Anzahl der auf logisch Eins gesetzten Datenbits gerade oder ungerade ist. Mit der Einstellung *Keine* wird auf das Paritätsbit verzichtet.

- *Analoge Rufnummer*: Hier wird die Rufnummer des Analogmodems angegeben. Diese Rufnummer wird beispielsweise vom Fax-Dienst übermittelt. Die Nummer sollte im Format *+49xxxxxxxxx* eingegeben werden.
- *Allgemeine Amtsholung benutzen*: Diese Option muss aktiviert werden, wenn die allgemeine Einstellung zur Amtsholung für dieses Modem verwendet werden soll.
- *Wahlverfahren*: Hier wird eingestellt, ob das Modem mit dem Mehrfrequenzverfahren oder mit Impulswahl arbeiten soll.

8.2.3 *IPMI-Einstellungen bearbeiten*

(Dieser Dialog befindet sich unter *Hardware – Systemgeräte & Komponenten*)

8.2.3.1 Felder in diesem Abschnitt

- *Medientyp*: Der Medientyp ist die Art des Kanals, sichtbar ist derzeit nur 802.3 LAN. Weitere mögliche Kanäle bei IPMI wären etwa „SMBus“ oder „Seriell“.
- *Protokoll*: Als IPMI-Protokoll wird „IPMB-1.0“ verwendet.
- *LAN-Zugriff erlauben*: Mit dieser Option wird der Zugriff auf den LAN-Kanal aktiviert.

- *Schnittstelle*: Ein LAN-Kanal benötigt eine definierte Schnittstelle für den IPMI-Zugriff. Diese wird hier ausgewählt.
- *IP-Adresse*: Hier wird die IP-Adresse konfiguriert, die für den LAN-Zugriff verwendet werden soll. Diese IP-Adresse darf nicht anderweitig verwendet werden.
- *Netzmaske*: Hier wird die zugehörige Netzmaske eingegeben.
- *MAC-Adresse des Gateways*: Soll aus entfernten Netzen der Zugriff über IPMI möglich sein, muss hier die MAC-Adresse des Gateways angegeben werden.
- *IP-Adresse des Gateways*: In diesem Feld wird entsprechend die IP-Adresse des Gateways eingegeben.
- *SNMP-Community*: In diesem Feld wird der „Community String" für die Authentifizierung bei SNMP angegeben.
- *Berechtigte Gruppen*: Alle aktivierten Gruppen erhalten Zugriff auf IPMI.

8.2.4 *Ethernet-Protokolle*

In diesem Formular können verschiedene Einstellungen vorgenommen oder bestimmte Dienste zu Ethernet aktiviert werden. Die Einstellungen werden generell gesetzt und sind somit unabhängig von den verwendeten lokalen Schnittstellen.

8.2.4.1 Abschnitt *STP/RSTP*

Felder in diesem Abschnitt

- *Verwende RSTP anstelle von STP*: Diese Option aktiviert einen Dienst für das Rapid Spanning Tree Protocol. Als Weiterentwicklung von STP beschleunigt das RSTP einerseits die Umstellung

auf alternative Netzwerkpfade. Zudem bleiben zum Zeitpunkt der Umstellung alle noch funktionierenden Pfade aktiv.

8.2.4.2 Abschnitt *GVRP*

Felder in diesem Abschnitt

- *VLANs mit GVRP registrieren*: Mit dem Generic Attribute Registration Protocol für VLAN (GVRP) können VLAN-Ports vom Server direkt am angeschlossenen Switch generiert werden. Der Switch muss dieses Protokoll unterstützen.

8.2.4.3 Abschnitt *LLDP*

Felder in diesem Abschnitt

- *LLDP aktivieren*: Hier kann das Link Layer Discovery Protocol (LLDP) aktiviert werden. Dieses Protokoll sendet und empfängt Informationen über die direkte Netzwerknachbarschaft.

Abschnitt *Andere Protokolle* ...

Felder in diesem Abschnitt

- *Aktiviere CDP (Cisco)*: Aktiviert CDP (Cisco).
- *Aktiviere FDP (Foundry)*: Aktiviert FDP (Foundry).
- *Aktiviere SONMP (Bay/Nortel/SynOptics)*: Aktiviert SONMP (Bay/Nortel/SynOptics).
- *Aktiviere EDP (Extreme)*: Aktiviert EDP (Extreme).

8.2.4.4 Aktionen für dieses Formular

- *Abbrechen*: Diese Aktion beendet den Dialog. Die Änderungen werden verworfen.
- *Speichern*: Diese Aktion beendet den Dialog. Die Änderungen werden gespeichert.

8.2.5 *Netzwerkschnittstellen*

(Dieser Dialog befindet sich unter *Systembetrieb – Hardware – Netzwerkschnittstellen*)

8.2.5.1 GUI-Referenz: *Netzwerkschnittstellen*
Spalten in der Tabelle

- *Art*: Die Art der Schnittstelle.
- *Name*: Der Name der Schnittstelle.
- *Kommentar*: Ein Kommentar zu dieser Schnittstelle.
- *Verwendung*: Anzeige, wo das Ethernet-Device verwendet wird.
- *Vorhanden*: Zeigt an, ob das Gerät vorhanden ist.

Aktionen für jeden Tabelleneintrag

- *Bridge bearbeiten*: Mit dieser Aktion wird die Konfiguration der Bridge bearbeitet.
- *Bridge löschen*: Mit dieser Aktion wird eine angelegte Bridge-Konfiguration gelöscht.
- *MacVLAN bearbeiten*: Hier kann ein auf MAC-Adressen bezogenes VLAN bearbeitet werden.

- *MacVLAN löschen*: Hier kann ein auf MAC-Adressen bezogenes VLAN gelöscht werden.
- *VLAN bearbeiten*: Mit dieser Aktion wird das gewählte VLAN bearbeitet.
- *VLAN löschen*: Mit dieser Aktion wird die Konfiguration des VLAN-Ports gelöscht. Dies ist nur möglich, wenn der VLAN-Port in keinem Link und in keiner Bridge mehr verwendet wird.
- *Bonding bearbeiten*: Mit dieser Aktion können die Einstellungen einer Bonding-Konfiguration bearbeitet werden.
- *Bonding löschen*: Mit dieser Aktion wird eine angelegte Bonding-Konfiguration gelöscht.
- *Ethernet bearbeiten*: Mit dieser Aktion können Einstellungen für die Ethernet-Schnittstellen vorgenommen werden.
- *Bridge hinzufügen*: Mit dieser Aktion können mehrere Ethernet-Schnittstellen zu einer Bridge zusammengeschaltet werden.

  Auch VLAN-Ports können mit in die Bridge aufgenommen werden. Dies sollte jedoch nicht mit zwei VLAN-Ports geschehen, die auf demselben physikalischen Ethernet-Port liegen. Dadurch würde das VLAN unbrauchbar.
- *VLAN-Port hinzufügen*: Mit dieser Aktion wird eine Ethernet-Schnittstelle für ein virtuelles LAN (VLAN) eingerichtet. Diese Schnittstelle kann danach nicht mehr für andere Zwecke benutzt werden. Es können jedoch mehrere VLAN-Ports auf derselben Ethernet-Schnittstelle eingerichtet werden.

  Hinweis: Die übrige Netzwerkinfrastruktur muss ebenfalls VLAN-fähig sein. Der auf dem Switch genutzte Ethernet-Port muss entsprechend konfiguriert sein.

  VLANs haben nichts (oder fast nichts) mit virtuellen Interfaces zu tun. Soll eine weitere IP-Adresse für den V-Cube vergeben werden, muss dazu nur ein weiterer Link auf dem Ethernet-Port angelegt werden.
- *MacVLAN-Port hinzufügen*:

- *Port-Bonding hinzufügen*: Mit dieser Aktion können mehrere Ethernet-Schnittstellen gebündelt werden, um dadurch gesteigerten Durchsatz und höhere Zuverlässigkeit zu erreichen.

8.2.5.2 *Ethernet-Einstellungen*

(Dieser Dialog befindet sich unter *Hardware – Netzwerkschnittstellen*)

In diesem Dialog wird eine einzelner Ethernet-Port bearbeitet.

Felder in diesem Dialog

- *Name*: Hier wird der Name des Ethernet-Ports angezeigt.
- *Jumbo-Frames verwenden*: Um Protokoll-Overhead zu minimieren kann es sinnvoll sein, größere Paketlängen als 1518 Bytes im Netzwerkverkehr auf dieser Schnittstelle zu verwenden. Voraussetzung für die Verwendung von Jumbo Frames, ist die Fähigkeit beteiligter Netzwerkgeräte ebenso mit Jumbo Frames umgehen zu können.
- *Kein GVRP auf diesem Port*: Verhindert, dass GVRP auf dem Port benutzt wird.

8.2.5.3 *VLAN-Port bearbeiten*

(Dieser Dialog befindet sich unter *Hardware – Netzwerkschnittstellen*)

In diesem Dialog wird ein einzelner VLAN-Port bearbeitet.

Auf einem physikalischen Ethernet-Port können ein oder mehrere VLANs konfiguriert werden. Das VLAN erscheint dann als virtueller

Port in der Hardwarekonfiguration und an allen Stellen, an denen ein Ethernet-Port ausgewählt werden kann (zum Beispiel in der Link-Konfiguration).

Ein physikalischer Ethernet-Port, auf dem ein VLAN konfiguriert wurde, kann nicht mehr für andere Zwecke verwendet werden. Er kann beispielsweise nicht mehr in eine Bridge integriert werden.

Felder in diesem Dialog

- *Ethernet-Port*: Hier wird die Netzwerkschnittstelle ausgewählt.
- *Jumbo-Frames verwenden*: Um Protokoll-Overhead zu minimieren kann es sinnvoll sein, größere Paketlängen als 1518 Bytes im Netzwerkverkehr auf dieser Schnittstelle zu verwenden. Voraussetzung für die Verwendung von Jumbo Frames, ist die Fähigkeit beteiligter Netzwerkgeräte ebenso mit Jumbo Frames umgehen zu können.
- *VLAN-Tag*: In diesem Feld wird das VLAN-Tag angegeben.

8.2.5.4 *MacVLAN-Port hinzufügen*

(Dieser Dialog befindet sich unter *Hardware – Ethernet*)

In diesem Dialog wird ein einzelner VLAN-Port hinzugefügt, dem eine Mac-Adresse zugewiesen werden kann.

Ein physikalischer Ethernet-Port, auf dem ein VLAN konfiguriert wurde, kann nicht mehr für andere Zwecke verwendet werden. Er kann beispielsweise nicht mehr in eine Bridge integriert werden.

Felder in diesem Dialog

- *Ethernet-Port*: Hier wird die Netzwerkschnittstelle ausgewählt.
- *Jumbo-Frames verwenden*: Um Protokoll-Overhead im Gigabitnetzwerk zu minimieren kann es sinnvoll sein, größere Paketlängen als 1518 Bytes im Netzwerkverkehr auf dieser Schnittstelle zu verwenden. Voraussetzung für die Verwendung von Jumbo Frames, ist die Fähigkeit beteiligter Netzwerkgeräte ebenso mit Jumbo Frames umgehen zu können.
- *MAC-Adresse*: Hier wird eine MAC-Adresse eingetragen, die von keinem anderen Gerät verwendet wird.

Aktionen für dieses Formular

- *Zufällige MAC*: Mit dieser Aktion wird eine MAC-Adresse generiert und in das Feld *MAC-Adresse* eingetragen.

8.2.5.5 *MacVLAN-Port bearbeiten*

Felder in diesem Formular

- *Ethernet-Port*: Hier wird die Netzwerkschnittstelle angezeigt.
- *Jumbo-Frames verwenden*: Um Protokoll-Overhead im Gigabitnetzwerk zu minimieren kann es sinnvoll sein, größere Paketlängen als 1518 Bytes im Netzwerkverkehr auf dieser Schnittstelle zu verwenden. Voraussetzung für die Verwendung von Jumbo Frames, ist die Fähigkeit beteiligter Netzwerkgeräte ebenso mit Jumbo Frames umgehen zu können.
- *MAC-Adresse*: Hier wird eine MAC-Adresse eingetragen, die von keinem anderen Gerät verwendet wird.

Aktionen für dieses Formular

- *Zufällige MAC*: Mit dieser Aktion wird eine MAC-Adresse generiert und in das Feld *MAC-Adresse* eingetragen.

Aktionen für dieses Formular

- *Abbrechen*: Diese Aktion führt zurück zur Übersicht. Die Änderungen werden verworfen.
- *Speichern*: Bearbeiten der Mac-VLAN-Konfiguration beenden. Die Änderungen werden gespeichert.

8.2.5.6 *Bridge bearbeiten*

(Dieser Dialog befindet sich unter *Hardware – Netzwerkschnittstellen*)

In diesem Dialog wird die Konfiguration einer Ethernet-Bridge vorgenommen.

Felder in diesem Dialog

- *Name*: Hier wird der Name der Bridge angezeigt. Wird eine neue Bridge angelegt, ist das Feld leer. Der Name wird automatisch erzeugt.
- *Kommentar*: Hier wird eine erweiterte Information eingefügt.
- *STP-Protokoll aktivieren*: Das „Spanning Tree Protokoll“ STP dient dazu, bei Konfigurationen mit mehreren Bridges (oder Switches) immer nur einen Datenpfad zwischen zwei Geräten aufzubauen. Mittels STP werden daher Routingschleifen verhindert.

  Wenn zwischen einzelnen Geräten mehrere Datenpfade kon-

figuriert werden, kann STP die Ausfallsicherheit erhöhen. STP aktiviert im Fehlerfall einen redundanten Pfad.

STP kann deaktiviert werden, wenn es keine anderen Bridges im Netzwerk oder keine redundanten Pfade gibt.

- *Priorität*: Wird STP verwendet, kann hier die Priorität der Bridge festgelegt werden. Gibt es mehrere Bridges im Netzwerk, wird die Bridge mit dem niedrigsten Prioritätswert zur „root"-Bridge. Bei mehreren Bridges mit gleicher Priorität wird zusätzlich die MAC-Adresse mit herangezogen, um die Root-Bridge festzulegen.
- *Ageing-Zeit (s)*: Dieser Parameter gibt an, wie lange die MAC-Adressen gespeichert werden. Diese Zeit wird nach dem letzten empfangenen Paket eines Systems heruntergezählt.

  Wird ein System an einen anderen Port der Bridge angeschlossen, dauert es mindestens so lange wie angegeben, bis es im Netzwerk von anderen Systemen erreicht werden kann.
- *Ethernet-Ports*: In dieser Liste werden die Ethernet-Ports für die Bridge aktiviert. Es stehen nur solche Ports zur Auswahl, die entweder schon für die Bridge verwendet oder bisher nicht konfiguriert wurden.

8.2.5.7 *Gebündelte Ethernet-Schnittstellen bearbeiten*

(Dieser Dialog befindet sich unter *Hardware – Netzwerkschnittstellen*)

Durch das Zusammenschalten („Bundling") von Ethernet-Leitungen können Zuverlässigkeit und Durchsatz erhöht werden. Dazu ist Unterstützung durch den eingesetzten Switch erforderlich. Der Switch muss „EtherChannel" oder „Trunking" unterstützen.

Eine (unvollständige) Liste von Switches mit der erforderlichen Unterstützung:

Bay Networks

Cabletron SmartSwitch
Cisco Catalyst 5000 series
Extreme Summit Switches
Foundry FastIron Switches
HP Advancestack Switch 800T
Plaintree WaveSwitch
Prominet P550 Cajun Switch

Felder in diesem Dialog

- *Name*: Der Name der Schnittstelle.
- *Arbeitsweise*: Hier wird die Arbeitsweise der gebündelten Schnittstellen festgelegt. Sämtliche Konfigurationen benutzen die MII-Link-Status-Überwachung.

  Möglich sind:

  Active Backup – Diese Arbeitsweise erfordert keine Unterstützung der Gegenstelle, erreicht aber keinen erhöhten Durchsatz, sondern nur erhöhte Zuverlässigkeit. Zu jedem Zeitpunkt ist nur ein Link aktiv. Zusätzlich zur MII-Link-Status-Überwachung kann in diesem Modus auch eine aktive Überprüfung des Links durch ARP-Anfragen erfolgen.

  Broadcast – In dieser Arbeitsweise werden alle Pakete auf allen Schnittstellen gesendet. Dieser Modus zielt auf Fehlertoleranz, kann aber auch z. B. für den Einsatz eines IDS nützlich sein.

  Round Robin – Es wird immer die nächste verfügbare physikalische Schnittstelle benutzt, um Pakete zu versenden. Diese Arbeitsweise ermöglicht Load Balancing und Ausfallsicherheit, erfordert aber die Unterstützung des Switches.

  XOR – Jede Gegenstelle wird immer über dieselbe physikalische Schnittstelle angesprochen. Dies ist die Arbeitsweise einiger Switches, es wird aber nur geringerer Durchsatz erreicht. Es ist

nicht erforderlich, zur Kommunikation mit diesen Switches auch XOR zu benutzen, jedoch ist auch für diese Arbeitsweise die Unterstützung des Switches erforderlich.

LACP (802.3ad) – Innerhalb der IEEE-Spezifizierung stellt das Link Aggregation Control Protocol (LACP) eine Methode zur Verfügung, um die Bündelung von mehreren physischen Anschlüssen zusammen zu kontrollieren und einen einzelnen logischen Kanal zu bilden. LACP erlaubt einem Netzwerkgerät eine automatische Aushandlung zur Bündelung von Anschlüssen indem es LACP Pakete an die Gegenstelle (direkt angeschlossenes Gerät, das auch LACP durchführt) sendet.

Adaptive Transmit Load Balancing – Ankommender Verkehr wird nur auf der aktiven Schnittstelle entgegengenommen, abgehender Netzwerkverkehr wird gemäß der gegenwärtigen Last auf jede Schnittstelle verteilt. Diese Option erfordert keine spezielle Switch-Unterstützung.

Adaptive Load Balancing – umfasst Adaptive Transmit Load Balancing inklusive Receive Load Balancing (RLB) für den IPV4-Verkehr. Diese Option erfordert keinen speziellen Switch-Unterstützung. Der Lastausgleich beim eingehenden Netzwerkverkehr wird durch die ARP-Verhandlung erreicht.

- *Verteilung nach*: Wählt die Sende-Richtlinie, um die korrekte Schnittstelle auszuwählen. Diese Option gilt für die XOR- und LACP-Arbeitsweise. Folgende Einstellungswerte sind möglich:

  Schicht 2 (MAC-Adressen) – Dieser Algorithmus lenkt den Netzwerkverkehr zu einer bestimmten Gegenstelle immer über dieselbe Schnittstelle.

  Schicht 2 und 3 (MAC- und IP-Adressen) – Arbeitet wie die Schicht 2-Verteilung, sorgt aber zusätzlich für ausgeglichenere Verteilung des Netzwerkverkehrs. Das trifft gerade in Umgebungen zu, in denen ein IP-Gateway eingesetzt wird.

Schicht 3 und 4 (MAC-, IP-Adressen und UDP/TCP) – Diese Richtlinie betrachtet höhere Protokollschichten um die Sendeschnittstellen auszuwählen. Fragmentierte Pakete werden ignoriert.

- *ARP-Überprüfung*: Hier wird die aktive Überprüfung des Links durch ARP-Anfragen aktiviert.
- *Überprüfungsintervall (in ms)*: Hier wird das Intervall festgelegt, in dem eine Überprüfung stattfinden soll. Die Zeit wird in Millisekunden (ms) angegeben, der kleinste gültige Wert ist 100.
- *Up-Verzögerung (in ms)*: Hier wird die Verzögerung eingestellt, die eingehalten werden soll, bevor eine Schnittstelle wieder verfügbar gemacht wird. Die Zeit wird in Millisekunden (ms) angegeben.
- *Down-Verzögerung (in ms)*: Hier wird die Verzögerung eingestellt die eingehalten werden soll, bevor eine Schnittstelle heruntergefahren wird. Die Zeit wird in Millisekunden (ms) angegeben.
- *Carrier-Auswertung des Treibers benutzen*: Gibt an, ob miimon MII- oder ETHTOOL-ioctls statt netif_carrier_ok () verwenden werden soll, um den Status zu bestimmen.
- *IP*: Hier wird die IP-Adresse angegeben, die für die ARP-Anfragen benutzt wird. Werden für diese IP-Adresse keine ARP-Anfragen beantwortet, wird der Link als fehlerhaft eingestuft.
- *Ethernet-Ports*: In dieser Liste werden die Ethernet-Schnittstellen ausgewählt, die gebündelt werden. Es werden nur die Ports angezeigt, die unkonfiguriert sind.
- *Primärer Port*: Hier wird die primäre Schnittstelle angegeben. Diese wird bevorzugt verwendet. Erst wenn diese Schnittstelle gestört ist, wird auf eine der anderen umgeschaltet. Sobald die primäre Schnittstelle wieder verfügbar ist, wird auf diese zurückgeschaltet.

Ein Anwendungsbeispiel ist die Failover-Bündelung einer

1000 MBit- und einer oder mehrerer 100 MBit-Schnittstellen, bei der bevorzugt die 1000 MBit-Schnittstelle benutzt werden soll.

8.2.5.8 *Gebündelte Ethernet-Schnittstellen bearbeiten*

(Dieser Dialog befindet sich unter *Hardware – Netzwerkschnittstellen*)

Hier werden die Einstellungen für gebündelte Ethernetports festgelegt. Diese können verwendet werden, um Zuverlässigkeit und Durchsatz zu erhöhen. Unter Umständen ist die Unterstützung des Switches erforderlich (genannt EtherChannel oder Trunking). Weitere Informationen finden sich unter „Arbeitsweise“.

Eine (unvollständige) Liste von Switches mit der erforderlichen Unterstützung:

Bay Networks
Cabletron SmartSwitch
Cisco Catalyst 5000 series
Extreme Summit Switches
Foundry FastIron Switches
HP Advancestack Switch 800T
Plaintree WaveSwitch
Prominet P550 Cajun Switch

Felder in diesem Dialog

- *Name*: Der Name der Schnittstelle.
- *Arbeitsweise*: Hier wird die Arbeitsweise der gebündelten Schnittstellen festgelegt. Sämtliche Arten benutzen MII-Link-Status-Überwachung.

  Möglich sind:

Active Backup – Diese Arbeitsweise erfordert keine Unterstützung der Gegenstelle, erreicht aber keinen erhöhten Durchsatz, sondern nur erhöhte Zuverlässigkeit. Zu jedem Zeitpunkt ist nur ein Link aktiv. Zusätzlich zur MII-Link-Status-Überwachung kann in diesem Modus auch eine aktive Überprüfung des Links durch ARP-Anfragen erfolgen.

Broadcast – In dieser Arbeitsweise werden alle Pakete auf allen Schnittstellen gesendet. Dieser Modus zielt auf Fehlertoleranz, kann aber auch z. B. für den Einsatz eines IDS nützlich sein.

Round Robin – Es wird immer die nächste verfügbare physikalische Schnittstelle benutzt, um Pakete zu versenden. Diese Arbeitsweise ermöglicht Load Balancing und Ausfallsicherheit, erfordert aber die Unterstützung des Switches.

XOR – Jede Gegenstelle wird immer über dieselbe physikalische Schnittstelle angesprochen. Dies ist die Arbeitsweise einiger Switches, es wird aber nur geringerer Durchsatz erreicht. Es ist nicht erforderlich, zur Kommunikation mit diesen Switches auch XOR zu benutzen, jedoch ist auch für diese Arbeitsweise die Unterstützung des Switches erforderlich.

LACP (802.3ad) – Innerhalb der IEEE Spezifizierung stellt das Link Aggregation Control Protocol (LACP) eine Methode zur Verfügung, die Bündelung von mehreren physischen Anschlüssen zusammen zu kontrollieren, um einen einzelnen logischen Kanal zu bilden. LACP erlaubt einem Netzwerkgerät eine automatische Aushandlung zur Bündelung von Anschlüssen indem es LACP Pakete an die Gegenstelle (direkt angeschlossenes Gerät, das auch LACP durchführt).

Adaptive Transmit Load Balancing – Ankommender Verkehr wird nur auf der aktiven Schnittstelle entgegengenommen, abgehender Netzwerkverkehr wird gemäß der gegenwärtigen Last auf jede Schnittstelle verteilt. jeder Sklave. Diese Option erfordert keine spezielle Switch-Unterstützung.

Adaptive Load Balancing – umfasst Adaptive Transmit Load Balancing inklusive Receive Load Balancing (RLB) für den IPV4-Verkehr. Diese Option erfordert keinen speziellen Switch-Unterstützung. Der Lastausgleich beim eingehenden Netzwerkverkehr wird durch die ARP-Verhandlung erreicht.

- *Verteilung nach*: Wählt die Sende-Richtlinie, um die korrekte Schnittstelle auszuwählen. Diese Option gilt für die XOR- und LACP-Arbeitsweise. Folgende Einstellungswerte sind möglich:

  Schicht 2 (MAC-Adressen) – Dieser Algorithmus lenkt den Netzwerkverkehr zu einer bestimmten Gegenstelle immer über dieselbe Schnittstelle.

  Schicht 2 und 3 (MAC- und IP-Adressen) – Arbeitet wie die Schicht 2-Verteilung, sorgt aber zusätzlich für ausgeglichenere Verteilung des Netzwerkverkehrs. Das trifft gerade in Umgebungen zu, in denen ein IP-Gateways eingesetzt werden.

  Schicht 3 und 4 (MAC-, IP-Adressen und UDP/TCP) – Diese Richtlinie betrachtet höhere Protokollschichten um die Sendeschnittstellen auszuwählen. Fragmentierte Pakete werden ignoriert.
- *ARP-Überprüfung*: Hier wird die aktive Überprüfung des Links durch ARP-Anfragen aktiviert.
- *Überprüfungsintervall (in ms)*: Das Intervall, in dem die Überprüfung stattfinden soll (in ms). Der kleinste gültige Wert ist 100.
- *IP*: Die IP-Adresse, die für die ARP-Anfragen benutzt wird. Falls für diese IP-Adresse keine ARP-Anfragen beantwortet werden, wird der Link als unbenutzbar eingestuft.
- *Ethernet-Ports*: In dieser Liste wird ausgewählt, welche Ethernet-Ports gebündelt werden. Es werden nur diejenigen Ports angezeigt, die ansonsten unbenutzt sind.
- *Up-Verzögerung (in ms)*: Hier wird die Verzögerung eingestellt die eingehalten werden soll, bevor eine Schnittstelle wieder

verfügbar gemacht wird. Die Zeit wird in Millisekunden (ms) angegeben.

- *Down-Verzögerung (in ms)*: Hier wird die Verzögerung eingestellt die eingehalten werden soll, bevor eine Schnittstelle heruntergefahren wird. Die Zeit wird in Millisekunden (ms) angegeben.
- *Carrier-Auswertung des Treibers benutzen*: Gibt an, ob miimon MII- oder ETHTOOL-ioctls statt netif_carrier_ok () verwenden werden soll, um den Status zu bestimmen.
- *Primärer Port*: Hier wird die primäre Schnittstelle angegeben. Wenn diese Schnittstelle gestört ist, werden alternative Schnittstellen benutzt, und dies auch nur solange, bis die primäre Schnittstelle wieder funktionsfähig ist. Ein Anwendungsbeispiel wäre die Failover-Bündelung einer 1000 MBit- und einer/mehrerer 100 MBit-Schnittstellen, bei der bevorzugt die 1000 MBit-Schnittstelle benutzt werden soll.

8.3 GUI-Referenz: *iSCSI Initiator*

(Dieser Dialog befindet sich unter *iSCSI – iSCSI Initiator*)

8.3.1 Abschnitt *Modus*

8.3.1.1 Felder in diesem Abschnitt

- *Aktiviert*: Mit dieser Option wird der iSCSI Initiator aktiviert. Die Aktivierung ist erforderlich, um iSCSI-Knoten ins System einzubinden.
- *Initiatorname*: Hier wird der eindeutig identifizierbare (IQN) Name des Initiator angegeben.

8.3.2 Abschnitt *iSCSI Discovery*

8.3.2.1 Felder in diesem Abschnitt

- *Authentifizierung*: Um iSCSI Targets zu ermitteln, kann es aus Sicherheitsgründen erforderlich sein, dass dafür Authentifizierungsdaten anzugeben sind. Die Option kann aktiviert werden, falls ein iSCSI discovery login erforderlich ist.
- *Benutzer*: Hier wird der Benutzer-Login für die Authentifizierung angegeben.
- *Passwort*: Hier wird das Passwort zum Benutzer-Login angegeben.

8.3.3 Aktionen für dieses Formular

- *Abbrechen*: Bearbeitung des Formulars beenden, die Einstellungen werden verworfen.
- *Speichern*: Bearbeitung des Formulars beenden, die Einstellungen werden gespeichert.

8.4 GUI-Referenz: *iSCSI-Knoten*

(Dieser Dialog befindet sich unter *iSCSI Initiator – iSCSI-Knoten*)

8.4.1 *iSCSI-Knoten wählen*

8.4.1.1 Spalten in der Tabelle

- *IP-Adresse*: Hier wird die IP-Adresse des definierten iSCSI-Knoten angezeigt.
- *Port*: Zeigt den TCP/IP-Port des iSCSI-Knoten.
- *iSCSI Target*: Hier wird der Name des iSCSI Target angezeigt. Üblicherweise ist dies ein iSCSI Qualified Name (IQN).
- *Info*: Zeigt Details des definierten iSCSI-Knoten.
- *Clustered*: Zeigt an, ob die iSCSI-Festplatte im Cluster-Verbund verwaltet wird.

8.4.1.2 Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion öffnet sich ein Dialog, um den iSCSI-Knoten zu bearbeiten.
- *Löschen*: Mit dieser Aktion wird der gewählte iSCSI-Knoten gelöscht.

8.4.1.3 Aktionen für dieses Formular

- *Target discovery*: Die Aktion ermittelt iSCSI Targets und weitere Informationen, um iSCSI-Knoten hinzuzufügen.
- *Hinzufügen*: Diese Aktion öffnet einen Dialog, um manuell iSCSI-Knoten hinzuzufügen.

8.4.2 *iSCSI-Knoten bearbeiten*

8.4.2.1 Tab *Grundeinstellungen*, Abschnitt *iSCSI-Knoten*
Felder in diesem Abschnitt

- *Name*: Hier wird der iSCSI Qualified Name angegeben oder angezeigt.
- *Info*: Hier können Details zum iSCSI-Knoten eingetragen werden.
- *IP-Adresse*: Hier wird die IP-Adresse eingegeben, unter der der iSCSI-Knoten angesteuert werden kann.
- *Port*: Hier wird der TCP/IP-Port angegeben, über den mit dem iSCSI-Knoten kommuniziert wird.

8.4.2.2 Tab *Grundeinstellungen*, Abschnitt *Authentifizierung*
Felder in diesem Abschnitt

- *iSCSI Initiator gegenüber iSCSI Target*: Diese Option muss aktiviert werden, wenn der iSCSI Initiator sich am iSCSI Target authentifizieren muss.
- *Benutzer*: Hier wird das CHAP-Login angegeben.

- *Passwort*: Hier wird das Passwort für die Authentifizierung angegeben.
- *iSCSI Target gegenüber iSCSI Initiator*: Diese Option muss aktiviert werden, wenn das iSCSI Target sich am iSCSI Initiator authentifizieren muss.
- *Benutzer*: Hier wird das CHAP-Login angegeben.
- *Passwort*: Hier wird das Passwort für die Authentifizierung angegeben.

8.4.2.3 Tab *Optionen*, Abschnitt *Name*

Felder in diesem Abschnitt

- *iSCSI Target verwendet ungültigen Namen*: Wird die Namens-Konvention auf Seite des iSCSI Target nicht eingehalten und kein iSCSI Qualified Name (IQN) verwendet, kann diese Option aktiviert werden, um dennoch eine korrekte Funktionsweise zu ermöglichen.

8.4.2.4 Aktionen für dieses Formular

- *Abbrechen*: Beenden der Bearbeitung, die Einstellungen werden verworfen.
- *Speichern*: Beenden der Bearbeitung, die Einstellungen werden gespeichert.

8.4.3 : *iSCSI Target Discovery*

8.4.3.1 Abschnitt *Einstellungen*

Felder in diesem Abschnitt

- *IP-Adresse*: Hier wird die IP-Adresse angegeben, auf der iSCSI Targets ermittelt werden sollen.
- *Port*: Hier wird der TCP/IP-Port angegeben, über den Informationen von iSCSI Targets zur Verfügung gestellt werden.

Aktionen für diesen Abschnitt

- *Prüfen*: Mit der Ausführung dieser Aktion wird versucht, iSCSI Targets über die angegebene IP-Adresse zu ermitteln.

8.4.3.2 Aktionen für dieses Formular

- *Importieren*: Die ermittelten Daten von iSCSI Targets können mit dieser Aktion für die weitere Bearbeitung übernommen werden.
- *Zurück*: Beenden der Bearbeitung.

8.5 GUI-Referenz: *iSCSI-Knoten Status*

(Dieser Dialog befindet sich unter *Überwachung/Auswertung – Status – iSCSI-Knoten*)

8.5.1 *iSCSI-Knoten - Status*

In diesem Dialog kann der Status von eingebundenen iSCSI-Knoten eingesehen werden.

8.5.1.1 Spalten in der Tabelle

- *IP-Adresse*: Hier wird die IP-Adresse des definierten iSCSI-Knoten angezeigt.
- *Port*: Zeigt den TCP/IP-Port des iSCSI-Knoten.
- *iSCSI Target*: Hier wird der Name des iSCSI Target angezeigt. Üblicherweise ist dies ein iSCSI Qualified Name (IQN).
- *Aktion*: Hier wird angezeigt, ob der iSCSI-Knoten im System eingebunden ist. Je nach Status, kann an dieser Stelle die entsprechende Aktion ausgeführt werden.

8.5.1.2 Aktionen für jeden Tabelleneintrag

- *Login*: Mit dieser Aktion kann der gewählte iSCSI-Knoten ins System eingebunden werden.
- *Logout*: Mit dieser Aktion kann der gewählte iSCSI-Knoten vom System gelöst werden.

- *Detail*: Mit dieser Aktion können Detailinformationen angezeigt werden.

8.5.2 *iSCSI-Knoten*

8.5.2.1 Tab *Info*
Felder in diesem Abschnitt

- *iSCSI Target*: Hier wird der vollständige Name des iSCSI-Targets angezeigt.
- *IP-Adresse*: Zeigt die IP-Adresse des Target-Hosts.
- *Port*: Zeigt den Port, über den der iSCSI-Knoten erreichbar ist.
- *Verbindung*: Zeigt an, ob der iSCSI-Knoten verbunden ist.

8.5.2.2 Tab *Info*, Abschnitt *Status*
Felder in diesem Abschnitt

- : In diesem Feld wird der detaillierte Status über den iSCSI-Knoten angezeigt.

8.5.2.3 Tab *Konfiguration*
Felder in diesem Abschnitt

- : Zeigt die detaillierte Konfiguration des iSCSI-Knoten an.

8.5.2.4 Aktionen für dieses Formular

- *Zurück*: Führt zurück zur Übersicht.

9 Firewall

9.1 Einführung

Eine Firewall sichert einzelne Netzwerksegmente gegeneinander ab. Die Firewall kontrolliert, welche Verbindungen zwischen den einzelnen Netzen zulässig sind, und lehnt verbotene Verbindungen ab.

Die einfachste Form einer Firewall ist der Paketfilter. Dieser entscheidet bei jedem IP-Paket anhand der Quell- und Zieladressen und der jeweiligen Ports, ob das Paket passieren darf oder nicht. Ein solcher Paketfilter muss in jedem der Netze, die er voneinander trennen soll, eine Netzwerkschnittstelle haben. Sind mehrere Netze auf einem Switch zusammengelegt, kann die Firewall leicht umgangen werden.

Im V-Cube ist eine leistungsfähige Firewall enthalten, die „Stateful Inspection“ (zustandsgesteuerte Filterung) unterstützt. Bei dieser Technik wird im Unterschied zu einem reinen Paketfilter für jede Verbindung im Speicher ein Eintrag erzeugt. So ist für jede aktive Verbindung der Status bekannt, und IP-Pakete können einer laufenden Verbindung zugeordnet bzw. fehlerhafte und gefälschte Pakete erkannt werden.

Ein weiterer Vorteil von Stateful Inspection ist die Unterstützung komplexer Protokolle, die mit getrennten Kontroll- und Datenverbindungen arbeiten, wie etwa FTP oder SIP. Die Firewall ist hier in der Lage, anhand des Kontrollkanals eine neu eröffnete Datenverbindung einer Verbindung zuzuordnen und passieren zu lassen.

In einer Firewall lassen sich Berechtigungen bis auf die Ebene eines einzelnen Hosts setzen. Meist werden jedoch zusammenhän-

gende IP-Bereiche zu Netzen zusammengefasst, etwa *LocalNet* oder *Internet*.

Pakete können auf zwei verschiedene Arten abgelehnt werden. Im einfachsten Fall verwirft die Firewall sie einfach. Alternativ kann zusätzlich eine Ablehnung in Form eines ICMP-Pakets mit dem Inhalt „Host unreachable – Zielhost nicht erreichbar“ verschickt werden. Im ersten Fall wird der IP-Stack des Absendersystems das Paket erneut versenden, bis sein Timeout abgelaufen ist. Im zweiten Fall erfolgt umgehend eine Rückmeldung, dass dieser Dienst nicht verfügbar ist.

Ein Paketfilter bzw. eine Stateful-Inspection-Firewall schaut nur in die IP-Header der Pakete und nimmt anhand der Quell- und Ziel-Portadressen eine Unterscheidung vor. Eine Ausnahme bildet die Behandlung spezieller Protokolle wie FTP oder SIP, bei denen das eigentliche Protokoll teilweise mitgelesen wird. Eine Analyse der Nutzdaten findet jedoch nicht statt. Ein „Application Layer Filter“ geht einen Schritt weiter: Hier wird der konkrete Inhalt des IP-Pakets untersucht. Bei einem HTTP-Proxy etwa wird der HTTP-Header gelesen und ausgewertet. Dann wird der Proxy seinerseits eine vollständig neue Anfrage generieren und an den ursprünglich adressierten Host senden. Dessen Antwort schickt der Proxy an den ursprünglichen Absender weiter, ebenfalls in einem neuen, wohlgeformten Paket. Durch diese Technik ist es unmöglich, den Zielport 80 für andere Dienste als HTTP zu missbrauchen, da der Proxy nur HTTP versteht und andere Pakete verwirft. V-Cube unterstützt solche Application Layer Filter für die oft genutzten Dienste HTTP und SMTP. Beim Application Layer Filter ist es zusätzlich möglich, konkrete Inhalte zu filtern, etwa zur Überprüfung auf Viren.

9.1.1 Firewall im V-Cube

Bei der im V-Cube eingesetzten Paketfilter-Firewall werden drei unterschiedliche Filter verwendet: Der INPUT-Filter bestimmt, welche Dienste auf dem V-Cube selbst erreichbar sind. Der FORWARD-Filter kontrolliert, welche Verbindungen von einem Netzwerk in ein anderes zulässig sind, und die OUTPUT-Regel gewährt dem V-Cube selbst Zugriff auf andere Systeme.

Diese Dreiteilung findet sich in der Konfiguration des V-Cubes wieder. Zugriffe auf Dienste im V-Cube (INPUT-Regel) werden über die Benutzungsrichtlinien (S. 33) gewährt. Zugriffe von einem Netz in ein anderes (FORWARD-Regel) werden in der *Firewallmatrix* eingestellt. Ausgehender Datenverkehr von Diensten innerhalb des V-Cubes (OUTPUT-Regel) ist grundsätzlich immer erlaubt und kann nicht eingeschränkt werden.

9.2 GUI-Referenz: Firewall

9.2.1 *Firewall – Allgemein*

(Dieser Dialog befindet sich unter *Netzwerk – Firewall – Allgemein*)

In den folgenden Abschnitten werden allgemeine Einstellungen für die Firewall vorgenommen. Dabei lässt sich u. a. der Umfang der Protokollierung in Logdateien sowie die Auswertung dieser Logdateien anpassen.

9.2.1.1 Tab *Grundeinstellungen*, Abschnitt *Grundeinstellungen*

In diesem Abschnitt werden einige Optionen für das Verhalten und die Protokollierung der Firewall eingestellt. Die Protokollierungsoptionen betreffen dabei nur Verbindungen, die direkt an den V-Cube gerichtet sind. Die Protokollierung durchlaufender Verbindungen wird in der Firewallmatrix konfiguriert. In Windows-Netzwerken verursachen Broadcast-Pakete oft eine Flut von Logmeldungen. Mit der Einstellung *Alles außer Broadcasts* werden solche Pakete ignoriert.

Felder in diesem Abschnitt

- *Verhalten bei ICMP-Echo-Request (Ping)*: ICMP-Echo-Request-Pakete (*pings*) dienen dazu, festzustellen, ob ein bestimmter Rechner erreichbar ist und wie lange die Laufzeit der Datenpakete dorthin ist. Hier wird eingestellt, wie der V-Cube auf ICMP-Echo-Requests reagiert.

  Normalerweise wird *ratenlimitiert* auf ICMP-Echo-Requests geantwortet. Dann werden ca. 10 Ping-Pakete pro Sekunde beantwortet, alle anderen werden verworfen. Falls viele Systeme gleichzeitig versuchen, den V-Cube anzupingen, kann es auch erforderlich sein, *unlimitiert* zu antworten (dann wird jedes Ping beantwortet).

9.2.1.2 Tab *Optionen*, Abschnitt *Logging für lokale Dienste*

Felder in diesem Abschnitt

- *Erlaubte Verbindungen*: Durch das Aktivieren dieser Option wird der Aufbau erlaubter Verbindungen auf den V-Cube protokolliert.
- *Verbotene Verbindungen*: Durch das Aktivieren dieser Option werden nichtautorisierte Verbindungsversuche protokolliert.

- *Verbindungen von gefälschten Absenderadressen*: Mit dieser Option werden Verbindungsversuche von gefälschten Absenderadressen protokolliert.
- *Verbindungen zu nicht vorhandenen Diensten*: Durch das Aktivieren dieser Option werden Verbindungsversuche auf Ports protokolliert, die keinen Diensten zugeordnet sind.

9.2.1.3 Tab *Optionen*, Abschnitt *Logging für Firewallmatrix*

Felder in diesem Abschnitt

- *Erlaubte Verbindungen*: Durch das Aktivieren dieser Option werden alle Verbindungen protokolliert, die in der Firewallmatrix als erlaubt eingestellt sind.
- *Verbotene Verbindungen*: Durch das Aktivieren dieser Option werden alle Verbindungsversuche zwischen Netzwerken protokolliert, deren Regel in der Firewallmatrix auf ablehnen oder wegwerfen gesetzt ist.

9.2.1.4 Tab *Optionen*, Abschnitt *Report*

Felder in diesem Abschnitt

- *Firewall-Report aktivieren*: Mit dieser Option wird die automatische Erstellung von Firewall-Reports aktiviert. Ein solcher Report enthält eine statistische Auswertung der Einträge in der Firewall-Logdatei.
- *Täglicher Report*: Mit dieser Option wird täglich ein Firewall-Report erstellt.
- *Wöchentlicher Report*: Mit dieser Option wird wöchentlich ein Firewall-Report erstellt.

- *E-Mail-Adresse des Empfängers*: In diesem Feld wird die E-Mail-Adresse angegeben, an die der Report gesendet wird.
- *Format*: Der Report kann wahlweise als einfacher Text oder HTML-formatiert werden.
- *Schwellenwert für Protokollierung*: Mit diesem Schwellenwert wird festgelegt, wie oft ein Ereignis auftreten muss, damit es in den Report aufgenommen wird.
- *Angezeigte Ereignisse pro Logreport beschränken*: Dieser Wert beschränkt die Anzahl der im Report aufgeführten Ereignisse.
- *IP-Adressen auflösen*: Durch das Aktivieren dieser Option werden IP-Adressen im Report über den Nameserver in Hostnamen aufgelöst. Dies kann erheblichen Netzwerkverkehr erzeugen und die Erstellung des Reports verlangsamen.
- *Nach Absenderadressen unterscheiden*: Verschiedene Logeinträge können als einzelne oder als getrennte Ereignisse aufgefasst werden. Durch das Deaktivieren dieser Option können mehrere Meldungen mit unterschiedlichen Absenderadressen zu einem Ereignis zusammengefasst werden.
- *Nach Zieladressen unterscheiden*: Durch das Deaktivieren dieser Option können mehrere Meldungen mit unterschiedlichen Zieladressen zu einem Ereignis zusammengefasst werden.
- *Nach Protokollen unterscheiden*: Durch das Deaktivieren dieser Option können mehrere Meldungen mit unterschiedlichen Protokollen (TCP, UDP usw.) zusammengefasst werden.
- *Nach Quellports unterscheiden*: Durch das Deaktivieren dieser Option können mehrere Meldungen mit unterschiedlichen Quellports zusammengefasst werden.
- *Nach Zielports unterscheiden*: Durch das Deaktivieren dieser Option können mehrere Meldungen mit unterschiedlichen Zielports zusammengefasst werden.

9.3 *Schutz vor Brut-Force-Attacken*

9.3.1 Abschnitt

9.3.1.1 Felder in diesem Abschnitt

- *Aktivieren*: Der Dienst zum Schutz vor Brut-Force-Attacken wird hier eingeschaltet.
- *Anzahl erlaubter Loginversuche*: Wenn ein Angreifer mehr als die angegebene Anzahl versucht hat, sich unerlaubt einzuloggen, wird die IP-Adresse des Angreifers gesperrt. Achtung: Eine Unterscheidung zwischen Angreifer und Benutzer kann nicht getroffen werden.
- *Dauer der Sperrung (Sek.)*: Die IP-Adresse kann für die hier angegebene Dauer in Sekunden nicht mehr auf den Server zugreifen. Die Sperrung wird nach Ablauf der Dauer automatisch aufgehoben. Alternativ kann die Sperrung im Status-Dialog manuell aufgehoben werden.

  Die IP-Adressen werden auch entsperrt, sobald der Server oder der Dienst neu gestartet wird.
- *Nicht sperren*: Selektierte Netzwerke werden nicht gesperrt. Diese Einstellung ist nützlich, um interne Netzwerke vor eventuellen Sperrungen zu bewahren. Möglicherweise ist es auch beabsichtigt gerade interne Netzwerke zu prüfen und IP-Adresse gegebenenfalls zu sperren. Dann sollten die internen Netzwerke hier nicht selektiert werden.

9.3.2 Aktionen für dieses Formular

- *Speichern*: Die Einstellungen werden gespeichert.

9.3.3 *Brute-Force-Schutz - Status*

9.3.3.1

In dieser Tabelle werden die gesperrten IP-Adressen gelistet.

XXX missing title found
Spalten in der Tabelle

- *Gesperrte IP-Adressen*: IP-Adressen können öffentlich oder im privaten Adressbereich liegen.

Aktionen für jeden Tabelleneintrag

- *Sperre aufheben*: Mit dieser Aktion wird die Sperre für die IP-Adresse aufgehoben. Ein Fenster mit entsprechendem Hinweis erscheint.

Aktionen für dieses Formular

- *Manuell sperren*: Mit dieser Aktion wird ein Dialog geöffnet, in dem weitere IP-Adressen manuell gesperrt werden können.
- *Aktualisieren*: Die Anzeige wird aktualisiert.

9.3.3.2 *IP-Adressen manuell sperren*

Abschnitt
Felder in diesem Abschnitt

- *IP-Adressen angeben*: In das Feld können mehrere IP-Adressen mit Leerzeichen getrennt eingegeben werden, die nachfolgend vom Serverzugriff gesperrt werden. IP-Adressen innerhalb der Netzwerke der Option *Nicht sperren* werden dennoch gesperrt.

Aktionen für dieses Formular

- *Jetzt sperren*: Die angebenen IP-Adressen werden für den Zugriff auf den Server sofort gesperrt. Die Sperre dauert so lange, wie in den Einstellungen angegeben.

10 DNS und DHCP

10.1 Einführung

10.1.1 Host- und Domainnamen

Die Adressierung von Computersystemen erfolgt im Internet durch die Angabe der IP-Nummer bzw. im Ethernet durch die Verwendung der MAC-Adresse. Im Normalfall erfolgt die Umsetzung der IP-Adresse auf eine MAC-Adresse durch das Betriebssystem selbst.

Die IP-Nummer besteht aus einer 32 Bit breiten Adresse, die gewöhnlich in vier durch Punkte getrennten Oktette dargestellt wird, etwa 192.168.9.9.

Um das Handling für Benutzer einfacher zu gestalten, werden den Systemen Namen zugewiesen, die damit auch IP-Adressen entsprechen. Diese werden meist als „Hostname“ bezeichnet. Im einfachsten Fall wird dazu eine Zuordnung vom Namen auf die IP-Nummer in der *hosts*-Datei vorgenommen. Diese befindet sich bei Windows-Systemen im Verzeichnis *\WINNT* und bei Unix/Linux-Systemen im Verzeichnis */etc*. Diese Datei muss auf jedem Computersystem separat gepflegt werden. Die Wartung ist daher recht aufwendig, da bei Neueinträgen und Änderungen jede Instanz dieser *hosts*-Dateien modifiziert werden muss.

10.1.2 Domain

Ein Hostname muss zu einem Zeitpunkt eindeutig auf eine IP-Nummer aufgelöst werden. Da aber in vielen Fällen an unterschiedlichen Standorten dieselben Namen für Computersysteme verwendet werden (oftmals auch symbolische Namen wie *mail* oder *www*), muss dem Namen eine weitere Bezeichnung hinzugefügt werden, die für Eindeutigkeit sorgt. Mitunter löst ein Hostname auf mehrere IP-Adressen auf, um damit über DNS eine Lastverteilung auf mehrere Server zu erreichen. Da diese Server allerdings alle gleiche Inhalte bereitstellen, ist dies ein Sonderfall von „einer IP-Nummer".

Dazu wird die „Domain" verwendet, die quasi den Namen des Unternehmens oder des Standorts darstellt.

Im Internet werden ebenfalls Domains genutzt. Im Unterschied zur Windows-Domäne können diese nicht beliebig gewählt werden. Stattdessen werden sie über zentrale Einrichtungen verwaltet. Ein Anwender muss prüfen, ob der von ihm gewünschte Domainname noch frei ist und kann diesen dann über einen Provider „registrieren". Ist die Domain bereits anderweitig vergeben, muss eine andere ausgesucht werden.

Im folgenden handelt es sich bei der Verwendung des Begriffs „Domain" immer um Internet-Domains. Bei Windows-Domänen wird dies explizit erwähnt.

Eine Domain gehört immer zu einer „Top-Level-Domain" TLD. Diese TLDs sind bis auf wenige Ausnahmen Landeskennungen mit einem Kürzel aus zwei Buchstaben, etwa „de" für Deutschland oder „at" für Österreich. Diese werden auch als „ccTLD" (= „Country-Code TLD") bezeichnet.

Daneben gibt es noch allgemeine TLDs, die in den USA beim Aufbau des Internet zunächst festgelegt wurden („gTLD" = „generic TLD"). Dazu gehören etwa „com" für kommerzielle Unternehmen,

„edu“ für Hochschulen (Education), „org“ für nicht-kommerzielle Organisationen oder „gov“ für US-amerikanische Regierungsorgane.

In letzter Zeit sind einige weitere TLDs hinzugekommen, von denen manche „gesponsert“ („sTLD“) sind und manche nicht („uTLD“ = „unsponsored TLD“). Ein Sponsor ist in diesem Fall eine Organisation, die eine bestimmte Klientel vertritt und die Vergaberichtlinien für Domains innerhalb der TLD festlegt. Zudem muss der Sponsor einen Registrar zur Abwicklung der Registrierungen beauftragen. Eine ungesponserte TLD unterliegt den normalen Richtlinien der *ICANN.*

Tabelle einiger ausgesuchter TLDs

Name	Erläuterung	Zuständiger Registrar	Typ	Seit
.at	Österreich	www.nic.at	ccTLD	1988
.ch	Schweiz	www.switch.ch	ccTLD	1987
.de	Deutschland	www.denic.de	ccTLD	1986
.com	Kommerzielle Organisationen	www.verisign-grs.com	g/uTLD	1985
.edu	Bildungseinrichtungen		g/uTLD	1985
.gov	Regierungsorgane der USA	www.dotgov.gov	g/uTLD	1985
.int	Internationale Regierungsorganisationen	http://www.iana.org/int-dom/int.htm	g/uTLD	1985
.mil	Miltärische Einrichtungen der USA	www.nic.mil/dodnic/	g/uTLD	1985
.net	Netzwerk-Organisationen	www.verisign-grs.com	g/uTLD	1985
.org	Nichtkommerzielle, Nicht-Regierungs-Organisationen	www.pir.org	g/uTLD	1985
.aero	Luftfahrtindustrie	www.information.aero	g/sTLD	2001

.biz	Handelsfirmen („Business“)	www.neulevel.biz	g / uTLD	2001
.coop	Kooperationen / Genossenschaften	www.nic.coop	g / sTLD	2001
.info	Informationsanbieter	www.afilias.info	g / uTLD	2001
.museum	Museen, Ausstellungen	musedoma.museum	g / sTLD	2001
.name	Für natürliche Personen oder Familien	www.gnr.com	g / uTLD	2001
.pro	best. Berufsgruppen	www.registrypro.pro	g / uTLD	2002
.eu	Europäische Personen und Einrichtungen	www.eurid.org	g / sTLD	2003
.travel	Reiseindustrie	http://www.tralliance.travel	g / sTLD	2005

Daneben existiert noch die weitere, zunächst provisorisch eingerichtete TLD „arpa“, die für Rückwärtsauflösung (siehe weiter unten) verwendet wird. Inzwischen wird sie als „Address and Routing Parameter Area“ übersetzt.

Unterhalb einer TLD kann eine Domain immer nur ein einziges Mal existieren. Allerdings darf eine Domain in mehreren TLDs genutzt werden. Beispiele wären etwa „google.com“ und „google.de“.

Vor allem große Unternehmen oder Einrichtungen müssen ihre Domain auf verschiedene Standorte oder Gebäude verteilen. Dies geschieht durch „Subdomains“, die unterhalb der Domain quasi abgeteilte eigene Domains bilden. Manchmal werden dazu die Namen der Standorte verwendet, etwa „muenchen.collax.com“ und „boston.collax.com“. Formal korrekt ist „muenchen.vcube.com“ eine Domain und gleichzeitig eine Subdomain von „vcube.com“. Diese wiederum ist eine Domain und gleichzeitig eine Subdomain von „.com“.

10.1.3 FQDN

Das Gebilde aus Hostname und Domain wird als „Fully Qualified Domain Name“ (FQDN) bezeichnet. Damit ist ein Computersystem mit einem weltweit einmalig vergebenen Namen versehen, der auf eine IP-Nummer verweist.

Der FQDN wird von links nach rechts aus mehreren Komponenten gebildet, die alle durch Punkte voneinander getrennt sind. Dies sind der Reihe nach der Hostname, Subdomain(s), Domain und Top-Level-Domain. Als Subdomain können keine, eine oder auch mehrere Komponenten verwendet werden.

Beispiele für gültige FQDNs sind etwa „www.heise.de“, „mail.muenchen.vcube.com“ oder auch „mail.intern.hamburg.de.unser-weltkonzern.com“.

10.1.4 Domain Name Service

Der „Domain Name Service“ (DNS) ist eine weltweit verteilte Datenbank, in der die IP-Adressen und ihre korrespondierenden Hostnamen gespeichert werden. Dabei muss nicht zwingend zu jeder IP-Nummer ein Hostname vorhanden sein. Bis auf Ausnahmen löst jeder Hostname auf eine IP-Nummer oder einen weiteren Hostnamen auf.

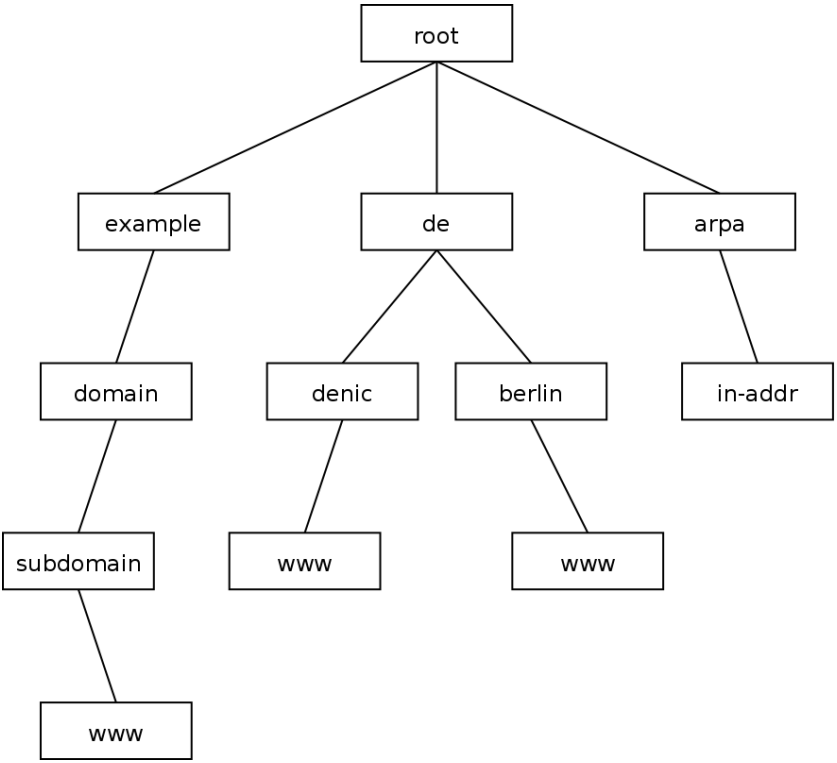
Die DNS-Datenbank wird in einer hierarchischen Baumstruktur verwaltet. Dabei ist die oberste Ebene die „Root-Zone“ (die „Wurzel“). Innerhalb dieser Root-Zone werden Verweise auf die untergeordnete Ebene gespeichert, in der die TLDs gespeichert sind. Weltweit existieren 13 Root-Nameserver, die in den meisten Systemen fest eingegeben sind und nicht manuell eingetragen werden müssen.

In der zweiten Ebene sind die einzelnen TLD-Zonen abgelegt, hier

werden Verweise auf die jeweiligen Domains (bei „com“ etwa 40 Millionen) gespeichert. Diese Nameserver werden von den zuständigen Registraren betrieben, in Deutschland von der DeNIC eG („Deutsches Network Information Center“).

In der nächsten Ebene liegen einzelne Host-Einträge oder Subdomains. Diese Informationen werden meist auf den Nameservern der zuständigen Provider gespeichert. In seltenen Fällen betreibt der Inhaber der Domain seine eigenen Nameserver.

Durch Subdomains können weitere Ebenen gebildet werden. Dabei können die ganzen Einträge unterhalb einer Domain auf einem einzigen Nameserver verwaltet werden. Es können jedoch auch für jede Subdomain eigenständige Nameserver betrieben werden.



Administrativ umfasst eine Domain immer auch alle Subdomains, d. h., für alle Geschehnisse inner- und unterhalb einer Domain ist der Domaininhaber verantwortlich.

Werden technisch für die Subdomains jeweils einzelne Nameserver betrieben, werden diese Subdomains als „Zonen“ im DNS bezeichnet. Jede Subdomain mit eigenständigem Nameserver ist eine solche Zone. Wenn alle Subdomains innerhalb der Domain selbst verwaltet werden, werden in diesem Fall die Begriffe „Domain“ und „Zone“ synonym verwendet.

In der weltweiten Datenbank ist jeder Nameserver nur für einen

kleinen Teil des gesamten Datenbestands verantwortlich. Er ist „autoritativ“ für seine Zonen. Sicherheitshalber gibt es zu jeder Zone mindestens zwei autoritative Nameserver, sonst wäre durch einen Ausfall des Servers die gesamte Domain „weg“.

Um die Datenhaltung zu vereinfachen, wird die Zone nur auf einem Masterserver, dem „Primary DNS“ gepflegt. Die weiteren autoritativen Server für diese Zone kopieren als *Slaves* nur die gesamten Zoneninformationen, sie sind „Secondary DNS“. Der Primary kennt die Secondaries und informiert diese bei Änderungen, so dass sie die Zone neu „transferieren“ können.

Um Anfragen an das gesamte Netzwerk von Nameservern möglichst rasch zu beantworten, dürfen die Zonen-Daten in einem Cache zwischengespeichert werden. Dazu gibt jede Zone jeweils eine Gültigkeitsdauer vor. Bei Änderungen im DNS kann es daher vorkommen, dass Teile des Internets noch eine gewisse Zeit mit veralteten Daten arbeiten.

10.1.5 Ablauf einer DNS-Anfrage

Um eine DNS-Anfrage zu stellen, schickt ein Clientrechner alle Anfragen gewöhnlich an einen DNS-Server im lokalen Netz. Dieser prüft, ob er für die Zone autoritativ ist und die Anfrage selbst beantworten kann.

Ist dies nicht der Fall, prüft der Nameserver, ob sich die Information in seinem Cache befindet und gültig ist und er damit die Anfrage direkt beantworten kann. Er arbeitet dann als „Resolver“.

Ist die Zone nicht im Cache vorhanden, muss der Nameserver selbst eine Anfrage stellen. Dazu kann er entweder alle Anfragen an einen bestimmten Nameserver weiterleiten (= „forwarden“). Dazu wird meist der DNS des Internet-Providers genutzt.

Ist im Nameserver kein Forwarder eingestellt, befragt dieser die Root-Nameserver nach den zuständigen Nameservern für die angefragte TLD. Dort fragt er nach den zuständigen Nameservern für die Domain und kontaktiert diese daraufhin, um die Anfrage aufzulösen oder weitere Verweise auf Nameserver für Subdomains zu erhalten. Der Nameserver hangelt sich durch den gesamten DNS-Baum bis hin zu dem Blatt, welches den angefragten Eintrag enthält.

Dieser aufgelöste Eintrag wird an den Client geschickt und für einen Zeitraum von wenigstens zehn Minuten im Cache zwischengespeichert. Erfolgt innerhalb des Zeitraums eine erneute Anfrage, wird diese direkt mit den Daten aus dem Cache beantwortet.

10.1.6 Rückwärtsauflösung

Die gesamten Mechanismen zu Auflösung von Hostnamen in IP-Adressen stehen auch für den rückwärtigen Weg zur Verfügung: Mit einem „Reverse-Lookup“ können IP-Adressen in Namen aufgelöst werden.

Technisch wird die Rückwärtsauflösung mit Hilfe der Domain *in-addr.arpa* realisiert. Um beispielsweise die IP-Adresse 192.0.2.129 aufzulösen, wird eine DNS-Anfrage nach „129.2.0.192.in-addr.arpa“ gestellt.

Unterhalb in-addr.arpa sind drei Ebenen von Subdomains realisiert, die jeweils für eins der Oktette der IP-Nummer zuständig sind. Dazu sind die Oktette in umgekehrter Reihenfolge in die Abfrage eingesetzt.

Über die Root-Nameserver erfolgt der Verweis auf die zuständigen Nameserver von in-addr.arpa und von dort ein weiterer Verweis abhängig von der ersten Subdomain (also dem ersten Oktett der IP-Nummer). Dort kann ein weiterer Verweis abhängig vom zweiten

Oktett erfolgen und dort wiederum einer abhängig vom dritten Oktett.

Auch für Reverse-DNS gibt es die Mechanismen von autoritativen Servern, Primaries und Secondaries sowie Zonentransfers.

Dadurch, dass für Domains und für IP-Netze jeweils separate DNS-Datenbanken bestehen, ist es nicht ungewöhnlich, dass Vorwärts- und Rückwärtsauflösung nicht synchron sind. Gerade bei Internetanbindung mit einfachen DSL-Leitungen lösen die IP-Adressen oft auf den Hostnamen des Leitungsproviders auf. Dies kann mitunter Schwierigkeiten verursachen, wenn hinter einer solchen Leitung Serverdienste betrieben werden.

10.1.7 Lokale Domain

Gerade diese Rückwärtsauflösung ist innerhalb eines Unternehmens sehr interessant, um einer IP-Nummer einen Namen zuordnen zu können. Meist werden im Unternehmen IP-Nummern aus den privaten Netzen verwendet. Zudem erfolgen sehr oft Änderungen durch Rechnerwechsel usw.

Hat das Unternehmen eine oder mehrere Domains bei einem Provider registriert, ist es aufwendig, all diese Einträge und Änderungen in der offiziellen Domain durchzuführen. Gelegentlich wird intern im Unternehmen unter der Adresse „www“ ein anderer Webserver genutzt als aus dem Internet.

Eine Möglichkeit ist, die offizielle Domain auf einem Nameserver im lokalen Netz des Unternehmens parallel zum Internet zu betreiben. Dieses Vorgehen kann allerdings gelegentlich zu Problemen führen, wenn Einträge aus dem offiziellen Nameserver beim Provider in den internen Nameserver kopiert wurden und der Provider Änderungen durchführt (Umstellung von IP-Adressen usw.).

Sinnvoller ist die Verwendung einer Subdomain *intern* oder *lan*, die dann als eigenständige Zone im lokalen Netz genutzt wird und so nicht mit der offiziellen Zone kollidiert.

Mitunter werden auch eigene TLDs im lokalen Netz verwendet, die auf die private, interne Nutzung hinweisen. Gängig sind *prv*, *priv* (jeweils für „privat“), *lan*, *local* oder *intern* (nicht *int*). Keine dieser TLDs ist allerdings für eine solche Verwendung offiziell freigegeben – die Nutzung erfolgt auf „eigene Gefahr“. *Apple Computer* benutzt inzwischen die TLD *local* für das „Bonjour-Protokoll“. Dies muss dann bei Macintosh-Geräten umgestellt werden.

10.1.8 Dynamische Adressvergabe

Die Konfiguration einer IP-Adresse für einen Computer kann meist manuell über das Betriebssystem vorgenommen werden. Eine einfachere und flexiblere Möglichkeit ist die Verwendung von DHCP („Dynamic Host Configuration Protocol“). Dabei fragt das Betriebssystem im Netzwerk nach einem DHCP-Server und lässt sich von diesem eine IP-Adresse zuteilen.

In der einfachsten Form wird dem DHCP-Server ein Bereich von IP-Nummern genannt, aus dem er nach Belieben IP-Adressen verwenden kann. Ein solcher Bereich wird auch als „Pool“ bezeichnet. Der Server identifiziert die Computer anhand ihrer Hardware-MAC-Adresse und verfolgt intern, welche IP-Adressen er an welches System zugewiesen hat (sog. „Leases“).

Eine DHCP-Lease hat eine bestimmte Laufzeit, nach deren Ablauf das System erneut beim DHCP-Server nach einer IP-Adresse fragen muss. Meist erhält es (auch nach Tagen) vom Server die gleiche IP-Adresse erneut, aber sie kann sich auch ändern.

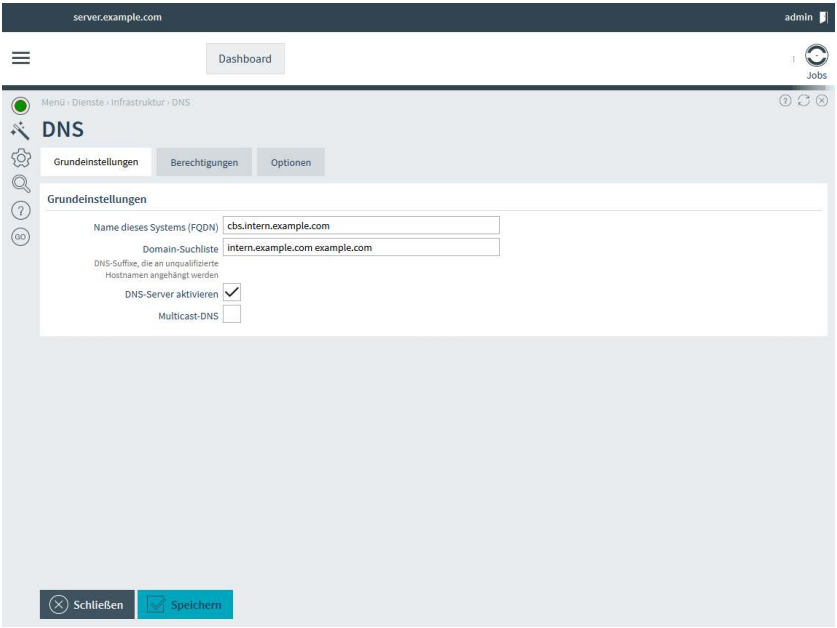
Um eine feste Zuweisung einer IP-Adresse an ein System zu erreichen, muss dieses anhand seiner MAC-Adresse bekannt sein. So ist eine dauerhafte statische Zuordnung der Adresse durch den DHCP-Server möglich.

Im V-Cube werden beide Varianten angeboten. Es kann ein Pool für unbekannte Rechner angelegt werden. Damit sind Systeme gemeint, die nicht als Hosts im V-Cube eingetragen sind. Sobald ein System in den *Benutzungsrichtlinien* bzw. unter *Netzwerk – DNS* als *Host* angelegt wird, können die MAC-Adresse und die IP-Adresse eingestellt werden. Ist der DHCP-Server aktiviert und stellt das System eine DHCP-Anfrage, wird die gesetzte IP-Adresse zugewiesen.

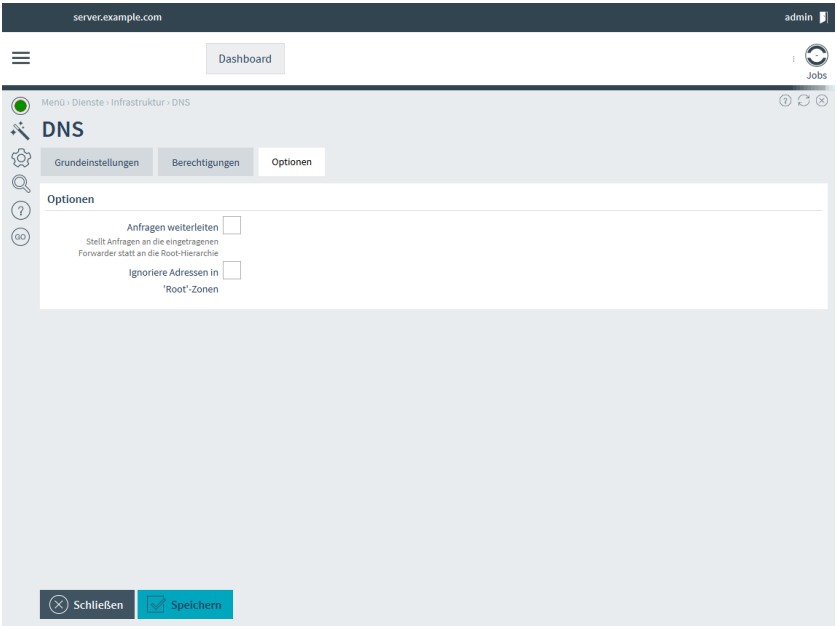
10.2 Schritt für Schritt: DNS für lokale Domain einrichten

Der V-Cube benötigt den Zugriff auf einen funktionsfähigen Nameserver, um die Registrierung durchzuführen und Updates herunterzuladen. Hierfür kann ein beispielsweise beim Provider ein anderer Server als Nameserver verwendet werden.

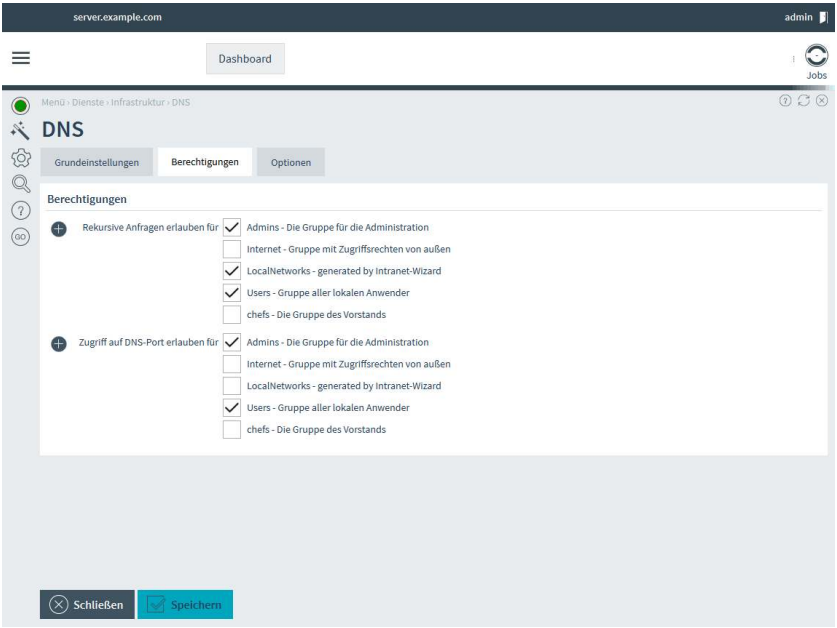
Wesentlich mehr Möglichkeiten bietet der Betrieb eines Nameservers auf dem V-Cube selbst. Hier können eigene Zonen verwaltet und so ein privates IP-Netz in Namen übersetzt werden.



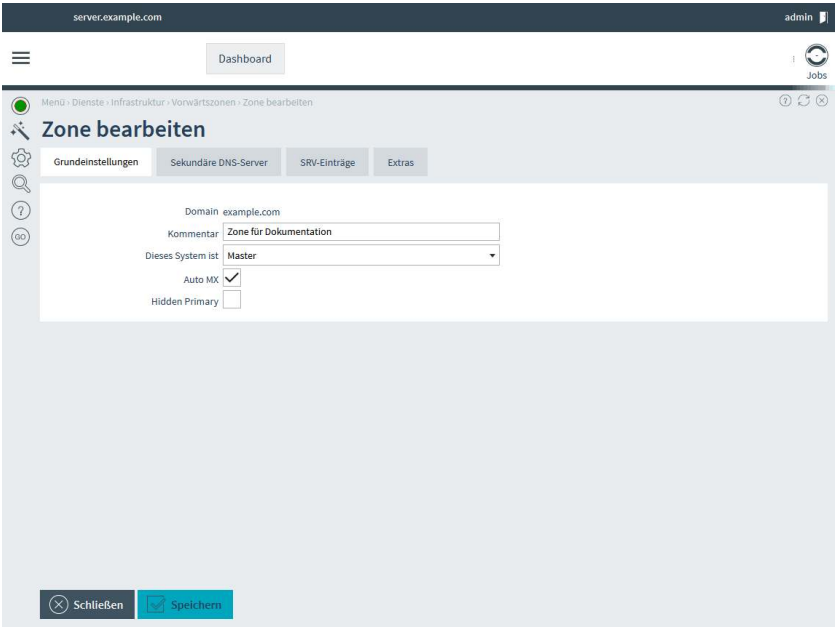
- Sie finden die Grundeinstellungen des Nameservers unter *Netzwerk – DNS – Allgemein*.
- Unter *Name dieses Systems* tragen Sie den FQDN des V-Cubes ein. Dieser Name wird u. a. vom Mail-Dienst verwendet.
- Mit *DNS-Server aktivieren* schalten Sie den Nameserver im V-Cube ein.



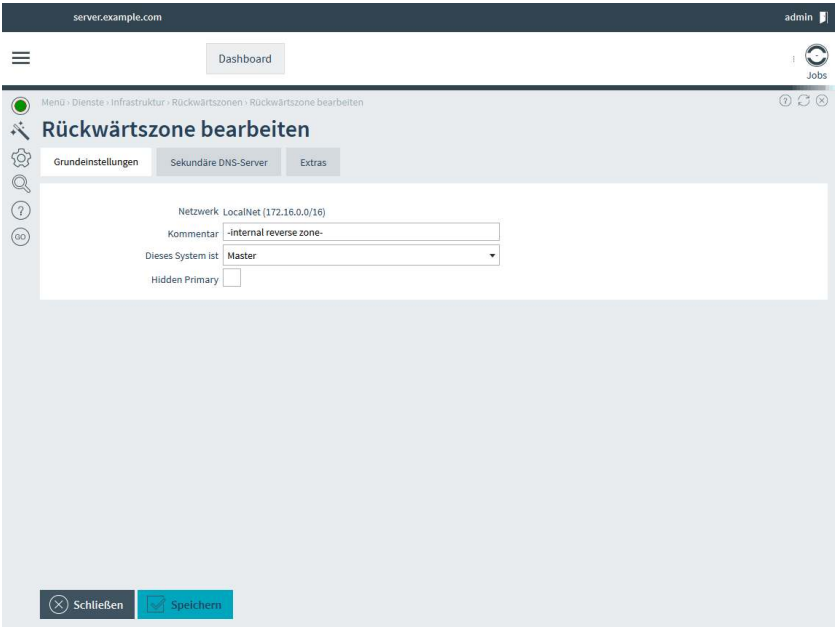
- Wechseln Sie auf den Reiter *Optionen*.
- Abhängig von der Einstellung *Anfragen weiterleiten* erfolgt die Auflösung von fremden Adressen. Lassen Sie die Option deaktiviert, befragt der V-Cube die Root-Nameserver eigenständig.
- Wenn Sie die Option hingegen aktivieren, können Sie bis zu zwei *Forwarder* angeben, an die alle DNS-Anfragen weitergereicht werden. Dabei sollten Sie die Nameserver Ihres Providers verwenden.



- Wechseln Sie auf den Reiter *Berechtigungen*.
- Hier können Sie auswählen, welche Gruppen Zugriff auf den Nameserver erhalten dürfen. Die Option *Rekursive Anfragen* erlaubt Anfragen nach jeglichen Namen.
- *Zugriff auf DNS-Port erlauben* hingegen gestattet nur Anfragen auf Systeme, deren DNS-Einträge auf dem V-Cube selbst verwaltet werden.
- Üblicherweise wird dem lokalen Netz der vollständige Zugriff auf den Nameserver gewährt. Das lokale Netz ist Mitglied der Gruppe *Users*, geben Sie daher der Gruppe Users beide Rechte.

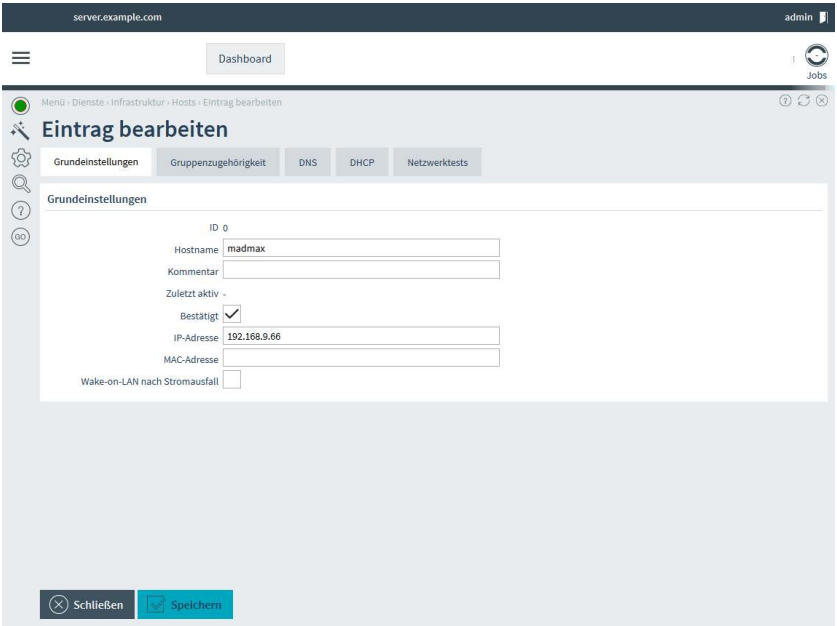


- Im nächsten Schritt legen Sie die lokale Domain an. Dabei kann es sich um Ihre offizielle Internet-Domain handeln. Meist ist es – auch im Hinblick auf die Verwendung privater IP-Adressen im lokalen Netz – jedoch besser, eine nicht existente Domain zu verwenden.
- Wechseln Sie hierfür zu *Netzwerk – DNS – Vorwärtszonen*.
- Legen Sie eine neue Zone an.
- Unter *Domain* tragen Sie den Namen der Zone ein.
- Belassen Sie die Einstellung *Dieses System ist* auf *Master*. Dadurch können Sie Einträge innerhalb der Domain auf dem V-Cube anlegen.

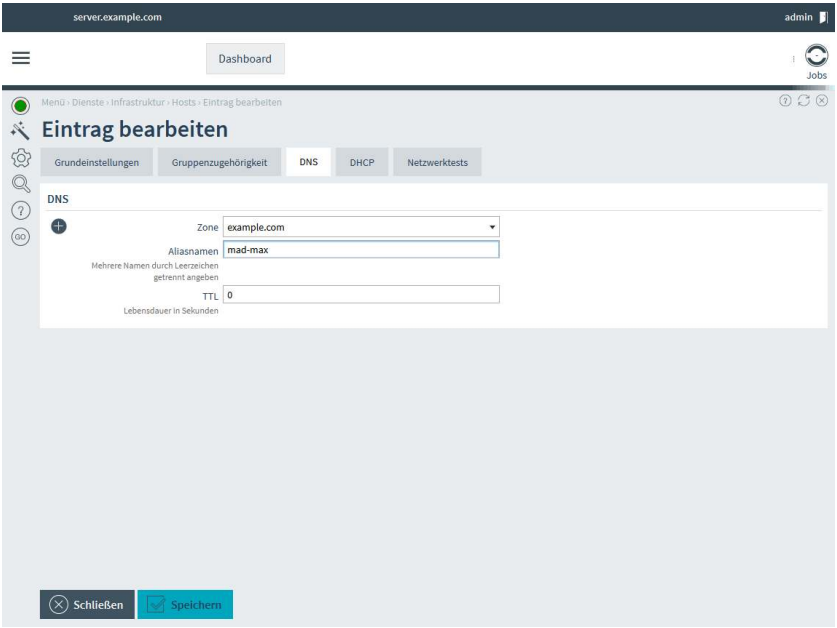


- Wechseln Sie zu den *Rückwärts-Zonen*.
- Legen Sie eine neue Rückwärts-Zone an.
- Wählen Sie als *Netzwerk* das *LocalNet* aus. Für diesen IP-Bereich sollen die Nameservereinträge verwaltet werden.
- Auch für diese Zone ist der V-Cube *Master*.

Nun ist der Nameserver grundlegend konfiguriert. Einzelne Einträge im Nameserver werden im Folgenden als *Hosts* angelegt.



- Wechseln Sie dazu nach *Netzwerk – DNS – Hosts*.
- Legen Sie einen neuen Host an.
- Setzen Sie den *Hostnamen*. Dieser kann später noch geändert werden.
- Prüfen Sie, ob *Bestätigt* aktivert ist. Andernfalls wird kein DNS-Eintrag erzeugt.
- Geben Sie unter *IP-Adresse* die IP-Nummer des Hosts an. Dabei muss die IP-Nummer nicht zwingend aus dem lokalen Netzwerk stammen.



- Wechseln Sie auf den Reiter *DNS*.
- Wählen Sie bei *Zone* die von Ihnen angelegte Domain aus.
- Unter *Aliasnamen* können Sie weitere Namen des Systems angeben.
- Speichern Sie den angelegten Host.

10.3 GUI-Referenz: DNS

10.3.1 *DNS*

(Dieser Dialog befindet sich unter *Netzwerk – DNS – Allgemein*)

In diesen Dialogen können die Einstellungen für den DNS-Dienst bearbeitet werden. Über diesen Dienst ist es möglich, Hostnamen in IP-Adressen aufzulösen und umgekehrt. Außerdem wird hier der Hostname des Systems gesetzt. Dieser wird u. a. vom Mailsystem verwendet.

10.3.1.1 Tab *Grundeinstellungen*, Abschnitt *Grundeinstellungen*

In diesem Dialog wird festgelegt, ob auf dem System der DNS-Dienst aktiviert werden soll. Andernfalls muss ein externer DNS eingestellt werden.

Hinweis: Ohne DNS-Dienst kann der V-Cube keine Registrierung durchführen, keine Updates herunterladen und keine E-Mails versenden.

Felder in diesem Abschnitt

- *Name dieses Systems (FQDN)*: Hier wird der vollständige DNS-Name (FQDN) dieses Systems angegeben, z. B. „vcube.example.com“.
- *Domain-Suchliste*: In diesem Feld kann eine Liste von Domains angegeben werden, die der Reihe nach an einfache Hostnamen angefügt werden, um einen vollständigen Hostnamen zu erhalten.

Wird hier „intern.example.com example.com“ angegeben und innerhalb dieses Systems nach dem Namen „abox“ gesucht, wird der DNS-Server der Reihe nach „abox.intern.example.com“, „abox.example.com“ und schließlich „abox“ abfragen, bis er eine Antwort enthält. Mehrere Einträge werden durch Leerzeichen getrennt. Es werden maximal sechs Domains und 256 Zeichen unterstützt.

- *DNS-Server aktivieren*: Mit dieser Option wird der DNS-Server aktiviert.

  Selbst wenn im lokalen Netz bereits ein DNS betrieben wird, kann es sinnvoll sein, auf diesem System einen DNS-Server als Gateway zu betreiben. Dadurch wird das interne System vom Internet abgeschottet.
- *Erster Nameserver*: Wird kein eigenes DNS betrieben, muss das System mindestens einen Nameserver kennen, um die Namensauflösung von Hosts durchzuführen. Dieser DNS-Server wird hier eingetragen.
- *Alternativer Nameserver*: Zusätzlich kann ein zweiter DNS-Server als Alternative eingetragen werden. Meist werden hier die Nameserver des Providers verwendet.

10.3.1.2 Tab *Berechtigungen*, Abschnitt *Berechtigungen*

Über die *Benutzungsrichtlinien* wird festgelegt, welche Rechner und Netze Zugriff auf den internen Nameserver haben und ob sie beliebige Domains oder nur interne Domains abfragen dürfen.

Felder in diesem Abschnitt

- *Rekursive Anfragen erlauben für*: Rechner und Netzwerke in den aktivierten Gruppen dürfen rekursive DNS-Anfragen stellen.

  Bei einer rekursiven Anfrage verwaltet der angefragte DNS-Server die Zone nicht selbst, sondern muss seinerseits einen weiteren DNS-Server befragen (eine Rekursion).

  Darf ein System keine rekursiven Anfragen stellen, kann es nur Hostnamen und IP-Adressen im lokalen Netz auflösen. Damit ist der Zugriff auf das Internet nicht bzw. nur sehr erschwert möglich.
- *Zugriff auf DNS-Port erlauben für*: Rechner und Netzwerke in den aktivierten Gruppen dürfen DNS-Anfragen stellen.

  Im Unterschied zu den *rekursiven Anfragen* ist über diese Berechtigung nur der Zugriff auf lokal verwaltete Zonen möglich.

10.3.1.3 Tab *Optionen*, Abschnitt *Optionen*

Felder in diesem Abschnitt

- *Anfragen weiterleiten*: Ein Nameserver kann zur Auflösung fremder Zonen entweder alle Anfragen an einen übergeordneten Nameserver („Forwarder“) schicken oder die Auflösung selbst in die Hand nehmen. Dazu muss ausgehend von den Root-Nameservern der zuständige Nameserver für die Zone ermittelt werden, der den gefragten Hostnamen oder die IP-Adresse auflösen kann.

  Durch das Aktivieren dieser Option werden keine Root-Nameserver befragt. Stattdessen werden alle Anfragen an einen oder zwei feste Nameserver weitergeleitet.
- *Vom Provider übermittelten DNS-Server benutzen*: Für Wählverbin-

dungen ins Internet besteht die Möglichkeit, den vom Provider übermittelten DNS-Server für die Namensauflösung zu benutzen. Hier wird die Option aktiviert, wenn der übermittelte Provider-DNS-Server als Forwarder benutzt werden soll.

- *Link*: Hier ist die Verbindung auszuwählen, über die der DNS-Server des Providers übermittelt wird.
- *Forwarder*: Hier wird die IP-Adresse des Nameservers eingetragen, an den die Anfragen weitergeleitet werden.
- *Alternativer Forwarder*: Hier kann ein zweiter, alternativer Nameserver eingetragen werden. Dieser wird befragt, wenn der erste Forwarder nicht antwortet.
- *Ignoriere Adressen in 'Root'-Zonen*: Manche Betreiber von „Root-Nameservern" antworten auf Anfragen nach unbekannten Domains mit einer IP-Adresse und leiten so die Verbindungen auf diesen Server um. Oft handelt es sich dabei um eine Werbeseite für DNS-Dienstleistungen.

  Meist ist die Ursache für das Abfragen einer falschen Domain jedoch, dass sich ein Benutzer bei der Eingabe einer E-Mail-Adresse oder einer URL vertippt hat. Durch diese Umleitung auf eine andere Seite können vertrauliche Daten wie Passwörter oder E-Mails in falsche Hände geraten. Zudem führt es zu Verwirrung, wenn statt der angeforderten Seite plötzlich eine ganz andere erscheint.

  Durch das Aktivieren dieser Option werden solche Umleitungen ignoriert. Ein Root-Nameserver kann dann nur noch auf einen anderen Nameserver verweisen.

10.3.2 *Vorwärtszonen*

Eine Zone umfasst in etwa alle DNS-Einträge einer einzelnen Domain. Im Gegensatz dazu sorgt eine „Rückwärtszone“ für die Auflösung von IP-Adressen in Hostnamen.

Es können auch Zonen angelegt werden, die nicht auf diesem System selbst, sondern auf einem anderen System verwaltet werden. Dies wird oft zur Einbindung einer ADS-Domäne genutzt.

10.3.2.1 *Zone auswählen*

(Dieser Dialog befindet sich unter *Netzwerk – DNS – Vorwärtszonen*)

In dieser Übersicht werden die angelegten Vorwärtszonen angezeigt. Hier können neue Zonen angelegt und vorhandene bearbeitet oder gelöscht werden.

Felder in diesem Dialog

- *Typ*: Hier wird die Art der Zone angezeigt.
- *Domain*: Hier steht der Name der Zone.
- *Kommentar*: Hier steht der Kommentartext zu der Zone.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion wird die Zone bearbeitet.
- *Löschen*: Mit dieser Aktion wird die Zone gelöscht.

Aktionen für diesen Dialog

- *Hinzufügen*: Mit dieser Aktion wird eine neue DNS-Zone angelegt.

10.3.2.2 *Zone bearbeiten*

(Dieser Dialog befindet sich unter *Netzwerk – DNS – Vorwärtszonen*)
In diesem Dialog wird die Konfiguration einer Zone bearbeitet.

Tab *Grundeinstellungen*
Felder in diesem Abschnitt

- *Domain*: Beim Anlegen einer neuen Zone wird hier die Domain angegeben, für die eine Zonenkonfiguration erstellt werden soll.
- *Domain*: Wird eine Zone bearbeitet, wird hier die Domain nur angezeigt. Sie kann nicht geändert werden.
- *Kommentar*: Hier kann ein Kommentartext eingegeben werden.
- *Dieses System ist*: Hier wird eingestellt, wie die Zone auf diesem System verwaltet wird.

  Wird dieses System zum *Master* der Zone, werden alle Einträge innerhalb der Zone auf diesem System verwaltet. Zusätzlich eingetragene sekundäre Slave-Server werden automatisch bei Änderungen der Daten informiert.

  Ist das System ein *Slave*, werden die Einträge in der Zone von einem *Master* geholt. Dieses System arbeitet nur als „Backup-System“ für die Zone. Dabei versucht es, einen „Zonentransfer“ durchzuführen, der von dem Master erlaubt werden muss.

  Wird hier *Forwarder* eingestellt, werden alle Anfragen zur Domain an diesen Forwarder geschickt. Im Unterschied zum Slave wird hier kein Transfer der ganzen Zone durchgeführt, sondern es werden nur die angefragten Einträge weitergeleitet.

Die Einstellung *Parent* ist notwendig, wenn die Zone selbst auf einem anderen DNS-Server verwaltet wird und dieses System gleichzeitig für die übergeordnete Zone zuständig ist. Dann muss auf dem System ein Verweis auf den oder die Nameserver dieser „Subdomain" vorhanden sein.

- *IP-Adresse des primären DNS-Servers*: Hier wird die IP-Adresse des zuständigen Nameservers für die Zone angegeben.
- *IP-Adresse des sekundären DNS-Servers*: Hier kann ein zusätzlicher Nameserver angegeben werden, der bei einem Ausfall des ersten DNS-Servers die Namensauflösung übernimmt.
- *Auto MX*: Wenn diese Option aktiviert ist und eine lokale Maildomain existiert, deren Name mit dem Namen dieser Zone übereinstimmt, wird der angegebene Mailserver und/oder dieses System als MX („Mail-Exchanger") eingetragen.

  Bleibt diese Option deaktiviert, können die MX-Einträge manuell vorgenommen werden.
- *Hidden Primary*: Normalerweise trägt sich der Master einer Zone selbst in die Zone als zuständiger DNS-Server ein. Wenn als verantwortliche Nameserver allerdings zwei andere Systeme genutzt werden (etwa zwei Server bei einem Provider), sollten diese in den Zonendaten aufgeführt werden und dieses System selbst entfallen.

  Durch das Aktivieren dieser Option wird genau dies erreicht. Das lokale System verwaltet als primärer Server die Zonendaten, trägt aber zwei andere Systeme in die Zonendaten ein.

Tab *Sekundäre DNS-Server*, Abschnitt *Sekundäre DNS-Server* Spalten in der Tabelle

- *IP-Adresse*: Hier wird die IP-Adresse des sekundären DNS-Servers angegeben. Diese Angabe sorgt dafür, dass der sekundäre Server

über Änderungen an den Zonendaten informiert wird und erlaubt ihm, eine Kopie der kompletten Zonendatei anzufordern.

- *FQDN*: Hier wird der vollständige Name (inklusive Domain-Suffix) des sekundären DNS-Servers angegeben.

  Hinweis: Wird der Name des Servers nicht angegeben, wird er auch nicht als Nameserver in die Zone eingetragen, er erhält jedoch weiterhin Informationen über Änderungen und kann Zonentransfers durchführen. Dies kann für spezielle Konfigurationen sinnvoll sein, im Allgemeinen sollte der Name jedoch angegeben werden.

Aktionen für jeden Tabelleneintrag

- *Löschen*: Mit dieser Aktion wird der zusätzliche sekundäre DNS-Server gelöscht.

Arbeitet das System als primärer DNS-Server für die Zone, können sekundäre Nameserver angelegt werden. Diese werden in die Zonendaten als zuständige Nameserver aufgenommen und erhalten die Berechtigung, einen „Zonentransfer“ durchzuführen. Bei Änderungen der Zoneneinträge werden sie von diesem System informiert.

Aktionen für diesen Dialog

- *Sekundären DNS-Server hinzufügen*: Mit dieser Aktion wird ein zusätzlicher sekundärer DNS-Server angelegt.

Tab *MX-Einträge*, Abschnitt *MX-Einträge (Mailrouting)* Spalten in der Tabelle

- *Host*: Hier wird der Name des Mailservers angegeben, der für diese Zone zuständig ist.

- *Wildcard*: Wird diese Option aktiviert, gilt dieser Eintrag auch für alle Subzonen.
- *Priorität*: Hier wird die Priorität angegeben, mit der der Nameserver verwendet werden soll. Niedrigere Zahlenwerte bedeuten eine höhere Priorität.

Aktionen für jeden Tabelleneintrag

- *Löschen*: Löscht den jeweiligen MX-Eintrag.

MX-Einträge in der Zone geben an, welcher Mailserver für E-Mails an Empfänger in dieser Domain zuständig ist. Dabei können auch mehrere Mailserver mit unterschiedlichen Prioritäten angegeben werden. Im V-Cube existiert mit der Option *Auto MX* ein Mechanismus, der MX-Einträge für auf dem System verwaltete Maildomains automatisch anlegt. Wird diese Option deaktiviert, können hier eigene MX-Einträge angelegt werden.

Aktionen für diesen Dialog

- *MX-Eintrag hinzufügen*: Diese Aktion legt einen neuen MX-Eintrag für diese Zone an.

Tab *SRV-Einträge*, Abschnitt *SRV-Einträge*
Spalten in der Tabelle

- *Dienst*: Hier wird der Dienst ausgewählt, für den ein SRV-Eintrag erstellt werden soll.
- *Host*: Hier wird der Name des Rechners angegeben, auf dem der Dienst läuft.
- *Priorität*: Hier wird die Priorität angegeben, mit der der Eintrag verwendet werden soll. Niedrigere Zahlenwerte bedeuten eine höhere Priorität.

- *Gewichtung*: Hier wird die Gewichtung angegeben, mit der dieser Eintrag verwendet werden soll. Wenn mehrere Einträge für einen Dienst mit gleicher Priorität vorhanden sind, erhält ein Server mit der höheren Gewichtung mehr Anfragen.

Aktionen für jeden Tabelleneintrag

- *Löschen*: Löscht den jeweiligen SRV-Eintrag.

SRV-Einträge sind ein weiterer Bestandteil des „zeroconf"-Systems. Über SRV-Einträge in der Zone können Authentifizierungsserver im Netz gefunden werden.

Hinweis: Werden mehrere Einträge für denselben Dienst in der Zone angegeben, müssen die entsprechenden Server auch den gleichen Datenstand haben. SRV-Einträge für die gesamte Zone sind nicht identisch mit den Einträgen, die für DNS-SD („DNS Service Discovery") benötigt werden.

Aktionen für diesen Dialog

- *SRV-Eintrag hinzufügen*: Mit dieser Aktion wird ein neuer SRV-Eintrag angelegt.

Tab *Extras*, Abschnitt *Zusätzliche Angaben*
Felder in diesem Abschnitt

- *Zusätzliche Angaben*: In diesem Eingabefeld können zusätzliche Einträge für die Zonendatei vorgenommen werden. Die Eingaben in diesem Feld werden hinter den SOA-Eintrag der Zonendatei kopiert.

  Hinweis: Fehlerhafte Einträge in diesem Feld können den Start des Nameservers verhindern.

- *Datei*: Alternativ zum Eingabefeld kann für den eigenen Konfigurationsabschnitt auch eine Datei importiert werden.

Aktionen für diesen Dialog

- *Importieren*: Mit dieser Funktion wird der Import der Konfiguration gestartet.

10.3.3 *Rückwärtszonen*

(Dieser Dialog befindet sich unter *Netzwerk – DNS – Rückwärtszonen*)

Eine „Rückwärtszone“ dient dazu, IP-Adressen in Hostnamen aufzulösen. Dazu wird die Domain „in-addr.arpa“ verwendet. Die Konfiguration einer „Reverse-Zone“ ist daher in vielen Belangen identisch mit einer normalen Zone.

Hinweis: Eine funktionierende Rückwärtsauflösung von IP-Adressen in Hostnamen sind im Internet für manche Dienste essenziell wichtig.

10.3.3.1 *Zone auswählen*

(Dieser Dialog befindet sich unter *Netzwerk – DNS – Rückwärtszonen*)

In diesem Dialog werden die angelegten Rückwärtszonen angezeigt und können bearbeitet werden. Weitere Zonen können angelegt werden.

In dieser Tabelle werden die angelegten Rückwärtszonen angezeigt.

Felder in diesem Dialog

- *Typ*: Hier wird die Art der Zone angezeigt.
- *Netzwerk*: Hier wird der Name des Netzwerks angezeigt, das zur Rückwärtszone gehört.
- *Kommentar*: Hier wird ein Kommentartext zu der Zone ausgegeben.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion wird die Zone bearbeitet.
- *Löschen*: Mit dieser Aktion wird die Zone gelöscht.

Aktionen für diesen Dialog

- *Hinzufügen*: Mit dieser Aktion wird eine neue Rückwärtszone angelegt.

10.3.3.2 *Rückwärtszone bearbeiten*

(Dieser Dialog befindet sich unter *Netzwerk – DNS – Rückwärtszonen*)

In diesen Dialogen werden die Einstellungen für die Rückwärtszonen vorgenommen.

Tab *Grundeinstellungen*
Felder in diesem Abschnitt

- *Netzwerk*: Hier wird das Netzwerk ausgewählt. Dabei stehen nur Netze zur Verfügung, die als Netzwerk auf dem System angelegt sind.

- *Netzwerk*: Wird eine Zone bearbeitet, wird das Netzwerk nur angezeigt. Es kann nicht mehr geändert werden.
- *Kommentar*: Hier kann ein Kommentartext zu der Zone angegeben werden.
- *Dieses System ist*: Hier wird eingestellt, wie die Zone auf diesem System verwaltet wird:

  Wird dieses System zum *Master* der Zone, werden alle Einträge innerhalb der Zone auf diesem System verwaltet. Zusätzlich eingetragene sekundäre Slave-Server werden automatisch bei Änderungen der Daten informiert.

  Ist das System ein *Slave*, werden die Einträge in der Zone von einem *Master* geholt. Dieses System arbeitet nur als „Backup-System“ für die Zone. Dabei versucht es, einen „Zonentransfer“ durchzuführen, der von dem Master erlaubt werden muss.

  Wird hier *Forwarder* eingestellt, werden alle Anfragen zur Domain an diesen Forwarder geschickt. Im Unterschied zum Slave wird hier kein Transfer der ganzen Zone durchgeführt, sondern es werden nur die angefragten Einträge weitergeleitet.

  Die Einstellung *Parent* ist notwendig, wenn die Zone selbst auf einem anderen DNS verwaltet wird und gleichzeitig dieses System für die übergeordnete Zone zuständig ist. Dann muss auf dem System ein Verweis auf den oder die Nameserver dieser „Subdomain“ vorhanden sein.
- *Primärer DNS-Server*: Hier wird die IP-Adresse des zuständigen Nameservers für die Zone angegeben.
- *Sekundärer DNS-Server*: Hier kann ein zusätzlicher Nameserver angegeben werden, der bei einem Ausfall des ersten DNS die Namensauflösung übernimmt.
- *Hidden Primary*: Normalerweise trägt sich der Master einer Zone selbst in die Zone als zuständiger DNS-Server ein. Wenn als verantwortliche Nameserver allerdings zwei andere Systeme

genutzt werden (etwa zwei Server bei einem Provider), sollten diese in den Zonendaten aufgeführt werden und dieses System selbst entfallen.

Durch das Aktivieren dieser Option wird genau dies erreicht: Das lokale System verwaltet als primärer Server die Zonendaten, trägt aber zwei andere Systeme in die Zonendaten ein.

Tab *Sekundäre DNS-Server*, Abschnitt *Sekundäre DNS-Server*

Spalten in der Tabelle

- *IP-Adresse*: Hier wird die IP-Adresse des sekundären DNS-Servers angegeben. Der sekundäre Server wird über Änderungen an den Zonendaten informiert und darf eine Kopie der kompletten Zonendatei anfordern.
- *FQDN*: Hier wird der vollständige Name (inklusive Domain-Suffix) des sekundären DNS-Servers angegeben.

  Hinweis: Wird der Name des Servers nicht angegeben, wird er nicht als Nameserver in die Zone eingetragen. Er erhält jedoch weiterhin Informationen über Änderungen und kann Zonentransfers durchführen. Dies kann für spezielle Konfigurationen sinnvoll sein, im Allgemeinen sollte der Namen jedoch angegeben werden.

Aktionen für jeden Tabelleneintrag

- *Löschen*: Mit dieser Aktion wird der zusätzliche sekundäre DNS-Server gelöscht.

Aktionen für diesen Dialog

- *Sekundären DNS hinzufügen*: Mit dieser Aktion wird ein zusätzlicher sekundärer DNS-Server angelegt.

Tab *Extras*, Abschnitt *Zusätzliche Angaben*
Felder in diesem Abschnitt

- *Zusätzliche Angaben*: In diesem Eingabefeld können zusätzliche Einträge für die Zonendatei vorgenommen werden. Die Eingaben in diesem Feld werden hinter den SOA-Eintrag der Zonendatei kopiert.

  Hinweis: Fehlerhafte Einträge in diesem Feld können den Start des Nameservers verhindern.
- *Datei*: Alternativ zum Eingabefeld kann für den eigenen Konfigurationsabschnitt auch eine Datei importiert werden.

Aktionen für diesen Dialog

- *Importieren*: Mit dieser Funktion wird der Import der Konfiguration gestartet.

10.3.4 *Hosts*

Als „Host“ werden einzelne Rechner bezeichnet, die dem V-Cube bekannt sind. Im einfachsten Fall muss nur die IP-Adresse eingetragen werden. Damit kann ein Host in den DNS eingetragen, überwacht oder in den *Benutzungsrichtlinien* einer Gruppe zugeordnet werden. Wird zusätzlich die MAC-Adresse angegeben, kann der Host mit DHCP seine IP-Adresse beziehen.

Wenn unter *Systembetrieb* die *passive Netzwerküberwachung* aktiviert wurde, kann in diesem Dialog über *Hosts importieren* eine Liste aller aktiven Systeme im Netz erstellt werden. Diese Systeme müssen zwar einzeln *bestätigt* werden, die aktuelle IP-Adresse sowie die MAC-Adresse sind allerdings bereits eingetragen.

10.3.4.1 *Übersicht*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Richtlinien – Hosts* sowie unter *Netzwerk – DNS – Hosts*)

In dieser Liste werden alle dem System bekannten Hosts im lokalen Netz angezeigt.

Felder in diesem Dialog

- *Hostname*: Hier wird der Name des Hosts angezeigt.
- *Zone*: Hier wird die zugehörige Zone angezeigt.
- *IP-Adresse*: Die IP-Adresse des Hosts.
- *MAC-Adresse*: Hier wird die Netzwerk-MAC-Adresse angezeigt.
- *Bestätigt*: Damit ein Host dauerhaft in die Liste aufgenommen wird und damit er überhaupt in der Konfiguration berücksichtigt wird, muss er *bestätigt* werden. Wenn ein Host automatisch importiert wird, ist diese Option zunächst deaktiviert.
- *AMT-Host*: Hier wird angezeigt, ob ein Rechner mit AMT-Unterstützung definiert wurde.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion können die Einstellungen zu einem Host bearbeitet werden.
- *Löschen*: Mit dieser Aktion wird ein Host gelöscht.

Aktionen für diesen Dialog

- *Hosts importieren*: Mit dieser Aktion werden alle derzeit aktiven Systeme im Netz, die von der passiven Netzwerküberwachung gefunden werden, in die angezeigte Liste importiert. Sie sind zunächst nicht *bestätigt* und müssen manuell übernommen werden.
- *Host anlegen*: Mit dieser Aktion wird ein neuer Eintrag für einen Host erzeugt.

10.3.4.2 *Eintrag bearbeiten*

(Dieser Dialog befindet sich unter *Benutzungsrichtlinien – Richtlinien – Hosts* sowie unter *Netzwerk – DNS – Hosts*)

In diesem Dialog werden die Einstellungen zu einem einzelnen System bearbeitet.

Tab *Grundeinstellungen*, Abschnitt *Grundeinstellungen*
Felder in diesem Abschnitt

- *ID*: Jeder auf dem V-Cube verwaltete Host wird intern unter einer eindeutigen ID verwaltet. Diese ID wird automatisch erzeugt und kann nicht geändert werden.
- *Hostname*: Der primäre Name des Hosts. Zusätzliche Namen können unter *DNS* im Feld *Aliasnamen* angegeben werden. Der Eintrag kann nur auf einen Hostnamen auflösen und liefert daher immer diesen Hostnamen.
- *Zuletzt aktiv*: Hier wird der Zeitpunkt angezeigt, an dem das System zuletzt erkannt wurde.
- *Bestätigt*: Damit ein Host in die aktive Konfiguration aufgenom-

men und im DNS eingetragen oder per DHCP mit einer IP-Adresse versorgt wird, muss er *bestätigt* werden.

Automatisch erkannte Systeme, die nicht bestätigt werden, werden nach einiger Zeit wieder gelöscht.

- *IP-Adresse*: Wenn dem Host eine bestimmte IP-Adresse zugewiesen werden soll, muss diese hier eingetragen werden.

  Bleibt das Feld leer und fragt der Host mit der passenden MAC-Adresse per DHCP an, bekommt er als Antwort eine IP-Adresse aus einem DHCP-Pool.
- *MAC-Adresse*: Wenn einem System im Netzwerk eine spezielle IP-Adresse zugewiesen werden soll, muss hier die MAC-Adresse eingetragen werden.
- *Wake-on-LAN nach Stromausfall*: Aufwecken eines Systems nach einem Stromausfall.

  Manche Systeme starten nach einem Stromausfall nicht wieder automatisch. Durch das Aktivieren dieser Option werden diese Systeme nach einem Stromausfall über das Netzwerk gestartet.

  Hinweis: Die „aufzuweckenden“ Systeme müssen über WOL-Funktionalität („Wake On LAN“) verfügen. Die MAC-Adresse des aufzuweckenden Systems muss bekannt sein.

Tab *Gruppenzugehörigkeit*, Abschnitt *Gruppenzugehörigkeit*
Felder in diesem Abschnitt

- *Einstellungen*: Ein Host kann direkt als Mitglied in ausgewählte Gruppen aufgenommen werden. Damit erhält er Zugriffsrechte auf verschiedene Dienste im V-Cube.

Tab *DNS*, Abschnitt *DNS*
Felder in diesem Abschnitt

- *Zone*: Hier wird eine DNS-Zone für das System ausgewählt. Zur Auswahl stehen die Zonen, die im Dialog *DNS-Zonen* konfiguriert wurden.
- *Aliasnamen*: Wenn der Rechner unter weiteren Namen bekannt sein soll, können diese, durch Leerzeichen getrennt, hier eingegeben werden. Endet der Name mit einem Punkt „.“, wird er als FQDN aufgefasst und in der entsprechenden Zone eingetragen, andernfalls wird der Name um die Zone erweitert.

  Wenn beispielsweise der Rechner „web01“ in der Zone „example.com“ angelegt wurde und der Alias „www“ gesetzt wurde, wird der Name zu „www.example.com“ erweitert.

  Aliase werden nur in den Zonen eingetragen, die als *Master* konfiguriert sind. Mehrere Namen werden durch Leerzeichen getrennt.
- *TTL*: Die Zeitspanne in Sekunden, für die die Angaben gültig sein sollen. Clients dürfen Anfragen für diese Zeit zwischenspeichern, ohne beim Server nochmals anzufragen. Wird hier nichts angegeben, wird als Voreinstellung der Wert 86400 s (ein Tag) eingesetzt.

Tab *DHCP*, Abschnitt *DHCP*
Felder in diesem Abschnitt

- *DHCP-Pool*: Soll dem System eine IP-Adresse automatisch zugewiesen werden, muss hier der Pool ausgewählt werden, aus dem eine IP-Adresse verwendet werden soll.

  Hinweis: Bleibt dieses Feld leer, kann die IP-Adresse nicht automatisch zugewiesen werden.

- *DHCP-Optionsgruppe*: Spezielle Optionen für DHCP können angegeben werden, indem Optionen für eine Gerätegruppe definiert werden und diese Gruppe hier ausgewählt wird.

Tab *Netzwerktests*, Abschnitt *Netzwerktests*

Hier können für den definierten Host Tests zur Überwachung aktiviert werden.

Spalten in der Tabelle

- *Test*: Durch das Aktivieren dieses Feldes wird der Dienst überwacht.
- *Dienst:* Hier wird der jeweilige Dienst angezeigt, der überwacht werden kann.
- *Extra:* In diesen Feldern können zusätzliche Parameter für den Test angegeben werden.
- *Port:* Hier kann die Portnummer angegeben werden, auf der der Dienst geprüft werden soll. Dies ist wichtig, wenn ein Dienst nicht auf dem gewöhnlichen Port läuft.
- *Host:* Hier kann eine gesonderte IP-Adresse angegeben werden, auf der der Dienst geprüft werden soll.
- *URL:* Hier kann eine URL angegeben werden, die bei der Überprüfung abgefragt werden soll.
- *Benutzer:* Bei Diensten, die eine Authentifizierung erfordern, kann hier das Login angegeben werden.
- *Passwort:* Hier wird das zugehörige Passwort für die Authentifizierung an einem Dienst angegeben.
- *Parameter:* Für Tests für die Fernüberwachung über NRPE kann hier der entsprechende Testparameter angegeben werden. Mit dem Parameter „Mailqueue“ kann als Beispiel die Anzahl der E-

Mails in der E-Mail-Warteschlange eines entfernten Collax-Servers überprüft werden.

- *Prozess:* Sollen Prozesse eines Microsoft Windows-Betriebssystems geprüft werden, ist hier der entsprechende ausführbare Prozess anzugeben.

Für jeden Rechner können die Dienste angegeben werden, die auf ihre Funktionsfähigkeit hin überwacht werden sollen. Diese Dienste werden dann regelmäßig kontaktiert. Wird ein Dienst als nicht mehr funktionsfähig erkannt, wird ein Alarm ausgelöst.

Die Überwachung funktioniert nur für Rechner, die eine feste IP-Adresse haben.

Die einzelnen Tests können nicht alle Aspekte eines bestimmten Dienstes überprüfen. Wenn beispielsweise der Test für den Dienst SMTP aktiviert ist, wird geprüft, ob eine Verbindung zum Mailserver hergestellt werden kann und ob der Server eine sinnvolle Antwort liefert, es wird jedoch nicht versucht, tatsächlich eine E-Mail zu versenden. Es kann also grundsätzlich vorkommen, dass der Dienst nicht funktioniert, obwohl der Test erfolgreich war.

Felder in diesem Abschnitt

- *Alarmierungszeitraum*: In dieser Liste kann der Zeitraum ausgewählt werden, in dem die unten angegebenen Tests durchgeführt werden und einen Alarm auslösen. Dies ist nützlich, wenn das System nur zu bestimmten Zeiten eingeschaltet ist, etwa während der Bürozeiten.

  Bleibt das Feld leer, wird die Einstellung der zu alarmierenden Gruppe benutzt.
- *Erreichbar über*: Ist das System über ein anderes System, etwa einen Router, erreichbar, kann hier dieser andere Host ausgewählt werden. Bei einem Ausfall des anderen Hosts wird für

dieses System keine Überprüfung mehr durchgeführt und kein Alarm ausgelöst. Es wechselt in den Zustand „unbekannt“. Bei Rückkehr des anderen Hosts werden die Tests für dieses System wieder aufgenommen. *Nagios* nutzt diese Information außerdem zur Darstellung der Netzwerkkarte.

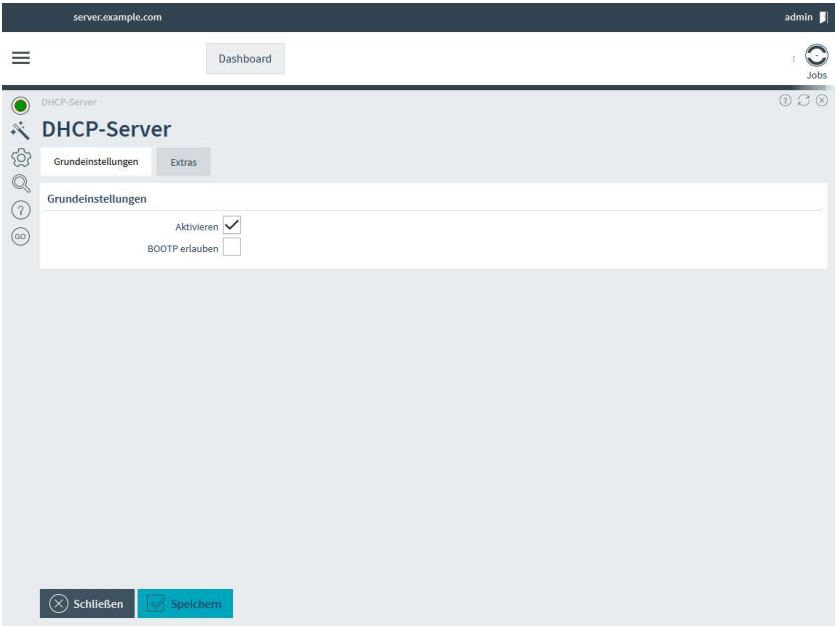
Bleibt das Feld leer, wird versucht, anhand der Routinginformationen den richtigen Router für den Rechner zu finden. Dies funktioniert allerdings nur, wenn der Host lediglich über einen einzigen anderen Router erreicht werden kann.

Wenn jedoch mehrere Router zwischen diesem System und dem Host liegen, sollte hier der letzte bekannte „Hop“ zum gewünschten Host angegeben werden. Wenn der Host „X“ über die Strecke „A“ – „B“ – „C“ erreichbar ist, muss hier „C“ angegeben werden. Für „C“ kann ebenfalls eine Überwachung angelegt werden, „C“ ist dann über „B“ erreichbar.

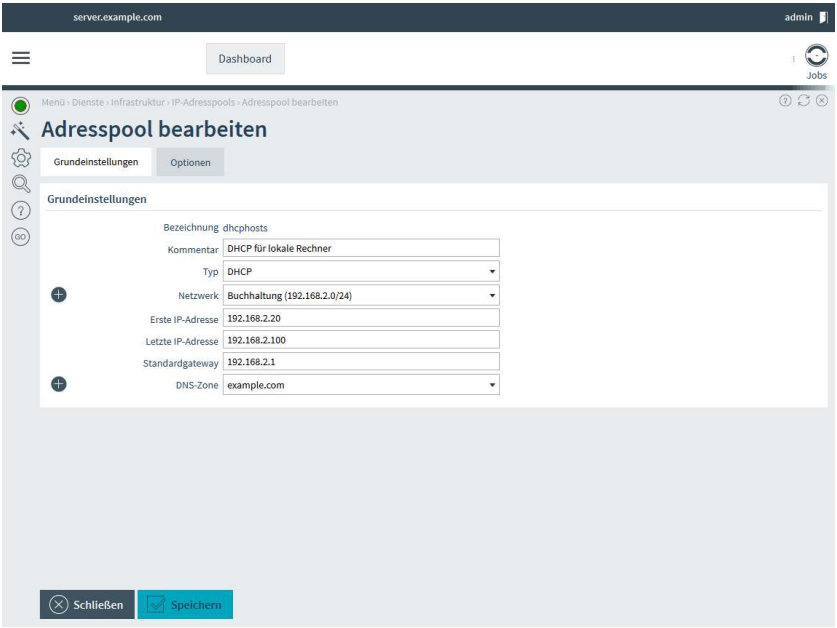
Tab *Netzwerktests*, Abschnitt *Hinweis*

Hier erscheint ein Hinweis zur Verwendung von NRPE-Checks.

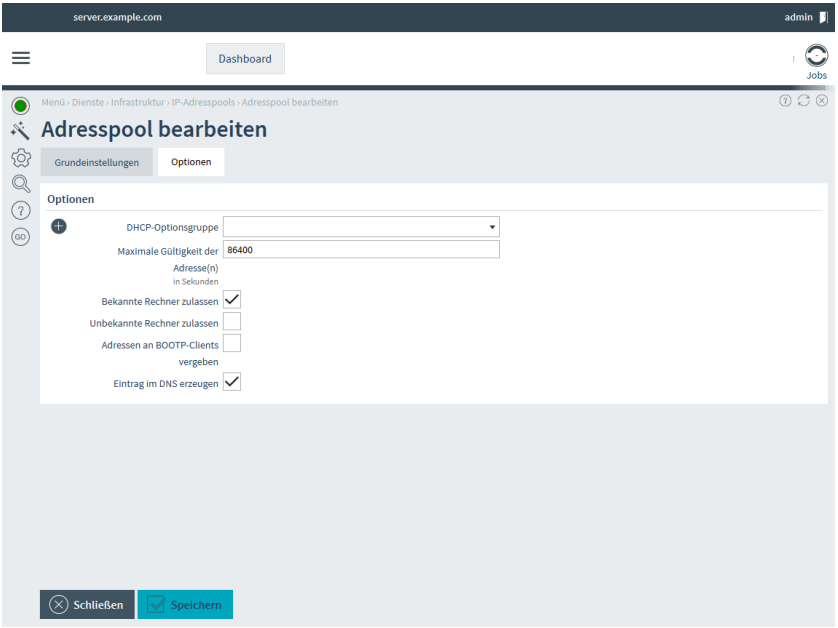
10.4 Schritt für Schritt: DHCP aktivieren



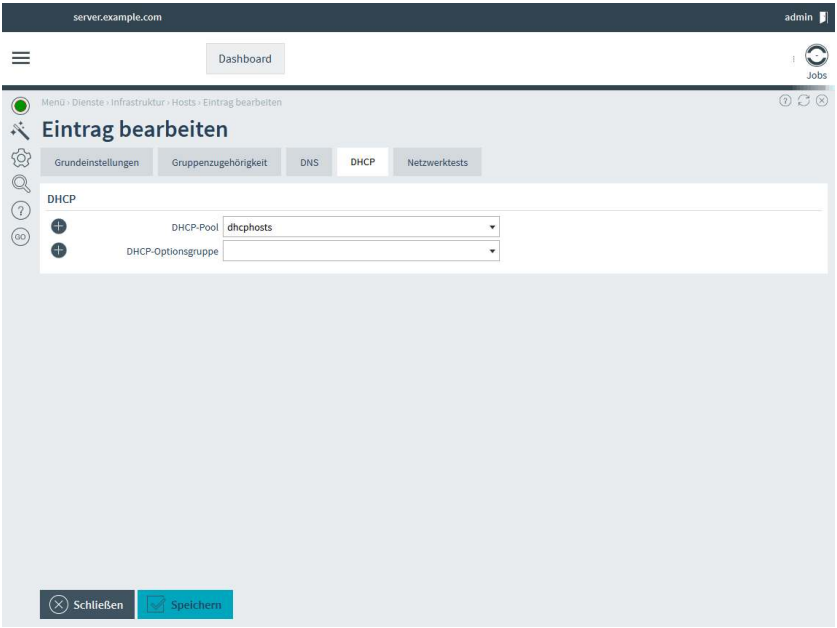
- Sie können den DHCP-Server unter *Netzwerk – DHCP – Allgemein* aktivieren.
- Die Option *BOOTP* wird nur benötigt, wenn Sie Systeme betreiben, die Ihr Betriebssystem über das Netzwerk booten. Lassen Sie sie daher zunächst deaktiviert.



- Wechseln Sie zu *Netzwerk – DHCP – IP-Adresspools*.
- Legen Sie einen neuen Pool an. Dabei handelt es sich um einen Adressbereich, aus dem der DHCP-Server IP-Adressen verteilen darf. Vergeben Sie keine IP-Adressen aus diesem Bereich manuell ohne Kenntnis des DHCP-Servers.
- Wählen Sie unter *Netzwerk* das *LocalNet* aus. Nur auf den Netzwerkschnittstellen, auf denen dieses Netz erreichbar ist, wird der V-Cube später DHCP-Anfragen beantworten.
- Mit der Angabe von *Erster* und *Letzter IP-Adresse* legen Sie den Bereich für den DHCP-Server fest.
- Unter *Standard-Gateway* geben Sie die IP-Adresse an, die per DHCP als Gateway an die Clients übermittelt wird.
- Unter *DNS-Zone* wählen Sie Ihre interne DNS-Zone aus.



- Wechseln Sie auf den Reiter *Optionen*.
- Aktivieren Sie die Option *Bekannte Rechner zulassen*, um später einzelnen Hosts immer die gleiche IP-Adresse zuweisen zu können.
- Haben Sie die Hosts im lokalen Netz noch nicht alle erfasst, aktivieren Sie den Eintrag *Unbekannte Rechner zulassen*. Aktivieren Sie dann auch *Eintrag im DNS erzeugen*.



- Um einzelne Systeme immer mit der gleichen IP-Adresse zu versorgen, muss die MAC-Adresse im V-Cube hinterlegt werden. Wechseln Sie dazu nach *Netzwerk – DNS – Hosts*.
- Wählen Sie ein System zur Bearbeitung aus oder legen Sie ein neues an.
- Wechseln Sie auf den Reiter *DHCP*.
- Wählen Sie hier den passenden *DHCP-Pool*.
- Geben Sie die *MAC-Adresse* des Systems ein.

Wenn Sie eine Anzahl von vorhandenen PCs erfassen möchten, können Sie unter *Überwachung – Passiv* die *Passive Netzwerküberwachung* aktivieren und nach einer gewissen Zeitspanne die Funktion *Hosts importieren* auslösen. Dadurch werden alle Systeme, die der V-Cube auf seinen Netzwerkschnittstellen erkannt hat, als Vorschläge importiert. Sie müssen nur noch einzeln *bestätigt* werden, IP- und MAC-Adressen sind jedoch bereits ausgefüllt.

10.5 GUI-Referenz: DHCP

10.5.1 *DHCP-Server*

(Dieser Dialog befindet sich unter *Netzwerk – DHCP – Allgemein*)

Der DHCP-Server dient dazu, den Systemen im lokalen Netz beim Starten eine IP-Adresse zuzuteilen und die Netzwerkkonfiguration zu übermitteln.

10.5.1.1 Tab *Grundeinstellungen*, Abschnitt *Grundeinstellungen* Felder in diesem Abschnitt

- *Aktivieren*: Durch das Aktivieren dieser Option wird der DHCP-Dienst auf diesem System gestartet.
- *BOOTP erlauben*: BOOTP ist der Vorläufer von DHCP, es gibt aber immer noch Clients, die dieses Protokoll benötigen. Mit dieser Option wird die Unterstützung für das BOOTP-Protokoll aktiviert.

10.5.1.2 Tab *Extras*, Abschnitt *Zusätzliche Angaben* Felder in diesem Abschnitt

- *Zusätzliche Angaben*: In diesem Eingabefeld können zusätzliche Einträge vorgenommen werden, die an den Anfang der Konfigurationsdatei des DHCP-Dienstes eingefügt werden.

  So können spezielle Optionen gesetzt werden, die über die Oberfläche nicht einstellbar sind.

  Hinweis: Fehlerhafte Einträge in diesem Feld können den Start des DHCP-Dienstes verhindern.

- *Datei*: Alternativ zum Eingabefeld kann für den Konfigurationsabschnitt auch eine Datei importiert werden.

Aktionen für diesen Dialog

- *Importieren*: Mit dieser Funktion wird der Import der Konfiguration gestartet.

10.5.2 *IP-Adresspools*

(Dieser Dialog befindet sich unter *Netzwerk – DHCP – IP-Adresspools*)

Der DHCP-Dienst vergibt IP-Adressen nur aus festgelegten Bereichen, den sogenannten „IP-Adresspools“. Für jedes angelegte Netzwerk können Pools angelegt werden.

DHCP-Anfragen werden nur innerhalb eines Netzwerksegments verschickt. Aus anderen Netzwerken sind DHCP-Anfragen nur mit Zusatzmodulen auf dem jeweiligen Router möglich.

10.5.2.1 *Adresspool wählen*

(Dieser Dialog befindet sich unter *Netzwerk – DHCP – IP-Adresspools*)

In diesem Dialog werden die angelegten Pools angezeigt. Hier können neue Pools angelegt sowie bestehende bearbeitet oder gelöscht werden.

Felder in diesem Dialog

- *Bezeichnung*: Hier wird die Bezeichnung des Adresspools angezeigt.
- *Typ*: In diesem Feld wird die Art des Pools angezeigt. Der Typ *DHCP* gibt an, dass Adressen aus diesem Pool über DHCP vergeben werden.
- *Kommentar*: Hier wird der Kommentartext zum Pool angezeigt.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion wird der Dialog zum Bearbeiten eines Pools geöffnet.
- *Löschen*: Diese Aktion löscht den ausgewählten Pool.
  Hinweis: Ein Pool kann nicht gelöscht werden, solange Clients noch IP-Adressen aus diesem Pool verwenden.

Aktionen für diesen Dialog

- *Adresspool anlegen*: Mit dieser Aktion wird ein neuer Pool von IP-Adressen angelegt.

10.5.2.2 *Adresspool bearbeiten*

(Dieser Dialog befindet sich unter *Netzwerk – DHCP – IP-Adresspools*)

In diesem Dialog werden die Einstellungen für einen Adresspool bearbeitet.

Tab *Grundeinstellungen*, Abschnitt *Grundeinstellungen* Felder in diesem Abschnitt

- *Bezeichnung*: Hier wird der Name des Pools eingegeben.
- *Bezeichnung*: Wird ein bereits vorhandener Pool bearbeitet, kann die Bezeichnung des Pools nicht mehr geändert werden. Hier wird die Bezeichnung nur angezeigt.
- *Kommentar*: In diesem Feld kann ein Kommentartext zu diesem Pool eingegeben werden.
- *Typ*: Hier wird festgelegt, welcher Dienst den Pool nutzen kann. Als Typen sind *DHCP* oder *L2TP/PPTP* möglich.
- *Netzwerk*: Hier muss das Netzwerk ausgewählt werden. Abhängig von den angelegten Links wird damit das Interface ausgewählt, auf dem auch die DHCP-Anfragen beantwortet werden.
- *Erste IP-Adresse*: Hier wird die erste IP-Adresse für diesen Adresspool angegeben.

  Wird hier keine Adresse angegeben, wird die kleinste mögliche Adresse verwendet.
- *Letzte IP-Adresse*: Hier wird die letzte IP-Adresse für diesen Adresspool angegeben.

  Wird hier keine Adresse angegeben, wird die größte mögliche Adresse verwendet.
- *Standardgateway*: Hier wird die Adresse des „Default-Gateways“ angegeben. Dieses wird per DHCP an die Clients übermittelt.

  Hinweis: Diese IP-Adresse muss im gleichen Subnetz liegen, aus dem die Adressen verteilt werden. Andernfalls können die Clients dieses Gateway nicht erreichen.
- *DNS-Zone*: Hier kann eine der DNS-Zonen ausgewählt werden, die in der Zonenkonfiguration angelegt sind.

  Diese Zone wird benötigt, um Rechnern mit dynamisch zugewiesenen Namen auch eine Domain zuordnen zu können. Auch

die zugewiesenen Nameserver werden aus der Zonendefinition übernommen.

Tab *Optionen*, Abschnitt *Optionen*
Felder in diesem Abschnitt

- *DHCP-Optionsgruppe*: Hier kann eine Optionsgruppe ausgewählt werden, die für diesen Pool verwendet wird. Über eine solche Optionsgruppe kann ein System über das Netzwerk einen *Kernel* mit Betriebssystem booten, etwa für plattenlose Clients.
- *Maximale Gültigkeit der Adresse(n)*: Mit diesem Parameter wird festgelegt, wie lange eine IP-Adresse aus diesem Pool höchstens gültig bleibt.
- *Bekannte Rechner zulassen*: Wird diese Option aktiviert, werden bekannten Rechnern (die als „Hosts“ angelegt sind) IP-Adressen aus diesem Pool zugewiesen.
- *Unbekannte Rechner zulassen*: Wird diese Option aktiviert, werden unbekannten Rechnern IP-Adressen aus diesem Pool zugewiesen.
- *Adressen an BOOTP-Clients vergeben*: Mit dieser Option werden IP-Adressen aus dem Pool an BOOTP-Clients vergeben.

  Hinweis: Adressen, die an BOOTP-Clients vergeben wurden, können nach Ablauf der maximalen Gültigkeitsdauer nicht zurückgezogen werden, da dies das BOOTP-Protokoll nicht vorsieht.
- *Eintrag im DNS erzeugen*: Wird diese Option aktiviert, wird für jede vergebene IP-Adresse ein Eintrag im Nameserver erzeugt.

10.5.3 *DHCP-Optionsgruppen*

(Dieser Dialog befindet sich unter *Netzwerk – DHCP – Optionsgruppen*)

In diesem Dialog können für Gruppen von Systemen oder für ganze Pools spezielle DHCP-Optionen angegeben werden.

10.5.3.1 *Optionsgruppe auswählen*

(Dieser Dialog befindet sich unter *Netzwerk – DHCP – Optionsgruppen*)

Felder in diesem Dialog

- *Bezeichnung*: Hier wird die Bezeichnung für die Optionsgruppe angezeigt.
- *Kommentar*: Hier wird der Kommentartext zu der Gruppe angezeigt.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion wird eine Optionsgruppe bearbeitet.
- *Löschen*: Diese Aktion löscht die Optionsgruppe.

Aktionen für diesen Dialog

- *Hinzufügen*: Mit dieser Aktion wird eine neue DHCP-Optionsgruppe hinzugefügt.

10.5.3.2 *DHCP-Optionsgruppe bearbeiten*

(Dieser Dialog befindet sich unter *Netzwerk – DHCP – Optionsgruppen*)

Tab *Grundeinstellungen*, Abschnitt *Grundeinstellungen* Felder in diesem Abschnitt

- *Bezeichnung*: Hier wird die Bezeichnung für die Gruppe angegeben.
- *Kommentar*: Hier kann ein Kommentartext zu dieser Gruppe angegeben werden.
- *TFTP-Server*: Hier wird die IP-Adresse des TFTP-Servers angegeben, von dem die Boot-Image-Datei geladen werden soll.
- *Boot-Image*: Hier muss der genaue Dateiname mit vollständigem Pfad zu der Boot-Image-Datei angegeben werden.
- *NFS-Root*: Als Boot-Image-Datei wird üblicherweise nur ein Betriebssystem-Kernel geladen. Um damit ein funktionsfähiges System zu erhalten, muss ein Dateisystem mit weiterer Software vorhanden sein. Bei Unix-/Linux-Systemen kann dieses Dateisystem über das Protokoll NFS über das Netzwerk eingebunden werden.

  In diesem Feld wird dazu der komplette NFS-Pfad angegeben. Wird kein Server vorangesetzt, wird das Verzeichnis auf diesem System gesucht. Um es von einem anderen Server zu verbinden, muss mit Doppelpunkt getrennt die IP-Nummer des NFS-Servers vorangestellt werden.

Tab *Extras*, Abschnitt *Zusätzliche Angaben*
Felder in diesem Abschnitt

- *Zusätzliche Angaben*: In diesem Eingabefeld können zusätzliche Einträge für diese Gerätegruppe vorgenommen werden. Die Eingaben in diesem Feld werden in die DHCP-Konfigurationsdatei eingefügt.

  Hinweis: Fehlerhafte Eingaben in diesem Feld können dazu führen, dass der DHCP-Server nicht mehr startet.

11 E-Mail

11.1 GUI-Referenz: *SMTP-Versand*

(Dieser Dialog befindet sich unter *Mail und Messaging – Mail – SMTP-Versand*

Dieser Dialog enthält die Basiseinstellungen für den allgemeinen Versand von E-Mails. Ist der Dienst nicht korrekt konfiguriert, kann das System keine eigenen Mails (etwa an den Administrator) versenden.

Soll dieser Dienst verschlüsselte Verbindungen über TLS verwenden, müssen zunächst eines oder mehrere Serverzertifikate erstellt oder installiert werden.

11.1.1 Felder in diesem Formular

- *Zertifikat*: Um TLS zu verwenden, kann für den SMTP-Dienst schon vorher ein Zertifikat erstellt oder importiert worden sein. In dieser Liste werden alle geeigneten Zertifikate auf dem System angezeigt. Hier wird das für den Mailserver entsprechende Zertifikat ausgewählt.

  Für abgehende und einkommende Verbindungen kann das gleiche Zertifikat verwendet werden, da es sich auch um den gleichen Mailserver handelt.

  Auch wenn kein Zertifikat ausgewählt wird, kann TLS für abgehende E-Mails verwendet werden.
- *TLS verwenden*: Hier wird eingestellt, ob und wann TLS für abgehende E-Mails verwendet werden soll. TLS dient zur

Verschlüsselung der SMTP-Sitzung und damit auch der Verschlüsselung der Authentifizierungsinformationen.

Niemals: Hier werden die Sitzungsinformationen im Klartext übertragen. Dies stellt kein Sicherheitsniveau dar, SMTP-Sitzungen funktionieren jedoch in den meisten aller Fälle.

Die Option *Wenn möglich* führt dazu, dass der Server TLS-Verschlüsselung verwendet, falls der Remoteserver dies ebenso unterstützt. Dies gilt als optimale Einstellung, da das Sicherheitsniveau bei Bedarf erhöht wird und gleichzeitig gewährleistet ist, dass E-Mails ins Internet ausgeliefert werden können.

Mit *Immer* und *Strikt* wird die TLS-Verschlüsselung der SMTP-Sitzung erzwungen, wobei *Strikt* zusätzlich den Namen des Remoteservers anhand der Zertifikatsinformationen prüft. Das Sicherheitsniveau ist damit hoch, allerdings sind diese Einstellungen für die Auslieferung von E-Mails ins Internet nicht geeignet.

- *Relay verwenden*: Diese Option muss aktiviert werden, wenn alle abgehenden E-Mails über einen bestimmten Relay-Server verschickt werden sollen.

  Dies ist meist dann der Fall, wenn die eigene Internetanbindung mit wechselnden IP-Nummern versehen ist. Dann kommt es meist zu Schwierigkeiten, E-Mails direkt selbst auszuliefern, da die aktuelle, eigene IP-Nummer bei manchen Mailservern geblockt sein kann. In diesem Fall wird alle ausgehende E-Mail immer an den Mailserver des Providers geschickt, der die E-Mail dann wiederum weiterleitet und zustellt („Relay-Server“).

  Ist diese Option nicht aktiviert, fragt der lokale SMTP-Server für jede Empfängerdomain im DNS den zuständigen Mailserver ab und baut eine SMTP-Verbindung zu ihm auf.
- *Relay-Host*: Soll ein Relay-Server verwendet werden, wird hier der Hostname (FQDN) oder die IP-Adresse dieses Servers eingetragen.
- *Port*: Soll ein Relay-Server verwendet werden, kann hier zusätz-

lich der Port des Relay-Hosts eingegeben werden, falls dieser vom Standard abweicht. Bleibt das Feld leer, wird der Standard-Port 25 für SMTP verwendet.

- *Benutzerkennung*: Verlangt der Relay-Server eine Authentifizierung, wird hier die Benutzerkennung zur Anmeldung hinterlegt.
- *Passwort*: Verlangt der Relay-Server eine Authentifizierung, wird hier das Passwort zur Anmeldung hinterlegt.
- *Maildomain*: Diese Domain wird bei abgehenden E-Mails angehängt, wenn der Absender keine Domain gesetzt hat. Dies ist insbesondere bei E-Mails der Fall, die vom System selbst generiert werden.

  Wird hier kein Eintrag ausgewählt, wird der Name dieses Systems (FQDN) verwendet. Dies kann jedoch zu Problemen führen, wenn Administrator-E-Mails an externe Empfänger weitergeleitet werden.
- *Wartezeit beim Versand*: Wenn hier eine Wartezeit eingetragen ist, wird der Versand von E-Mails entsprechend lange verzögert. Nach Ablauf der von der ersten E-Mail ausgelösten Zeitspanne werden alle E-Mails in der Mailqueue versendet. Dadurch kann bei Wählverbindungen die Anzahl der Verbindungen ins Internet reduziert werden.
- *Absenderdomain auf Maildomain umschreiben*: Durch das Aktivieren dieser Option wird in den E-Mails von Benutzern, die den Mailbox-Namen als Absenderadresse verwenden, die Absenderadresse so umgeschrieben, dass sie einer der „offiziellen“ E-Mail-Adressen entspricht.

  Wenn der Benutzer mehr als eine Aliasadresse hat (z. B. weil mehr als eine Maildomain verwendet wird), wird die erste im LDAP gefundene Adresse verwendet. Welche das ist, ist mehr oder weniger zufällig.
- *Alternativer SMTP-Servername*: Für die Kommunikation über SMTP

ist ein SMTP-Servername erforderlich. Soll der SMTP-Servername sich vom internen Hostnamen unterscheiden, ist hier der über externe DNS-Server auflösbarer Servername für den MX-Record einzutragen. Wird dieses Feld leergelassen, wird als SMTP-Servername der eingetragene FQDN dieses Servers verwendet.

11.1.2 Aktionen für dieses Formular

- *Abbrechen*: Bearbeiten von SMTP-Versand beenden. Die Änderungen werden verworfen.
- *Speichern*: Bearbeiten von SMTP-Versand beenden. Die Änderungen werden gespeichert.

12 Fileserver

12.1 Einführung

Über den Fileserver im V-Cube können Verzeichnisse zum Ablegen und Bereitstellen von Daten exportiert werden. Dafür stehen mehrere verschiedene Protokolle zur Verfügung, je nach gewünschtem Einsatzzweck. Ein solches Vereichnis wird auch als „Share“ oder „Freigabe“ bezeichnet.

Eine Freigabe kann gleichzeitig über unterschiedliche Protokolle in verschiedene Netze exportiert werden. So kann beispielsweise die Unternehmenswebseite im Internet mit HTTP oder HTTPS abgerufen und innerhalb des Unternehmens als Windows-Laufwerksfreigabe aktualisiert werden.

Über die *Benutzungsrichtlinien* werden Zugriffsberechtigungen auf die Freigaben und Größenlimits („Quotas“) gesetzt. Mittels Quota kann der maximal nutzbare Speicherplatz im System eingeschränkt werden. Es gibt einen Quotawert für Benutzer und einen zweiten für die Gruppe. Durch Nutzen von Quota wird vermieden, dass einzelne Benutzer den gesamten Festplattenplatz belegen können.

12.1.1 Unterstützte Protokolle

FTP ist ein sehr altes Protokoll zum Übertragen von Dateien. Es ist unverschlüsselt und wird heutzutage meist genutzt, um größere Datenbestände (Treiber und Softwarepakete) im Internet zugänglich zu machen.

SMB bzw. CIFS ist das unter Windows genutzte Verfahren zum

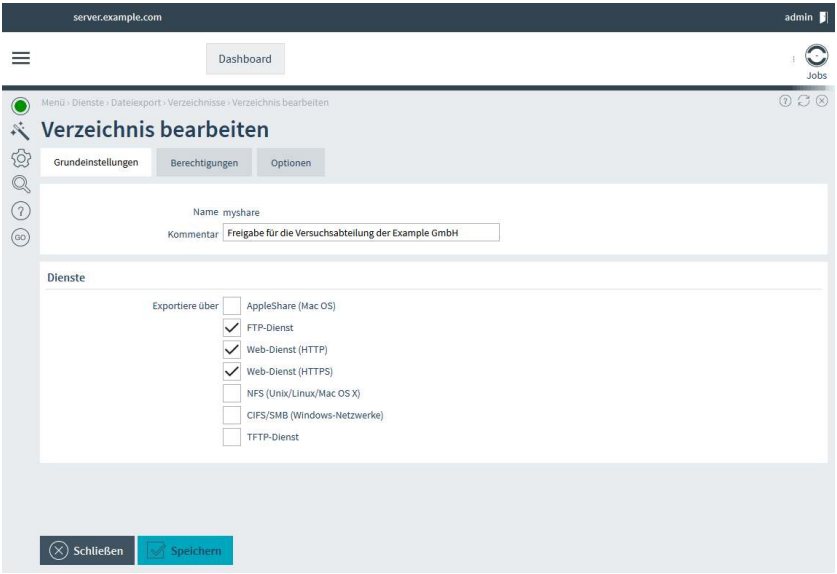
Austausch von Dateien und zur Unterstützung von Druckdiensten. Dieser Dienst arbeitet ohne Verschlüsselung und sollte nur im lokalen Netz eingesetzt werden.

NFS ist ein Protokoll zum Dateiaustausch in der Unix-Welt und wird von Linux, Unix und MacOS X unterstützt. Unter Windows kann es mit Zusatzsoftware genutzt werden. Dieses Protokoll ist unverschlüsselt und daher für den Einsatz im lokalen Netz geeignet.

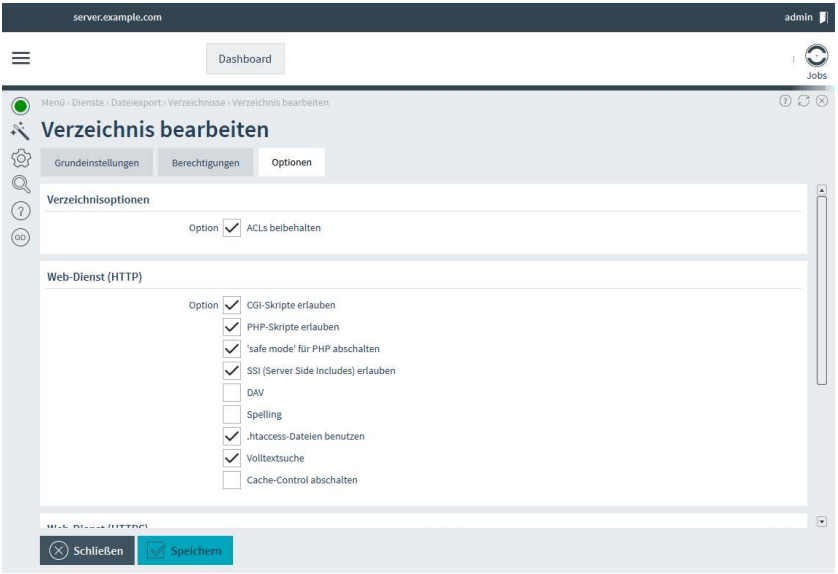
TFTP ist eine FTP-Variante mit eingeschränktem Funktionsumfang. Es wird hauptsächlich verwendet, um Konfigurationen und Softwareupdates auf Netzwerkkomponenten wie Switches und Router aufzuspielen. Die Daten werden unverschlüsselt übertragen, es sollte daher nur für öffentliche Daten oder im lokalen Netz verwendet werden.

12.2 Schritt für Schritt: Ein Share anlegen

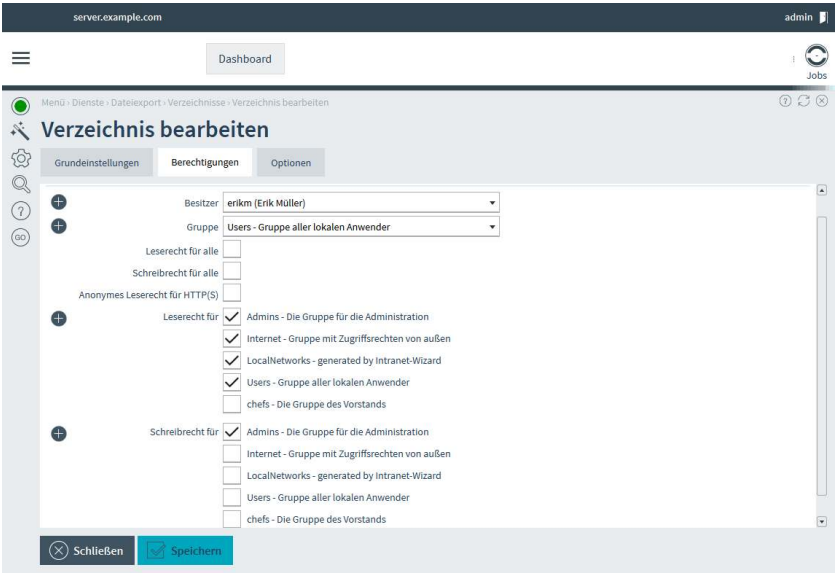
In diesem Beispiel soll ein Share angelegt werden, welches für Windows-Netze über SMB/CIFS und zuätzlich über HTTP exportiert wird. Damit dies möglich ist, müssen sowohl die Dienste *Windows-Networking* und *HTTP-Webserver* aktiviert sein.



- Rufen Sie unter *Serverdienste – File-Shares – Verzeichnisse* die Konfiguration der Shares auf.
- Legen Sie durch *Verzeichnis anlegen* ein neues Share an.
- Geben Sie dem Share einen *Namen*. Dieser kann später nicht mehr geändert werden.
- Unter *Dienste* wählen Sie die Dienste aus, über die das Share exportiert werden soll. Abhängig von den hier vorgenommenen Einstellungen werden unter dem Reiter *Optionen* weitere Einstellungen ein- bzw. ausgeblendet.
- Im Beispiel werden hier *CIFS/SMB* und *HTTP* aktiviert. Damit ist das Share über Fileserverdienste und zusätzlich über Webserver erreichbar.
- Zum Exportieren des Shares müssen Sie zusätzlich die jeweils erforderlichen Dienste wie Webserver, Windows-Fileserver usw. aktivieren.



- Wechseln Sie auf den Reiter *Optionen*.
- Aktivieren Sie *ACLs beibehalten*. In den ACLs werden u. a. die Windows-Dateiberechtigungen gespeichert.
- Mit *Share verstecken* können Sie das Share im Windows-Netz „unsichtbar“ machen, d. h., Nutzer können sich nur mit Kenntnis des Freigabenamens dorthin verbinden.
- Im Abschnitt *Web-Dienst (HTTP)* befinden sich einige Einstellungen für den Webserver. Aktivieren Sie *PHP-Skripte erlauben*, damit der Webserver später PHP-Skripte in diesem Verzeichnis ausführt. Andernfalls bietet er die PHP-Dateien zum Download an. Wenn Sie kein PHP nutzen möchten, lassen Sie die Option deaktiviert.
- Aktivieren Sie *Volltextsuche*, wenn Sie die Dateien im Share mit in die Suchmaschine des V-Cubes aufnehmen möchten. Diese ist über das User-Portal „Web-Access“ zugänglich.



- Wechseln Sie auf den Reiter *Berechtigungen*.
- Unter *Besitzer* wählen Sie aus den angelegten Benutzern denjenigen aus, der als Eigentümer des Shares fungieren soll.
- Unter *Gruppe* können Sie eine Gruppe auswählen. Bleibt das Feld leer, wird die Gruppe des *Besitzer* verwendet.
- Mit *Leserecht für alle* und *Schreibrecht für alle* wird anonymen Benutzern Zugriff auf das Share gewährt. Wenn Sie eine Authentifizierung wünschen, lassen Sie beide Punkte deaktiviert.
- Unter *Leserecht für* und *Schreibrecht für* wählen Sie die Gruppen aus, deren Mitglieder Zugriff auf das Share erhalten sollen. In der Abbildung wird die Gruppe *Users* genutzt, um Nutzern aus dem lokalen Netz den Zugriff zu erlauben.

12.3 GUI-Referenz: File-Shares

12.3.1 *Allgemein*

(Diese Option befindet sich im Zusatzmodul *Collax Network Storage*)

(Dieser Dialog befindet sich unter *Serverdienste – File-Shares – Allgemein*)

12.3.1.1 Felder in diesem Dialog

- *aTP-Logauswertung aktivieren*: Diese Option aktiviert die Logauswertung für den FTP-Server. Über die Logauswertung sind Statistiken über die Nutzung des FTP-Dienstes abrufbar.

12.3.2 *Verzeichnisse*

(Dieser Dialog befindet sich unter *Serverdienste – File-Shares – Verzeichnisse*)

In diesem Dialog werden Verzeichnisse („Shares“) verwaltet, die den Benutzern über das Netzwerk zur Verfügung gestellt werden.

12.3.2.1 *Verzeichnis wählen*

(Dieser Dialog befindet sich unter *Serverdienste – File-Shares – Verzeichnisse*)

In diesem Dialog kann ein bestehendes Verzeichnis bearbeitet

oder gelöscht werden, oder es kann ein neues Verzeichnis angelegt werden.

Felder in diesem Dialog

- *Name*: Hier wird der Name des Verzeichnisses angezeigt. Das Verzeichnis wird im Dateisystem des V-Cubes unterhalb von „/export“ angelegt.
- *Kommentar*: Hier wird ein Kommentartext zum Verzeichnis angezeigt.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion können die Einstellungen zu einem Verzeichnis bearbeitet werden.
- *Löschen*: Mit dieser Aktion wird das Verzeichnis gelöscht. Damit das Verzeichnis auf der Festplatte dieses Systems gelöscht werden kann, müssen zunächst alle Dateien manuell gelöscht werden.

Aktionen für diesen Dialog

- *Verzeichnis anlegen*: Mit dieser Aktion wird ein neues Verzeichnis angelegt.

12.3.2.2 *Verzeichnis bearbeiten*

(Dieser Dialog befindet sich unter *Serverdienste – File-Shares – Verzeichnisse*)

In diesem Dialog werden die Einstellungen für ein Verzeichnis bearbeitet.

Tab *Grundeinstellungen*
Felder in diesem Abschnitt

- *Name*: Hier wird der Name des Verzeichnisses angegeben. Das Verzeichnis wird unterhalb von „/export“ mit diesem Namen auf der Festplatte dieses Systems angelegt. Das Eingabefeld ist nur sichtbar, wenn ein neues Verzeichnis angelegt wird. Danach kann der Name des Verzeichnisses nicht mehr geändert werden.
- *Name*: Hier wird der Name eines bestehenden Verzeichnisses angezeigt.
- *Kommentar*: Hier kann ein Kommentartext zu diesem Verzeichnis eingegeben werden. Dieser erscheint u. a. in der Übersicht.

Tab *Grundeinstellungen*, Abschnitt *Dienste*
Felder in diesem Abschnitt

- *Exportiere über*: In dieser Liste sind alle Dienste und Protokolle aufgeführt, über die das Verzeichnis exportiert werden kann.
- *Exportiere über*: Über alle in dieser Liste aktivierten Dienste wird das Verzeichnis exportiert.

Tab *Berechtigungen*, Abschnitt *Berechtigungen*
Felder in diesem Abschnitt

- *Besitzer*: Hier kann der Eigentümer des Verzeichnisses festgelegt werden. Der eingetragene Benutzer erhält Lese-, Schreib-, und Ausführungsberechtigungen auf das Verzeichnis im System. Ist kein Benutzer angegeben, wird automatisch der Systembenutzer www-data mit eingeschränkten Rechten als Eigentümer eingetragen.
- *Gruppe*: Hier wird die Gruppe ausgewählt, der das Verzeichnis

zugeordnet wird. Wird keine Gruppe ausgewählt, wird automatisch die Gruppe des Besitzers verwendet.

- *Leserecht für alle*: Wird diese Option aktiviert, ist das Verzeichnis für jeden Benutzer lesbar, der auf dem V-Cube authentifiziert ist. Zusätzlich muss das Leserecht für alle Netzwerke erteilt werden, aus denen Anfragen zulässig sind.
- *Schreibrecht für alle*: Wird diese Option aktiviert, ist das Verzeichnis für jeden Benutzer beschreibbar, der auf dem V-Cube authentifiziert ist. Zusätzlich muss das Schreibrecht für alle Netzwerke erteilt werden, aus denen Anfragen zulässig sind. In der Regel wird dies das Internet sein. Das Schreibrecht schließt nicht automatisch das Leserecht mit ein.
- *Anonymes Leserecht für FTP*: Ist diese Einstellung aktiviert, wird das Verzeichnis per FTP für jeden anonymen Benutzer lesbar, d. h. für jede Anfrage, die den Account „anonymous“ verwendet. Zusätzlich muss das Leserecht für alle Netzwerke erteilt werden, aus denen Anfragen zulässig sind. In der Regel wird dies das Internet sein. Diese Einstellung ist geeignet, wenn zwischen Zugriff einer Gruppe und anonymem Zugriff unterschieden werden soll.
- *Anonymes Schreibrecht für FTP*: Ist diese Einstellung aktiviert, wird das Verzeichnis per FTP für jeden anonymen Benutzer beschreibbar, d. h. für jede Anfrage, die den Account „anonymous“ verwendet. Zusätzlich muss das Schreibrecht für alle Netzwerke erteilt werden, aus denen Anfragen zulässig sind. In der Regel wird dies das Internet sein. Das Schreibrecht schließt nicht automatisch das Leserecht mit ein. Diese Einstellung ist geeignet, wenn zwischen Zugriff einer Gruppe und anonymem Zugriff unterschieden werden soll.
- *Anonymes Leserecht für SMB*: Ist diese Einstellung aktiviert, wird das Verzeichnis per SMB für jeden anonymen Benutzer lesbar, d. h. für jede Anfrage, die den Account *GUEST* verwendet.

Zusätzlich muss das Leserecht für alle Netzwerke erteilt werden, aus denen Anfragen zulässig sind. Diese Einstellung ist geeignet, wenn zwischen Zugriff einer Gruppe und anonymem Zugriff unterschieden werden soll.

- *Anonymes Schreibrecht für SMB*: Ist diese Einstellung aktiviert, wird das Verzeichnis per SMB für jeden anonymen Benutzer beschreibbar, d. h. für jede Anfrage, die den Account *GUEST* verwendet. Zusätzlich muss das Schreibrecht für alle Netzwerke erteilt werden, aus denen Anfragen zulässig sind. Das Schreibrecht schließt nicht automatisch das Leserecht mit ein. Diese Einstellung ist geeignet, wenn zwischen Zugriff einer Gruppe und anonymem Zugriff unterschieden werden soll.
- *Leserecht für*: Benutzer, die zu einer der aktivierten Gruppen gehören, erhalten Leserecht auf das Verzeichnis.

  Gleichzeitig werden die Dienste, die das Verzeichnis freigeben, nur für Rechner und Netze zugänglich, die zu einer der aktivierten Gruppen gehören.
- *Schreibrecht für*: Benutzer, die zu einer der aktivierten Gruppen gehören, erhalten Schreibrecht auf das Verzeichnis.

  Gleichzeitig werden die Dienste, die das Verzeichnis freigeben, nur für Rechner und Netze zugänglich, die zu einer der aktivierten Gruppen gehören.

Tab *Optionen*
Felder in diesem Abschnitt

- *ACLs beibehalten*: Wird diese Option aktiviert, werden existierende ACLs in diesem Share nicht modifiziert; andernfalls werden die ACLs des übergeordneten Verzeichnisses auf alle Dateien und Unterverzeichnisse angewandt.
- *Share verstecken*: Bei der Freigabe des Verzeichnisses in Win-

dows-Netze über SMB kann das Verzeichnis unsichtbar exportiert werden. Dann ist zum Verbinden die Kenntnis des Namens des Verzeichnisses notwendig.

- *Resource-Fork für jede Datei anlegen*: Macintosh-Betriebsysteme speichern unstrukturierte Daten in Data-Forks und strukturierte Daten in Resource-Forks ab. Mit dieser Option wird für jede Datei ein Resoure-Fork erzeugt.

12.4 GUI-Referenz: *Antivirus Dateiprüfung*

(Dieser Dialog befindet sich unter *Serverdienste – File-Shares – Antivirus Dateiprüfung*)

12.4.1 Tab *Grundeinstellungen*, Abschnitt *Prüfung*

12.4.1.1 Felder in diesem Abschnitt

- *Aktivieren*: Hier kann die Filterung auf Viren für Dateien eingeschaltet werden. Voraussetzung dafür ist ein aktivierter Virenscanner.
- *E-Mail-Adresse des Virus-Administrators*: Hier wird eine E-Mail-Adresse für einen Administrator angegeben. Diese Administrator erhält Statusinformationen vom Virenfilter.
- *Infizierte Dateien*: Infizierte Dateien können durch unterschiedliche Methoden behandelt werden. Standardmäßig wird bei jeder Methode der Zugriff auf infizierte Dateien immer blockiert. Zusätzlich können infizierte Dateien in Quarantäne verschoben oder gelöscht werden.

12.4.2 Tab *Grundeinstellungen*, Abschnitt *Scanner Backends*

12.4.2.1 Felder in diesem Abschnitt

- *Benutze*: Hier werden Scanner ausgewählt, die für Dateifilterung eingesetzt werden sollen.

12.4.3 Tab *Grundeinstellungen*, Abschnitt *Benachrichtigung*

12.4.3.1 Felder in diesem Abschnitt

- *Benachrichtigung an*: Falls infizierte Dateien entdeckt werden kann hier gesteuert werden, an wen eine Benachrichtigunge erfolgen soll.

12.4.4 Tab *Grundeinstellungen*, Abschnitt *Quarantäneverzeichnis*

12.4.4.1 Felder in diesem Abschnitt

- *Exportiere über*: Um das Quarantäneverzeichnis im Netzwerk verfügbar zu machen, wird hier das gewünschte Protokoll eingestellt.
- *Automatisch löschen nach (Tage)*: Im administrativen Ordner abgelegte Dateien können nach Ablauf von den angegeben Tagen automatisch gelöscht werden.

12.4.5 Tab *Berechtigungen*, Abschnitt *Quarantäneverzeichnis*

12.4.5.1 Felder in diesem Abschnitt

- *Zugriff erlauben für*: Die ausgewählten Gruppenmitglieder, Benutzer und Netzwerke erhalten Zugriff auf das Quarantäneverzeichnis.

12.4.6 Tab *Verzeichnisse*, Abschnitt *Regelmäßig prüfen*

12.4.6.1 Felder in diesem Abschnitt

- *Diese Verzeichnisse regelmäßig prüfen*: Die gewählten Verzeichnisse werden einmal täglich auf Viren überprüft. Eine Statusmeldung wird an den Administrator gesendet.
- *Dateien in Heimatverzeichnissen regelmäßig prüfen*: Werden von Benutzern die Heimatverzeichnisse benutzt, können diese mit dieser Option ebenso auf Viren geprüft werden. Ist diese Option aktiviert, werden alle Systembenutzer als Lizenzbenutzer gerechnet.

12.4.7 Tab *Verzeichnisse*, Abschnitt *On-Access*

12.4.7.1 Felder in diesem Abschnitt

- *Dateien in diesem Verzeichnis bei Zugriff prüfen*: Werden vorhandene Dateien aufgerufen, können diese direkt beim Öffnen auf Viren gescannt (On-Access Scan) werden. Hier werden die gewünschten Verzeichnisse für den On-Access Scan ausgewählt.
- *Dateien in Heimatverzeichnissen bei Zugriff prüfen*: Werden von Benutzern die Heimatverzeichnisse benutzt, können diese mit dieser Option ebenso On-Access auf Viren geprüft werden. Ist

diese Option aktiviert, werden alle Systembenutzer als Lizenzbenutzer gerechnet.

12.4.8 Aktionen für dieses Formular

- *Abbrechen*: Beendet den Dialog, die Änderungen werden verworfen.
- *Speichern*: Beendet den Dialog, die Änderungen werden gespeichert.

13 Datensicherung

13.1 Bacula Datensicherung - Einführung

Regelmäßige Datensicherung ist die einzige Möglichkeit, bei unvorhersehbaren Ereignissen wie Hardwareschäden abgesichert zu sein. Der V-Cube unterstützt u. a. die Sicherung auf externe Bandlaufwerke sowie auf Laufwerksfreigaben anderer Server.

Die eingesetzte Backuplösung besteht aus zwei Komponenten: einem Client und einem Server. Beide Komponenten können auf ein und demselben System parallel eingesetzt werden.

13.2 Schritt für Schritt: Datensicherung auf Windows-Freigabe einrichten

13.2.1 Grundeinstellungen und Sicherungsziel

- Unter *E-Mail-Adresse des Operators* tragen Sie die Adresse ein, an die Benachrichtigungen vom Backupsystem geschickt werden sollen. Wenn Sie ein Bandlaufwerk nutzen, wird eine Aufforderung zum Bandwechsel an diese Adresse geschickt.
- Wechseln Sie zu *Datensicherung – Sicherungsziele*.
- Öffnen Sie über *Hinzufügen* den Dialog zum Anlegen eines neuen Sicherungsziels.
- Geben Sie einen *Name* und einen *Kommentar* ein. Der Name kann später nicht mehr geändert werden.
- Wählen Sie als *Typ* das Windows-Netzwerkprotokoll *Entfernte SMB-/CIFS-Freigabe* aus.

- Unter *Sichern auf Rechner* geben Sie den Hostnamen oder die IP-Adresse des Zielservers an.
- Unter *Verzeichnis* müssen Sie den Namen der auf dem Zielserver exportierten Freigabe angeben.
- Geben Sie den *Login* und das passende *Passwort* ein, um auf die Freigabe zuzugreifen.
- Die Option *Spooling aktivieren* bleibt für *Entfernte SMB-/CIFS-Freigabe* ausgeschaltet.

13.2.2 Sicherungsvorgang

- Wechseln Sie zu *Datensicherung – Sicherungspläne*.
- Öffnen Sie mit der Aktion *Hinzufügen* den Dialog zum Anlegen eines neuen Sicherungsplans.
- Geben Sie eine *Bezeichnung* und einen *Kommentar* ein. Die Bezeichnung kann später nicht mehr geändert werden.
- Fügen sie mit Klick auf *Sicherungsvorgang hinzufügen* einen neuen Vorgang in den Sicherungsplan ein.
- Geben Sie eine Bezeichnung für den *Volume-Pool* ein, der ausschließlich für Vollsicherungen verwendet werden soll.
- Wählen Sie als *Sicherungs-Level Vollsicherung* aus und geben Sie als *Zyklus Wöchentlich* beginnend ab *Wochentag Samstags* an.
- Eine Vollsicherung soll vier Zyklen lang aufbewahrt werden, bevor sie überschrieben werden darf. Geben Sie als *Aufbewahrungsdauer (Tage)* 27 an.
- Die Sicherung kann *um:* Uhr 2:00 standardmäßig stattfinden.
- Fügen sie mit Klick auf *Sicherungsvorgang hinzufügen* einen zweiten Vorgang in den Sicherungsplan ein.
- Geben Sie eine andere Bezeichnung für den *Volume-Pool* ein, der ausschließlich für differenzielle Sicherungen verwendet werden soll.

- Wählen Sie als *Sicherungs-Level Differenzielle Sicherung* aus und geben Sie als *Zyklus Täglich* beginnend *Am: Ganze Woche (Mo-So)* an.
- Auch diese Sicherung kann *um:* Uhr 2:00 standardmäßig stattfinden.

13.2.3 Zuordnung

- Wechseln Sie ins Formular *Datensicherung Zuordnungen*.
- Öffnen Sie mit der Aktion *Hinzufügen* eine neue Zuordnung zur Bearbeitung.
- Wählen Sie als *Quelle/Client* den lokalen Rechner aus.
- Wählen Sie als *Zu sichernde Daten Alles*.
- Als *Sicherungsplan* wählen Sie den zuvor erstellten Ablaufplan aus und geben danach das definierte SMB-CIFS- *Ziel* an.

Speichern Sie die Einstellungen und aktivieren Sie anschließend die vorgenommene Konfiguration.

13.3 GUI-Referenz: Datensicherung *Allgemein*

(Dieser Dialog befindet sich unter *Datensicherung – Allgemein*

13.3.1 Tab *Grundeinstellungen*, Abschnitt *Operator*

13.3.1.1 Felder in diesem Abschnitt

- *E-Mail-Adresse des Operators*: Statusmeldungen der Datensicherung werden an die hier eingetragene E-Mail-Adresse gesendet.

13.3.2 Tab *Grundeinstellungen*, Abschnitt *Fremder Backup-Server*

13.3.2.1 Felder in diesem Abschnitt

- *Erlaube Zugriff von fremdem Backup-Server*: Übernimmt ein anderer Collax Server die Sicherung lokaler Daten muss der Zugriff hier erlaubt werden.
- *Identifikator des Backup-Servers*: Der entfernte Sicherungsservers muss sich mit dem Identifikator am lokalen System ausweisen, um die Datensicherung übernehmen zu können.
- *Internes Passwort des lokalen Backup-Systems*: Zeigt das Passwort des lokalen Sicherungssystems. Wird verwendet bei Kommunikation zwischen mehreren Sicherungssystemen.
- *Identifikator des lokalen Backup-Systems*: Zeigt den Identifikator des lokalen Sicherungssystem. Wird bei Kommunikation mehrerer Sicherungssysteme verwendet.

13.3.3 Tab *Grundeinstellungen*, Abschnitt *Einstellungen*

13.3.3.1 Felder in diesem Abschnitt

- *Verhalten bei Platzbedarf*: Hier wird eingestellt, ob bei einem Sicherungsvorgang mit weiterem Platzbedarf die Medien automatisch erweitert werden können, oder ob dies von Hand durchgeführt werden soll.
- *Quota des Backup-Systems (GB)*: Größenbegrenzung für lokale Sicherung. Beschreibt den maximal zu belegenden Platz auf der Platte.
- *Detaillierte Dateilisten nach Datenwiederherstellung*: Nach einer durchgeführten Datenwiederherstellung wird eine E-Mail mit Statusinformation an den Backup-Administrator versendet. Ist diese Option gesetzt, wird zusätzlich eine Liste aller wiederhergestellten Dateien versendet. Diese Liste ist potenziell sehr lang.
- *Dateilistenabgleich bei Datensicherung (Accurate mode)*: Standardmäßig wird bei Inkrementellen Backups anhand des Änderungszeitpunktes der Datei entschieden ob eine Datei gesichert werden muss. Dadurch lässt sich nicht feststellen, welche Dateien seit dem letzten Backup gelöscht worden oder mit einem älteren Änderungsdatum hinzugefügt worden sind. Ist diese Option gesetzt, so werden auch diese Dateien mitgesichert, indem mit einer Liste aller Dateien des letzten Backups verglichen wird. Dabei ist zu beachten, dass der Ressourcenbedarf (CPU und Arbeitsspeicher) steigt.
- *Ziel für Recovery-Informationen*: Falls eine Zuordnung die für eine Wiederherstellung von Bandlaufwerken nötigen Verwaltungsdaten der Sicherungsprozesse mitsichert, lässt sich dafür mit dieser Option ein weiteres, separates Sicherungsziel festlegen. Auf dieses werden dann die Informationen über Kataloge und dergleichen gesichert, so dass Sicherungen auch nach einem

Komplettausfall von einem Tapelaufwerk zurückgespielt werden können. Für diese Option stehen nur dateibasierte Sicherungsziele zur Auswahl.

13.3.4 Tab *Grundeinstellungen*, Abschnitt *Kompression und Verschlüsselung*

13.3.4.1 Felder in diesem Abschnitt

- *Datenkompression*: Ist diese Option aktiviert, so werden alle Dateien mit GNU ZIP komprimiert. Dies geschieht auf Dateibasis, das heißt falls eine der Dateien unlesbar wird, so ist tatsächlich nur diese Datei betroffen und nicht alle Dateien einer Sicherung. Diese Einstellung sollte nur dann aktiviert werden, wenn das Sicherungsziel keine Hardwarekompression unterstützt.
- *Kompressionsstärke*: Daten können unterschiedlich stark komprimiert werden, was sich in Speicherbedarf und Rechenaufwand auswirkt. Bei der schnellsten Kompression (Wert 1) erhält man größere Dateien als bei einer langsamen Kompression (Wert 9). Es wird prinzipiell nicht empfohlen eine Kompressionsstärke größer als 6 zu wählen, da der Rechenaufwand unverhältnismäßig zum Platzersparnis wächst.
- *Zertifikat für Datenverschlüsselung*: Falls es gewünscht ist, dass sämtliche Daten bei Sicherungsvorgängen verschlüsselt und damit für dritte unleserlich gemacht werden, kann hier ein Zertifikat ausgewählt werden, das als Schlüssel verwendet werden soll. Beim Wiederherstellen werden die Dateisignaturen überprüft und der Vorgang bei Unstimmigkeiten unterbrochen. Metadaten einer Datei wie Pfadname und Berechtigungen werden dabei nicht mitverschlüsselt.
- *Master-Zertifikat*: Bei der Verschlüsselung von Sicherungen gilt es

zu beachten, dass diese nicht wiederherstellbar sind, wenn die Schlüssel verloren gegangen sind. Um das Risiko, Sicherungen aufgrund verloren gegangener Zertifikate nicht wieder herstellen zu können, zu minimieren, kann mit einem zweiten sogenannten Master-Zertifikat verschlüsselt werden. Im Falle von Master-Zertifikaten ist es empfehlenswert, den privaten Schlüssel nicht auf dem Server zu lagern, sondern diesen nur zu importieren, wenn tatsächlich ein Zertifikat verloren gegangen ist und Sicherungen nicht mehr anders wiederherzustellen sind.

13.3.5 Tab *Laufzeitbeschränkung*, Abschnitt *Laufzeitbeschränkung für Jobs*

13.3.5.1 Felder in diesem Abschnitt

- *Max. Startverzögerung (Stunden)*: Die maximale Startverzögerung, gibt an wie lange sich ein Job eines geplanten Sicherungsjobs verzögern darf, weil beispielsweise noch ein vorhergehender Job läuft
- *Max. Laufzeit (Stunden)*: Die maximale Laufzeit gibt an, wie lange ein Job aktiv sein darf.
- *Max. Wartezeit (Stunden)*: Innerhalb eines Jobs gibt die maximale Wartezeit an, wie lange ein Job unterbrochen werden darf, um zum Beispiel ein Band zu wechseln.
- *Max. Dauer (Stunden)*: Die maximale Dauer gibt an, wie lange ein Job inklusive Startverzögerung, Lauf- und Wartezeit überhaupt dauern darf, damit Jobs zum Beispiel nicht während der Arbeitszeit durchgeführt werden.

13.3.6 Tab *Berechtigungen*, Abschnitt *Zugriff erlauben für ...*

13.3.6.1 Felder in diesem Abschnitt

- *Bacula-Netzwerkzugriff*: Beschreibt die Berechtigungen für den Netzwerkzugriff wenn mehrer Sicherungssysteme verwendet werden.

13.3.7 Aktionen für dieses Formular

- *Passwort zurücksetzen*: Diese Aktion ändert das angegebene Passwort des lokalen Sicherungssystems. Wenn das Passwort schon zur Kommunikation verwendet wird, können nach Ausführen dieser Aktion Probleme auftauchen.
- *Abbrechen*: Bearbeiten der Allgemeinen Sicherungseinstellungen beenden. Die Änderungen werden verworfen.
- *Speichern*: Bearbeiten der Allgemeinen Sicherungseinstellungen beenden. Die Änderungen werden gespeichert.

13.4 GUI-Referenz: *Zuordnungen*

(Dieser Dialog befindet sich unter *Systembetrieb – Datensicherung – Zuordnungen* .)

Durch dieses Formular ist es möglich, sehr flexible Sicherungsabläufe zu definieren. Zuvor definierte Rechner, Ziele, Pläne und Datensätze können durch entsprechende Zuordnung auf die Anforderungen solcher Abläufe im lokalen Netzwerk angepasst werden. Eine Sicherung lokaler Daten auf entfernte Verzeichnisse wie auch die Sicherung von entfernten Arbeitsstationen auf lokal angeschlossene Bandlaufwerke sind möglich.

Zuordnungen sind zudem Voraussetzung, um Datenwiederherstellung, System-Recovery oder Monitor-Zugriff durchführen zu können.

13.4.1 Liste: *Zuordnungen*

In diesem Dialog werden alle angelegten Zuordnungen aufgelistet. Es können neue Zuordnungen hinzugefügt, editiert oder gelöscht werden.

13.4.1.1 Felder in diesem Formular

- *Bezeichnung*: Zeigt die Bezeichnung der Zuordnung.
- *Kommentar*: Weitere Beschreibung der Zuordnung.
- *Quelle*: Zeigt an, von welcher Quelle die Daten gesichert werden.
- *Ziel*: Zeigt an, wohin die Daten gesichert werden.

13.4.1.2 Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Durch Doppelklick oder Klick im Kontextmenü, kann ein ausgewählter Tabelleneintrag editiert werden.
- *Löschen*: Durch diese Aktion im Kontextmenü kann ein ausgewählter Tabelleneintrag gelöscht werden.

13.4.1.3 Aktionen für dieses Formular

- *Hinzufügen*: Mit dieser Aktion wird eine Zuordnung hinzugefügt.

13.4.2 *Zuordnung bearbeiten*

13.4.2.1 Abschnitt *Grundeinstellungen*

Felder in diesem Abschnitt

- *Bezeichnung*: Hier wird die Bezeichnung der Zuordnung eingegeben oder angezeigt.
- *Kommentar*: Weitere Beschreibungen können in diesem Feld hinzugefügt werden.

13.4.2.2 Abschnitt *Zuordnung*

Felder in diesem Abschnitt

- *Quelle/Client*: Hier wird ausgewählt, welcher Rechner gesichert werden soll.
- *Zu sichernde Daten*: Hier wird ausgewählt, welche Daten gesichert werden sollen. Wird der lokale Server gesichert, können einzelne Sicherungselemente unterschieden werden.
- *In die Sicherung aufnehmen*: Zeigt einzelne Sicherungselemente, die für die zu sichernden Daten ausgewählt werden können.
- *Sichere Zustand des Backup-Servers*: Verwaltungsdaten der Sicherungsprozesse können separat mit dieser Option gesichert werden.
- *Inhaltsliste*: Ist der zu sichernde Server oder Rechner kein V-Cube, ist eine zuvor zu definierende Inhaltsliste der zu sichernden Daten anzulegen. Diese spezielle Inhaltliste kann hier ausgewählt werden.
- *Sicherungsplan*: Ein zuvor erstellter Sicherungsplan kann hier verwendet werden, um festzulegen, wann über welchen Volume-Pool gesichert werden soll.
- *Ziel*: Hier wird ausgewählt, wohin gesichert werden soll.

- *Band nach Sicherung freigeben*: Wenn das Sicherungsziel ein Band ist, kann hier eingestellt werden, ob der Sicherungs-Job das Band automatisch freigibt, um es anschließend zurückzuspulen und auswerfen zu können. Wenn diese Option nicht gesetzt ist, kann das Band manuell unter *Datensicherung – Status und Betrieb* mit der Aktion *Aushängen* freigegeben werden.

  Soll das Band auch automatisch zurück gespult und ausgeworfen werden, kann die Option *Band wird nach Freigabe zurückgespult/ausgeworfen* bei den Einstellungen zum Sicherungsziel aktiviert werden.
- *Vor Sicherung Slot-Belegung bestimmen*: Wenn Bandmagazine für Sicherungen gewechselt werden müssen, muss dem Sicherungssystem vor der Sicherung die Slot-Belegung bekannt gegeben werden. Dies kann manuell geschehen, in dem im Formular *Status und Betrieb* die Aktion *Slot-Belegung bestimmen* ausgeführt wird. Mit der hier angegeben Option kann die Slot-Belegung für die definierte Sicherungszuordnung auch automatisch vor Start der Sicherung bestimmt werden. Können Barcodes zur Identifizierung der Bänder verwendet werden, ist die Bestimmung der Slot-Belegung sehr schnell abgeschlossen. Ist kein Barcode-Reader vorhanden, muss zur Bestimmung zunächst jedes Band an den Anfang zurückgespult werden. Dies dauert entsprechend länger als die Bestimmung anhand von Barcodes.

  Hinweis: Um die Bestimmung zeitlich zu steuern, kann eine separate Zuordnung ohne zu sichernde Komponenten definiert werden, welche die Slot-Belegung automatisch bestimmt.

13.4.2.3 Aktionen für dieses Formular

- *Abbrechen*: Bearbeiten der Zuordnung beenden. Die Änderungen werden verworfen.
- *Speichern*: Bearbeiten der Zuordnung beenden. Die Änderungen werden gespeichert.

13.5 GUI-Referenz: *Sicherungsziele*

(Dieser Dialog befindet sich unter *Datensicherung – Ziele*)

13.5.1 Liste: *Sicherungsziele*

13.5.1.1 Felder in diesem Formular

- *Bezeichnung*: Hier wird die Bezeichnung des Ziels angezeigt.
- *Kommentar*: Weitere Beschreibung des Ziels.
- *Typ*: Zeigt den Typ des Sicherungziels an.
- *Details*: Je nach Typ des Sicherungziels wird in dieser Spalte der entsprechende Systempfad oder der UNC-Pfad angezeigt.

13.5.1.2 Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Durch Doppelklick oder Klick im Kontextmenü, kann ein ausgewählter Tabelleneintrag editiert werden.
- *Ziel überprüfen (nur CIFS/NFS)*: Durch diese Aktion im Kontextmenü kann ein Schreibtest für CIFS und NFS Ziele durchgeführt werden.

- *Medien-Initialisierung und -Status*: Durch diese Aktion können Wechselmedien für VTL Initialisiert werden, oder der Status der Medien abgerufen werden.
- *Löschen*: Durch diese Aktion im Kontextmenü kann ein ausgewählter Tabelleneintrag gelöscht werden.

13.5.1.3 Aktionen für dieses Formular

- *Hinzufügen*: Mit dieser Aktion wird ein Sicherungsziel hinzugefügt.

13.5.2 *Ziel bearbeiten*

13.5.2.1 Abschnitt *Sicherungsziel*

Felder in diesem Abschnitt

- *Bezeichnung*: Hier wird die Bezeichnung des Ziels eingegeben oder angezeigt.
- *Kommentar*: Weitere Beschreibungen können in diesem Feld hinzugefügt werden.
- *Typ*: Hier wird die Art des Sicherungsziels ausgewählt, entsprechende individuelle Einstellungen sind vorzunehmen.

13.5.2.2 Abschnitt *Grundeinstellungen*

Felder in diesem Abschnitt

- *Spooling aktivieren*: Um die Sicherung auf Bandlaufwerke zu optimieren, kann hier Spooling aktiviert werden. Dadurch werden Daten zunächst in ein Spool-Verzeichnis geschrieben, bevor die Daten auf Band geschrieben werden.

- *Spool-Größe (GB)*: Gibt die maximale Größe des Spool-Verzeichnisses an.
- *Automatisch neue Medien belegen*: Ist diese Option aktiviert, so werden bei einer Sicherung bisher ungenutzte Mediendefinitionen automatisch auf freie Medien dieses Sicherungsziels angewendet. Um also einen vollständig automatisierten Ablauf zu gewährleisten, muss diese Option aktiviert und in den Grundeinstellungen unter "Verhalten bei Platzbedarf" der Punkt "Automatisch neue Mediendefinitionen anlegen" gewählt werden.

13.5.2.3 Abschnitt *Model/Typ*
Felder in diesem Abschnitt

- *Gerätemodell/Gerätetyp*: Je nach Bandlaufwerk kann hier der entsprechende Typ ausgewählt werden. Im Normalfall kann die Einstellung *Standard-Laufwerk* unverändert bleiben. Falls das Bandlaufwerk weder mit den Standardeinstellungen noch mit den vorhandenen Laufwerkstypen korrekt funktioniert, können Feineinstellungen mit dem *Expertenmodus* vorgenommen werden.

13.5.2.4 Abschnitt *Einstellungen für Bandlaufwerk*
Felder in diesem Abschnitt

- *Linux-Device-Name des Bandlaufwerks*: Ist ein Bandlaufwerk angeschlossen, muss hier der Linux-Gerätename eingetragen werden.

13.5.2.5 Abschnitt *Bandlaufwerk Detaileinstellungen*

Felder in diesem Abschnitt

- *Bandlaufwerk versteht "End of Medium"-Anfragen*: If No, the archive device is not required to support end of medium ioctl request, and the storage daemon will use the forward space file function to find the end of the recorded data. If Yes, the archive device must support the ioctl MTEOM call, which will position the tape to the end of the recorded data. In addition, your SCSI driver must keep track of the file number on the tape and report it back correctly by the MTIOCGET ioctl. Note, some SCSI drivers will correctly forward space to the end of the recorded data, but they do not keep track of the file number. Default setting for Hardware End of Medium is Yes. This function is used before appending to a tape to ensure that no previously written data is lost. We recommend if you have a non-standard or unusual tape drive that you use the btape program to test your drive to see whether or not it supports this function. All modern (after 1998) tape drives support this feature.
- *Bandlaufwerk kann schnell vorspulen*: If No, the archive device is not required to support keeping track of the file number (MTIOCGET ioctl) during forward space file. If Yes, the archive device must support the ioctl MTFSF call, which virtually all drivers support, but in addition, your SCSI driver must keep track of the file number on the tape and report it back correctly by the MTIOCGET ioctl. Note, some SCSI drivers will correctly forward space, but they do not keep track of the file number or more seriously, they do not report end of medium. Default setting for Fast Forward Space File is Yes.
- *Benutze MTIOCGET-Anfragen*: f No, the operating system is not required to support keeping track of the file number and repor-

ting it in the (MTIOCGET ioctl). The default is Yes. If you must set this to No, Bacula will do the proper file position determination, but it is very unfortunate because it means that tape movement is very inefficient.

- *BSF am Medienende*: If No, the default, no special action is taken by Bacula with the End of Medium (end of tape) is reached because the tape will be positioned after the last EOF tape mark, and Bacula can append to the tape as desired. However, on some systems, such as FreeBSD, when Bacula reads the End of Medium (end of tape), the tape will be positioned after the second EOF tape mark (two successive EOF marks indicated End of Medium). If Bacula appends from that point, all the appended data will be lost. The solution for such systems is to specify BSF at EOM which causes Bacula to backspace over the second EOF mark. Determination of whether or not you need this directive is done using the test command in the btape program.
- *Doppelte Medienende-Markierung*: If Yes, Bacula will write two end of file marks when terminating a tape -- i.e. after the last job or at the end of the medium. If No, the default, Bacula will only write one end of file to terminate the tape.
- *Laufwerk kann Records zurückspulen*: If Yes, the archive device supports the MTBSR ioctl to backspace records. If No, this call is not used and the device must be rewound and advanced forward to the desired position. Default is Yes for non random-access devices. This function if enabled is used at the end of a Volume after writing the end of file and any ANSI/IBM labels to determine whether or not the last block was written correctly. If you turn this function off, the test will not be done. This causes no harm as the re-read process is precautionary rather than required.
- *Laufwerk kann Dateien zurückspulen*: If Yes, the archive device

supports the MTBSF and MTBSF ioctls to backspace over an end of file mark and to the start of a file. If No, these calls are not used and the device must be rewound and advanced forward to the desired position. Default is Yes for non random-access devices.

- *Laufwerk kann Records vorspulen*: If Yes, the archive device must support the MTFSR ioctl to forward space over records. If No, data must be read in order to advance the position on the device. Default is Yes for non random-access devices.
- *Laufwerk kann Dateien vorspulen*: If Yes, the archive device must support the MTFSF ioctl to forward space by file marks. If No, data must be read to advance the position on the device. Default is Yes for non random-access devices.

13.5.2.6 Abschnitt *Einstellungen für Bandwechsler*

Felder in diesem Abschnitt

- *Gerät ist Bandwechsler*: Um einen Bandlaufwerk mit Bandwechsler korrekt anzusteuern, muss hier angegeben werden, dass das Gerät ein Bandwechsler ist.
- *Wechsler*: Hier ist der Geräte-Name des Bandwechslers auszuwählen.
- *Barcode-Leser*: Hier ist anzugeben, mit welcher Art Barcode-Leser das Bandwechselgerät ausgerüstet ist.
- *Forcierter Bandauswurf*: Für spezielle Bandwechselgeräte ist es erforderlich, das Band offline zu setzen, damit ein Wechselvorgang ausgeführt werden kann. Bandwechselgeräte des heutigen Standards benötigen diese Option üblicherweise nicht. Deshalb kann diese Option zuächst leergelassen werden.

13.5.2.7 Abschnitt *Band-Handhabung*
Felder in diesem Abschnitt

- *Band wird nach Freigabe zurückgespult/ausgeworfen*: Wenn das Laufwerk MTOFFL unterstützt, wird das Band mit dieser aktivierten Option nach abgeschlossenem Sicherungs-Job zurückgespult und ausgeworfen. Voraussetzung für den Auswurf des Bandes ist die gesetzte Option *Band nach Sicherung freigeben* in den Einstellungen einer Zuordnung.
- *Suche regelmäßig nach eingelegtem Band (in Sekunden)*: Der eingestellte Zeitwert gibt vor, in welchem Zyklus das Laufwerk nach einem neuen Band durchsucht wird. Mit dieser Option kann das neue Band eingelegt werden, der Sicherungsprozess erkennt dies und setzt die Sicherung automatisch fort.

13.5.2.8 Abschnitt *Einstellungen für CIFS-Sicherung*
Felder in diesem Abschnitt

- *Sichern auf Rechner*: Hier wird der Name oder die IP-Nummer des Systems angegeben, welches die Laufwerksfreigabe bereitstellt.
- *Verzeichnis*: Bei Sicherung per SMB/CIFS wird auf eine Freigabe des Zielrechners gesichert. Es kann Freigabe/Unterverzeichnis oder nur eine Freigabe hier angegeben werden. Auf dem Zielrechner wird das Unterverzeichnis automatisch angelegt.
- *Login*: Ist die Freigabe durch bestimmte Gruppenrechte geschützt, ist hier der passende Login-Name einzutragen, damit der V-Cube auf die Freigabe zugreifen kann.
- *Passwort*: Ist ein Login angegeben, sollte hier das entsprechende Passwort für einen korrekten Zugriff auf die Freigabe eingetragen werden.

13.5.2.9 Abschnitt *Einstellungen für NFS-Sicherung*

Felder in diesem Abschnitt

- *Sichern auf Rechner*: Hier wird der Name oder die IP-Nummer des Systems angegeben, welches das NFS-Verzeichnis bereitstellt.
- *Verzeichnis*: Hier wird das NFS-Verzeichnis angegeben.

13.5.2.10 Abschnitt *Einstellungen für USB- und ähnliche Ziele*

Felder in diesem Abschnitt

- *Partition*: Hier kann die Partition eines vorhandenen Medium ausgewählt werden. Als Medien können hier USB-, iSCSI-, eSATA-Festplatten oder Logische Volumes erkannt werden.

13.5.2.11 Abschnitt *Einstellungen für Virtual Tape Libraries mit Wechselmedien*

Felder in diesem Abschnitt

- : Hier wird ein Hinweis zur Benutzung des Assistenten angezeigt, wenn eine neues ziel erstellt werden soll.

Abschnitt *Medium*

Felder in diesem Abschnitt

- *Partition*: Sind Medien definiert, kann hier die gewünschte Partition gewählt werden.

Aktionen für diesen Abschnitt

- *Entfernen*: Mit dieser Aktion wird das Element gelöscht.

Aktionen für diesen Abschnitt

- *Medium hinzufügen*: Hier können Laufwerke als Wechselmedium hinzugefügt werden. Falls die Laufwerke nicht über den Assistenten vorbereitet werden, muss nach dem Abspeichern die Aktion Medien initialisieren im Kontextmenü ausgeführt werden.

13.5.2.12 Aktionen für dieses Formular

- *Abbrechen*: Bearbeiten des Sicherungsziels beenden. Die Änderungen werden verworfen.
- *Speichern*: Bearbeiten des Sicherungsziels beenden. Die Änderungen werden gespeichert.

13.6 GUI-Referenz: *Inhaltslisten*

(Diese Option befindet sich im Zusatzmodul *Collax Net Backup*)
(Dieser Dialog befindet sich unter *Systembetrieb – Datensicherung – Inhaltslisten*.)

Bei Sicherung von Arbeitsstationen sind zunächst Inhaltslisten zu definieren. Diese Listen geben vor, welche Dateien und Verzeichnis durch diesen Server von der Arbeitsstation gesichert werden sollen.

13.6.1 Liste: *Inhaltslisten*

Hier werden die angelegten Inhaltslisten tabellarisch angezeigt.

13.6.1.1 Felder in diesem Formular

- *Bezeichnung*: Diese Spalte zeigt die Bezeichnung der Inhaltsliste.
- *Kommentar*: Weitere Informationen stehen in diese Spalte.

13.6.1.2 Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Durch Doppelklick oder die Aktion im Kontextmenü kann ein Element bearbeitet werden.*
- *Löschen*: Durch diese Aktion im Kontextmenü wird das Element gelöscht.

13.6.1.3 Aktionen für dieses Formular

- *Hinzufügen*: Das Formular zur Definition von Inhaltslisten wird geöffnet.

13.6.2 *Inhaltsliste bearbeiten*

13.6.2.1 Abschnitt *Kennzeichnung*

Felder in diesem Abschnitt

- *Bezeichnung*: Hier wird die Bezeichnung der Inhaltsliste eingegeben oder angezeigt.
- *Kommentar*: Weitere Beschreibungen können in diesem Feld hinzugefügt werden.

13.6.2.2 Abschnitt *Inhalt*

Felder in diesem Abschnitt

- *Inhaltslistentyp*: Für Windows- oder Unix-Arbeitsstationen wird hier der Typ der Liste definiert. Bei Auswahl von *Dateiliste* werden die Laufwerke, Verzeichnisse und Dateien, sowie die nicht zu sichernden Elemente in der folgenden Textbox angegeben.

  Ist *Entfernte Dateiliste* gewählt, werden die Informationen über die zu sichernden und nicht zu sichernden Laufwerke und Dateien direkt aus einer Datein von der jeweiligen Arbeitsstation gelesen.

  Mit dem Typ *Applikationsspezifisch* kann nachfolgend eine Anwendung gewählt werden, deren Informationen von dem entsprechenden Client gesichert wird.
- *Zu sichernde Dateien*: Hier können die Laufwerke, die Verzeichnisse und Dateien für die Sicherung der Arbeitsstation angegeben. Wildcards sind bei der Angabe möglich.

  Hinweis: Bei Angabe von Windows-Verzeichnissen ist unbedingt der Schrägstrich statt des umgekehrten Schrägstrichs für die Trennung von Verzeichnissen zu verwenden.
- *Schließe Dateien aus*: Die hier angegebenen Dateien werden nicht

in die Sicherung mit einbezogen. Wildcards sind bei der Angabe möglich.

- *Lese Dateiliste aus Remote-Datei*: Hier wird eine Datei angegeben, die die Informationen über die zu sichernden Dateien enthält. Die Angabe ist mit kompletten Zielpfad einzugeben.
- *Lese Ausschlussliste aus Remote-Datei*: Hier wird eine Datei angegeben, die die Informationen über die nicht zu sichernden Dateien enthält. Die Angabe ist mit kompletten Zielpfad einzugeben.
- *Führe vor Sicherung aus*: Hier kann ein ausführbares Skript angegeben werden, das auf dem Zielrechner vor dem Start der Sicherung ausgeführt wird.

  Für Skripts unter Windows muss die Pfadangabe mit Schrägstrich erfolgen: „C:/Verzeichnis/skript.bat“.
- *Führe nach Sicherung aus*: Hier kann ein ausführbares Skript angegeben werden, das auf dem Zielrechner nach dem Abschluss der Sicherung ausgeführt wird.

  Für Skripts unter Windows muss die Pfadangabe mit Schrägstrich erfolgen: „C:/Verzeichnis/skript.bat“.
- *Volume Shadow Copy Support (für Windows-Clients)*: Optimierung für Sicherung von Windows-Arbeitsstationen.
- *Unterstützung für MacOS X-Clients*: Für die Optimierung der Sicherung von MacOS x-Arbeitsstationen.
- *Zu sichernde Applikation*: Soll Applikationsspezifisch gesichert werden, kann hier die Anwendung gewählt werden.

  Die Sicherung von *Microsoft Exchange Server 2003/2007* ist als Vollsicherung mit VSS möglich. Um nun inkrementelle oder differenzielle Sicherungen zu ermöglichen, oder die Möglichkeit zu bieten, einzelne Datenbanken wieder herzustellen, kann die applikationsspezifische Sicherung von Microsoft Exchange Server ausgewählt werden. Damit werden die gesamten oder bestimmte Storage Groups gesichert.

- *Beschränke auf Storage Group*: Hier kann eine bestimmte Storage Group des MS Exchange Servers angegeben werden. Wird hier kein Wert eingegeben, werden die gesamten Storage Groups gesichert.
- *Unterstützung für erweiterte Attribute*: Erweiterte Attribute beschreiben Metadaten von Dateien, die nicht vom Dateisystem intepretiert werden. Erweiterte Attribute werden überwiegend von Linux- und Unix-basierenden Betriebssystemen unterstützt (Linux, FreeBSD, OpenBSD, Max OS X, Solaris). Als erweitertes Attribut kann zum Beispiel die Autorin, die Prüfsumme oder die Zeichenkodierung einer Datei gesetzt sein. Mit dieser Option können diese erweiterten Attribute mitgesichert werden. Diese Option sollte nicht gesetzt werden, wenn Datenverschlüsselung für Sicherungen benutzt wird.

13.6.2.3 Aktionen für dieses Formular

- *Abbrechen*: Bearbeiten der Inhaltsliste beenden. Die Änderungen werden verworfen.
- *Speichern*: Bearbeiten der Inhaltsliste beenden. Die Änderungen werden gespeichert.

13.7 GUI-Referenz: *Clients*

(Diese Option befindet sich im Zusatzmodul *Collax Net Backup*)

(Dieser Dialog befindet sich unter *Systembetrieb – Datensicherung – Clients*.)

In diesem Formular werden Clients für die Datensicherung definiert. Als Client wird hier unter anderem eine Arbeitsstatione mit Windows-, Mac- oder Unix-Betriebssystem bezeichnet. Als Client versteht man auch einen weiteren Collax Server, der über diesen Server gesichert werden soll.

13.7.1 Liste: *Sicherungs-Clients*

Hier wird die Liste der definierten Arbeitsstationen oder Collax Server angezeigt.

13.7.1.1 Felder in diesem Formular

- *Identifikator*: Diese Spalte zeigt den Identifikator des Clients.
- *Kommentar*: Hier stehen weitere Informationen.
- *Rechnername*: Zeigt den Netzwerknamen oder IP-Adresse des Clients.
- *Passwort*: Zeigt das Passwort des Clients.

13.7.1.2 Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Durch Doppelklick oder die Aktion im Kontextmenü kann ein Element bearbeitet werden.
- *Löschen*: Durch diese Aktion im Kontextmenü wird das Element gelöscht.
- *Client-Konfigurationsdatei*: Hier kann eine Konfigurationsdatei für den Client heruntergeladen werden.

13.7.1.3 Aktionen für dieses Formular

- *Hinzufügen*: Das Formular zur Definition von Clients wird geöffnet.

13.7.2 *Sicherungs-Client bearbeiten*

13.7.2.1 Felder in diesem Formular

- *Identifikator*: Der Identifikator ist hier keine frei zu wählende Bezeichnung, sondern muss die tatsächliche Bezeichnung des Sicherungs-Clients beschreiben. Bei Collax Servern, die als Client gesichert werden sollen, kann der Identifikator in den Grundeinstellungen eingesehen werden.
- *Kommentar*: Zeigt eine weitere Beschreibung des Sicherungs-Clients.
- *Rechnername oder Adresse*: Hier wird der Netzwerkname oder die IP-Adresse des Clients, die einer netzwerkseitigen Verbindung dient, hinterlegt.
- *Passwort des Clients*: Für die vollständige Authorisierung muss hier noch das Passwort des Clients hinterlegt werden. Bei

Collax Servern, die als Client gesichert werden sollen, kann das Passwort in den Grundeinstellungen eingesehen werden.
- *Art des Backup-Clients*: Hier wird ausgewählt, ob der Client eine Standardarbeitsstation ist, oder ob ein Collax Server als Client gesichert werden soll.
- *Herunterladbare Konfigurationsdateien für*: Für die einfache Konfiguration eines Clients, gibt es die Möglichkeit vordefinierte Dateien für den jeweiligen Client herunterzuladen. Hier wird ausgewählt, für welchen Client-Typ diese Datei zur Verfügung gestellt werden soll.

13.7.2.2 Aktionen für dieses Formular

- *Abbrechen*: Bearbeiten des Clients beenden. Die Änderungen werden verworfen.
- *Speichern*: Bearbeiten des Clients beenden. Die Änderungen werden gespeichert.

13.7.3 *Download*

13.7.3.1 Felder in diesem Formular

- *Client-Konfigurationsdatei*: Wurde die Aktion *Client-Konfigurationsdatei* ausgeführt, wird dieses Formular angezeigt.

13.7.3.2 Aktionen für dieses Formular

- *Zurück*: Diese Aktion führt zurück zur Liste der Clients.

13.8 GUI-Referenz: *Pläne*

(Dieser Dialog befindet sich unter *Datensicherung – Pläne*)

In diesem Formular können Sicherungsvorgänge, Sicherungszeiten und Sicherungs-Level zu einem Plan verknüpft werden. Zudem ist es hier möglich, verschiedene Vorgänge auf verschiedene Volume-Pools sichern zu lassen. Dies ist letztendlich die Voraussetzung um das Vorhaben der Band-Rotation innerhalb einer Sicherungsstrategie umzusetzen, ebenso ist dadurch die Umsetzung von Sicherungsschemata, wie Türme-von-Hanoi, oder Großvater-Vater-Sohn, möglich.

Es wird empfohlen, zur Erstellung von Sicherungsplänen den Assistenten für Datensicherung zu benutzen. Die dort generierten Pläne können anschließend flexibel modifiziert werden.

13.8.1 Liste *Pläne*

Die Liste zeigt die definierten Sicherungspläne.

13.8.1.1 Felder in dieser Tabelle

- *Bezeichnung*: In dieser Spalte steht der Name des Sicherungsplans.
- *Kommentar*: Zeigt weitere Beschreibung des Plans.

13.8.1.2 Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion im Kontextmenü, oder mittels Doppel-Klick, kann der Eintrag bearbeitet werden.
- *Löschen*: Mit dieser Aktion im Kontextmenü kann der Eintrag gelöscht werden.

13.8.1.3 Aktionen für dieses Formular

- *Hinzufügen*: Das Formular für einen neuen Eintrag wird geöffnet.

13.8.2 *Plan bearbeiten*

13.8.2.1 *Plan bearbeiten*, Abschnitt *Grundeinstellungen*

Felder in diesem Abschnitt

- *Bezeichnung*: Hier wird der Name des Plans angezeigt oder eingegeben.
- *Kommentar*: Zusätzliche Informationen zu Plan können hier hinterlegt werden.

13.8.2.2 *Plan bearbeiten*, Abschnitt *Vorgang*

Felder in diesem Abschnitt

- *Volume-Pool*: Hier wird eine beliebige Bezeichnung für den Volume-Pool angegeben. Ein Volume-Pool ist eine Menge von Medien, die für die Sicherung in einem Vorgang verwendet wird. Es können verschiedene Volume-Pools über mehrere Sicherungsvorgänge definiert werden. Im einfachsten Fall wird ausschließlich ein Volume-Pool für alle Sicherungsvorgänge benutzt.

- *Aufbewahrungsdauer*: Dieser ganzzahlige Wert kennzeichnet die minimale Aufbewahrungsdauer in Tagen, bevor die gesicherten Daten überschrieben werden. Im einfachen Fall ist die Aufbewahrungsdauer genau der Zyklusdauer abzüglich einem Tag. Es besteht ein Datansatz, der innerhalb des nächsten Vorgangs überschrieben wird. Ist die Aufbewahrungsdauer zweimal so lange wie die Zyklusdauer, abzüglich einem Tag, so bestehen immer zwei Datensätze dieses Sicherungsvorgangs. Um einen Datensatz über 26 Wochen zu erhalten, wäre der Wert 181 in Verbindung mit einem wöchentlichen Zyklus zu setzen.

  Ein Wert der kleiner ist, als die Zyklusdauer, bedeutet, dass der Datensatz vor dem nächsten Vorgang zum Überschreiben freigegeben wird. Der Vorgang wird, wie vorgegeben, zum nächsten Zyklus ausgeführt.
- *Sicherungs-Level*: Es werden 3 Sicherungs-Level unterschieden.
  - Vollsicherung: Hier werden alle Daten gesichert, unabhängig vom Datum der letzten Sicherung innerhalb desselben Sicherungsplans.
  - Inkrementelle Sicherung: Bei der inkrementellen Sicherung werden alle Daten gesichert, die sich seit der letzten durchgeführten Sicherung innerhalb desselben Sicherungsplans verändert haben, oder die seit der letzten durchgeführten Sicherung innerhalb desselben Sicherungsplans neu hinzu gekommen sind.
  - Differenzielle Sicherung: Hier werden alle Daten gesichert, die sich seit der letzten Vollsicherung innerhalb desselben Sicherungsplan geänderten haben oder neu hinzugekommen sind.
- *Zyklus*: Hier wird die regelmäßige Wiederholung eines Sicherungsvorgangs festgelegt. Die längste Dauer eines Zyklus' beträgt ein Jahr, die kürzeste Dauer beträgt einen Tag.

- *Im:*: Angabe des Monats in dem der Vorgang ausgeführt werden soll, wenn die Zyklusdauer ein Jahr beträgt.
- *Am:*: Bestimmt den Tag der Durchführung, entweder absolut am ersten Tag des gewählten Monats, oder ein Wochentag einer bestimmten Woche innerhalb des gewählten Monats.
- *Für:*: Hier wird eine bestimmte Woche für die Durchführung gesetzt, wenn als Zyklus *In bestimmten Wochen* angegeben ist. Die Angabe der Wochen beziehen sich auf das laufende Kalenderjahr.
- *Wochentag*: Verwendung bei jährlichem, monatlichem oder wöchentlichem Zyklus.
- *Am:*: Der Vorgang kann Werktags oder jeden Tag der Woche durchgeführt werden.
- *Um:*: Gibt die Uhrzeit der Durchführung an.

Aktionen für diesen Abschnitt

- *Löschen*: Mit dieser Aktion wird ein Sicherungsvorgang innerhalb eines Plans gelöscht.

13.8.2.3 Aktionen für dieses Formular

- *Sicherungsvorgang hinzufügen*: Hier wird ein Vorgang zu dem geöffneten Plan hinzugefügt.
- *Abbrechen*: Die Bearbeitung des Formulars wird beendet. Änderungen werden verworfen.
- *Speichern*: Die Bearbeitung des Formulars wird beendet. Änderungen werden gespeichert.

13.9 GUI-Referenz: *Monitor-Zugriff*

(Diese Option befindet sich im Zusatzmodul *Collax Net Backup*)

(Dieser Dialog befindet sich unter *Systembetrieb – Datensicherung – Monitor-Zugriff*.)

Für Arbeitsstationen besteht die Möglichkeit mittels eines Client-Programm auf den Sicherungsserver zuzugreifen. Für eine Verbindung über den Tray-Monitor sind in diesem Formular die erforderlichen Monitorzugänge zu definieren.

Damit der Zugang netzwerktechnisch zustande kommt, ist in den Berechtigungen die gewünschte Gruppe mit Netzwerk anzuhaken.

13.9.1 Liste: *Monitorzugänge*

Hier werden die definierten Zugänge aufgelistet.

13.9.1.1 Felder in diesem Formular

- *Bezeichnung*: Zeigt den Namen des eingerichteten Monitorzugangs.
- *Kommentar*: Hier werden nähere Informationen angezeigt.
- *Passwort*: Hier wird das erforderliche Passwort für den Zugang angezeigt.

13.9.1.2 Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion im Kontextmenü, oder mittels Doppel-Klick, kann der Eintrag bearbeitet werden.
- *Löschen*: Mit dieser Aktion wird der gewählte Monitor-Zugriff gelöscht.
- *Tray-Monitor-Konfigurationsdatei*: Hier kann die Konfigurationsdatei für den Tray-Monitor auf der Client-Seite heruntergeladen werden.

13.9.1.3 Aktionen für dieses Formular

- *Hinzufügen*: Mit diese Aktion wird das Formular für einen neuen Monitorzugang geöffnet.

13.9.2 *Monitor-Zugang bearbeiten*

13.9.2.1 Felder in diesem Formular

- *Bezeichnung*: Hier wird die Bezeichnung oder Identifikation des Monitors eingetragen. Wird der Tray-Monitor mit Hilfe der herunterladbaren Datei konfiguriert, kann die Bezeichnug frei gewählt werden.
- *Kommentar*: Hier werden weitere Informationen eingetragen.
- *Passwort des Zugangs*: Hier ist ein Passwort zur Authentifizierung durch den Tray-Monitor zu hinterlegen.

13.9.2.2 Aktionen für dieses Formular

- *Abbrechen*: Bearbeiten des Monitorzugangs beenden. Die Änderungen werden verworfen.
- *Speichern*: Bearbeiten des Monitorzugangs beenden. Die Änderungen werden gespeichert.

13.9.3 *Download*

Dieser Dialog erscheint, wenn die Aktion *Tray-Monitor-Konfigurationsdatei* aufgerufen wurde.

13.9.3.1 Felder in diesem Formular

- *Hinweis*: Hier wird beschrieben, wie die Konfigurationsdatei auf dem Client installiert wird.

13.9.3.2 Aktionen für dieses Formular

- *Zurück*: Beendet die Anzeige und führt zurück zur Monitorzugangs-Liste.

13.10 GUI-Referenz: *Status und Betrieb*

(Dieser Dialog befindet sich unter *Datensicherung – Status und Betrieb*)

Über diesen Dialog können Statusinformationen des Datensicherungssystems abgerufen sowie administrative Aufgaben erledigt werden.

13.10.1 Abschnitt Anzeigen

13.10.1.1 Aktionen in diesem Abschnitt

- *Alle Jobs anzeigen*: Mit dieser Aktion werden alle Sicherungs- und Restore-Jobs des Systems angezeigt. In der Detailansicht sind unter Anderem der Umfang und Inhalt von Sicherungen sowie der Status von Jobs ersichtlich.
- *Laufende Jobs anzeigen*: Mit dieser Aktion werden alle Sicherungs- und Restore-Jobs angezeigt, die aktuell noch nicht beendet sind.
- *Erfolgreiche Jobs anzeigen*: Mit dieser Aktion werden alle Sicherungs- und Restore-Jobs angezeigt, die erfolgreich beendet worden sind.
- *Nicht erfolgreiche Jobs anzeigen*: Mit dieser Aktion werden alle Sicherungs- und Restore-Jobs angezeigt, die mit einem Fehler oder einem schweren Fehler beendet worden sind.

13.10.2 Abschnitt Anzeigen

13.10.2.1 Aktionen in diesem Abschnitt

- *Pools anzeigen*: Die in den Sicherungsvorgängen verwendeten Volume-Pools können hier aufgelistet werden. Weitere Informationen über die Volume-Pools können über das Kontext-Menü eines Pools, Rechter-Maus-Klick, aufgerufen werden.
- *Medien anzeigen*: Die über einen Sicherungs-Job erzeugten Medien können über diese Aktion angezeigt werden. Die Bearbeitung oder Veränderung von Medien sollte nur im Notfall erfolgen.

13.10.3 Abschnitt Definierte Jobs starten

13.10.3.1 Felder in diesem Abschnitt

- *Quelle/Client*: Hier wird die entsprechende Quelle, oder ein Client ausgewählt, der manuell gesichert werden soll.
- *File-Set*: Hier wird angegeben, welche Daten manuell gesichert werden sollen. Es kann nur ein einzelner Datensatz ausgewählt werden. Sollen mehrere Datensätze von Hand gesichert werden, kann dies seriell durchgeführt werden.
- *Volume-Pool*: Hier wird ausgewählt in welchen Volume-Pool gesichert werden soll.
- *Sicherungs-Level*: Hier kann zwischen verschiedenen Sicherungstypen gewählt werden.
- *Ziel*: Die manuelle Sicherung erfolgt beim Start auf das hier angegebene Sicherungsziel.

13.10.3.2 Aktionen in diesem Abschnitt

- *Start*: Mit dieser Aktion wird die eingestellte manuelle Sicherung gestartet. Der Status des gestarteten Sicherungs-Jobs kann anschließend über die Anzeige der Jobs eingesehen werden.

13.10.4 Abschnitt Datenträger hinzufügen/beschriften...

13.10.4.1 Felder in diesem Abschnitt

- *Ziel/Gerät*: Hier wird ein Ziel oder ein Gerät gewählt, für das ein neues Medium hinzugefügt oder beschriftet werden soll.
- *Name*: Hier wird die Bezeichnung des neuen Mediums angegeben, das erzeugt oder beschriftet werden soll.

13.10.4.2 Aktionen in diesem Abschnitt

- *Hinzufügen*: Mit dieser Aktion wird ein Medium/Datenträger mit dem angegebenen Namen innerhalb des ausgewählten Ziels angelegt. Die angelegten Informationen sind Meta-Daten, es wird entsprechend kein physikalisches Medium beschriftet. Diese Aktion ist im Allgemeinen nur sinnvoll, wenn für das Ziel die Option *Automatisch neue Medien belegen* aktiviert ist.
- *Beschriften*: Mit dieser Aktion wird ein Medium mit dem angegebenen Namen beschriftet. Die Aktion führt zum physikalischen Beschriften, des Mediums, es werden damit Informationen auf das Band oder die Festplatte übertragen. Diese Aktion ist sinnvoll, wenn Bänder mit bestimmten Namen belegt werden sollen.

13.10.5 Abschnitt Storage-Geräte verwalten

13.10.5.1 Felder in diesem Abschnitt

- *Storage-Geräte*: In diesem Feld kann ein Sicherungsgerät gewählt werden, welches verwaltet werden soll.
- *Laufwerk Nummer (falls vorhanden)*: Falls vorhanden, kann hier die Laufwerksnummer angegeben werden. Diese Angabe ist nur für Bandwechsler mit mehreren Laufwerken erforderlich.

13.10.5.2 Aktionen in diesem Abschnitt

- *Einhängen*: Das gewählte Sicherungsgerät wird eingehängt.
- *Aushängen*: Das gewählte Sicherungsgerät wird ausgehängt.
- *Freigeben*: Das gewählte Sicherungsgerät wird freigegeben.
- *Status*: Hier wird der Status des gewählten Geräts abgefragt und in der Ausgabe dargestellt.
- *Slot-Belegung bestimmen*: Wird ein Bandwechsler benutzt, muss mit dieser Aktion nach einem Magazin-Wechsel das System dazu veranlasst werden, die Bänder in den Magazinen zu erkennen. Diese Aktion kann zeitaufwendig sein.
- *Mit Barcodes beschriften*: Wird ein Bandwechsler mit Barcode-Unterstützung benutzt, können mit dieser Aktion die eingelegten Bänder automatisch mit ihrem jeweiligen Barcode beschriftet werden. Der Vorgang entspricht dem Schritt *Beschriften*, wobei für jedes Band der entsprechende Barcode als Name benutzt wird. Im Allgemeinen sollte diese Aktion nur mit neuen Medien durchgeführt werden. Diese Aktion kann zeitaufwendig sein.

13.11 GUI-Referenz: *Datenwiederherstellung*

(Dieser Dialog befindet sich unter *Datensicherung – Datenwiederherstellung*)

In diesem Formular können einzelne Elemente zurückgesichert werden. Zusätzlich können Status- und Detailinformationen einzelner Jobs eingesehen werden.

Im Menü Media können der aktuelle Zustand der verwendeten Sicherungsziel abgerufen werden.

13.11.1 Felder in diesem Formular

- *Hinweis*: Für eine Datenrücksicherung muss eine funktionierende Sicherung durch Zuordnung definiert sein. Ansonsten erscheint ein entsprechende Hinweis.

13.12 GUI-Referenz: *Katalog-Wiederherstellung*

(Dieser Dialog befindet sich unter *Datensicherung – Katalog-Wiederherstellung*)

Das Inhaltsverzeichnis (Katalog) aller Sicherungsdaten ist im Normalbetrieb dem System bekannt. Der Katalog wird für Datenwiederherstellung benutzt und ist in dem Formular *Datensicherung – Datenwiederherstellung* in einer Baumstruktur abgebildet. Wenn alle Daten gesichert werden, wird dieser Katalog üblicherweise ebenso auf einem Ziel gesichert.

Ist der Zustand dieser Informationen auf einem laufenden System

nicht mehr korrekt, kann über dieses Formular der Katalog aus gesicherten Daten auf einem Sicherungsziel wieder hergestellt werden.

Für das Auffinden des auf einem Sicherungsziel gespeicherten Katalogs ist eine Datei BackupCatalog*.bsr erforderlich. Diese wird nach jeder Sicherung dem Administrator per E-Mail zugestellt oder ist, je nach Einstellung, ebenso auf dem Sicherungsziel gespeichert.

13.12.1 Abschnitt *Hinweis*

13.12.1.1 Felder in diesem Abschnitt

- *Hinweis*: Erläutert den Zweck einer Katalog-Wiederherstellung. Auf einem funktionierenden System muss üblicherweise eine Katalog-Wiederherstellung nicht durchgeführt werden.

13.12.2 Abschnitt *Katalog-Wiederherstellung*

13.12.2.1 Felder in diesem Abschnitt

- *Bootstrap-Datei (BackupCatalog_XXX-XXX.bsr)*: Hier wird die Bootstrap-Datei gewählt, die Informationen enthält, wie der Katalog wieder hergestellt werden kann. Die Bootstrap-Datei wird bei erfolgreicher Datensicherung per E-Mail an den Backup-Operator gesendet.
- *Lese Katalog von Sicherungsziel*: Der Katalog (Inhaltverzeichnis aller gesicherten Daten) befindet sich auf einem Sicherungsziel. Hier wird angegeben, von welchem Sicherungsziel der Katalog gelesen und auf dem Server wieder hergestellt werden soll.

13.12.3 Abschnitt *Hinweis*

13.12.3.1 Felder in diesem Abschnitt

- : Statusmeldung des Prozesses.

13.12.4 Abschnitt *Ausgabe*

13.12.4.1 Felder in diesem Abschnitt

- *Ausgabe*: Ausgabe des Prozesses.

13.12.5 Aktionen für dieses Formular

- *Bootstrap-Datei laden*: Die Bootstrap-Datei wird mit dieser Aktion hochgeladen.
- *Zurück*: Beendet die Eingabe ins Formular. Änderungen werden verworfen.

14 Virtualisierung

14.1 Einführung

Die Virtualisierung, basierend auf KVM (Kernel based Virtual Machine), ist eine vollständige Virtualisierungslösung für x86-Hardware mit entsprechender Hardware-Virtualisierungserweiterungen Intel VT oder AMD-V. Mit dem V-Cube können virtuell mehrere unmodifizierte Gastbetriebssysteme betrieben werden, wobei jede virtuelle Maschine ihre eigene virtualisierte Hardware , wie Netzwerkkarten, Festplatten, Grafikkarte, USB-Geräte oder ISDN-Karte besitzt. Als virtuelle Maschinen unterstützt der V-Cube Linux (32 Bit und 64 Bit), Windows (32 Bit und 64 Bit), FreeDOS, Solaris und diverse BSD-Derivate.

14.2 Paravirtualisierung

Im Gegensatz zum Ansatz der vollständigen Virtualisierung, bei dem unmodifizierte Betriebssysteme auf virtuelle Hardware zugreifen, interagieren paravirtualisierte Maschinen über eine von der Virtualisierungsschicht bereitgestellte Programmierschnittstelle direkt mit der gemeinsamen Hardware - gesteuert und kontrolliert durch den Hypervisor. Dies erfordert die Anpassung des Betriebssystems der virtuellen Maschine, zumeist der Kernel des Betriebssystems.

Die Nutzung der Paravirtualisierung für virtuelle Festplatten, Netzwerkkarten und CPU geschieht bei Linux-Gastsystemen ab Kernel 2.6.25 automatisch, sofern der Kernel die entsprechende Treiber vorhält. Bei paravirtualisierten Block-Geräten muss das Linux-Gastsystem /dev/vda-Geräte unterstützen.

Wird Windows als Gastbetriebssystem eingesetzt, so ist eine Paravirtualisierung von Netzwerkschnittstellen möglich, die durch die Installation eines Treibers initiiert werden kann. Das ISO-Image mit dem entsprechenden Treiber wird mit dem V-Cube mitgeliefert und kann innerhalb einer virtuellen Maschine verfügbar gemacht werden.

Vorteile durch die Nutzung der Paravirtualisierung liegen im schonenden Umgang mit den Ressourcen des Host-Systems. Dadurch gewinnt das gesamte System an erheblicher Leistungsfähigkeit.

14.3 Allgemein

Der Virtualisierungsdienst ist standardmäßig aktiviert. Gastsysteme mit der Einstellung *Autostart* werden beim Neustart des V-Cube automatisch gebootet.

Für die Bereitstellung von ISO- oder Festplatten-Images für die virtuellen Maschinen steht das Verzeichnis „vmData“ zur Verfügung. Dieses Verzeichnis kann für den Zugriff über FTP, NFS oder SCP freigegeben werden.

14.4 GUI-Referenz: *Virtualisierung*

14.4.1 Abschnitt *Hinweis*

14.4.1.1 Felder in diesem Abschnitt

- : Voraussetzung für die Benutzung der Virtualisierung ist Hardware mit Unterstützung von Intel VT oder AMD-V.

14.4.2 *Assistent zur Einrichtung virtueller Maschinen*

Der Assistent zur Einrichtung virtueller Maschinen richtet in wenigen Schritten das Virtualisierungssystem ein und generiert eine virtuelle Maschine mit der erforderlichen Hardware-Einstellung.

14.4.2.1 Felder in diesem Formular

- *Ablauf*: Im Schritt Eins und Zwei werden Basiseinstellungen vorgenommen. Hierzu zählt der Typ der virtuellen Maschine. Prinzipiell kann hier unterschieden werden, ob ein Collax System, ein Klon eines schon installierten Disk-Images oder andere Betriebssysteme auf der Maschine starten sollen.

  Im zweiten Schritt kann ebenso entschieden werden, ob eine Bildschirmkonsole (VNC) gestartet werden soll.

  Im Schritt Drei wird das Installationsmedium ausgewählt. Üblicherweise wird ein ISO-Image ausgewählt. Beim Typ „Collax Server“ kann ebenso eine Vorlage für einen bestimmtes Collax Produkt gewählt werden. Soll ein Klon installiert werden, muss ein schon vorhandenes Disk-Image gewählt werden.

Im vierten Schritt wird die virtuelle Netzwerkschnittstelle eingerichtet. Bei einer Collax Server-Vorlage kann zusätzlich die Konfiguration der IP-Adresse und der Netzwerkmaske mit angegeben werden. Ansonsten wird der Treiber und die Schnittstelle des Host-Systems gewählt, auf die sich die virtuelle Schnittstelle binden soll.

Im letzten Schritt wird die Art der Virtualisierung der zu verwendenden Festplatte konfiguriert. Ein vorhandenes Disk-Image oder ein vorhandenes logisches Volume kann verwendet werden. Alternativ kann eine neue Festplatte mit einem der beiden Typen erzeugt werden.

- *Konfiguration*: Beim Fertigstellen des Assistenten werden die angegebenen Hardware-Elemente der virtuellen Maschine angelegt und der Maschine zugeordnet. Durch das Fertigstellen wird der Virtualisierungsdienst gestartet, falls dieser noch nicht aktiviert wurde. Zeigt der Logauszug die Meldung „Done“, kann die Maschine gestartet werden.

  Wurde eine Collax Server-Vorlage gewählt, werden bei der Fertigstellung die erforderlichen Image-Daten online herunter geladen und der Server komplett installiert.

14.4.3 *Assistent zum Klonen virtueller Maschinen*

(Dieser Dialog befindet sich unter *Einstellungen – Virtualisierung – Virtuelle Maschinen Klonen*

Der Assistent zum Klonen virtueller Maschinen dupliziert in wenigen Schritten vorhandene virtuelle Maschinen und generiert eine neue virtuelle Maschine mit den schon vorhandenen Hardware-Einstellungen.

14.4.3.1 Felder in diesem Formular

- *Ablauf*: Im Schritt Eins werden der Name der neuen virtuellen Maschine angegeben. Weiter wird die Maschine ausgewählt, deren Einstellungen und Hardware dupliziert werden soll. Es können nur Maschinen ausgewählt werden, die nicht in Betrieb sind.
- *Konfiguration*: Beim Fertigstellen des Assistenten werden die Hardware-Elemente der ausgewählten virtuellen Maschine kopiert und der neuen Maschine zugeordnet. Zusätzlich wird eine Kopie der Festplatte erzeugt und der neuen virtuellen Maschine als Laufwerk zugeordnet.

  Nach dem Abschluss des Assistenten steht der Klon als virtuellen Maschine zur Verfügung und kann gestartet werden. Die duplizierte Maschine kann anschließend nur noch als Vorlage für weitere Klone benutzt werden, sie kann jedoch nicht mehr gestartet werden.

14.4.4 *Allgemein*

(Dieser Dialog befindet sich unter *Einstellungen – Virtualisierung – Allgemein*

14.4.4.1 Tab *Grundeinstellungen*, Abschnitt *Sicherungsoptionen* Felder in diesem Abschnitt

- *Unterstützung für inkrementelle Datensicherung*: Dies ermöglicht die Sicherung von VMs durch inkrementelle Datensicherungen. Wenn diese Option aktiviert ist, wird bei jeder Sicherung ein

neuer Snapshot erzeugt. Dadurch wird in großem Umfang Speicherplatz bei Sicherungen der VMs eingespart.

Bitte beachten Sie, dass bei Aktivierung dieser Option die Performance der VMs beeinflusst werden kann.

14.4.4.2 Tab *Berechtigungen*, Abschnitt *Zugriff erlauben für ...* Felder in diesem Abschnitt

- *VNC-Verbindung für temporäre VMs*: Hier wird der Zugriff auf die Bildschirmkonsolen von Instant-VMs über VNC gesteuert. Die gewählten Gruppen erhalten Netzwerkzugriff auf den VNC-Port. Die VNC-Ports beginnen für Instant-VMs bei 6100.

14.4.4.3 Aktionen für dieses Formular

- *Abbrechen*: Bearbeitung abschließen, Änderungen werden verworfen.
- *Speichern*: Bearbeitung abschließen, Änderungen werden gespeichert.

14.4.5 *Konfiguration Virtueller Maschinen*

(Dieser Dialog befindet sich unter *Einstellungen – Virtualisierung – Konfiguration*

Die Einstellungen der virtuellen Maschinen werden in diesem Dialog verwaltet. In der Virtualisierungsumgebung können Server und Arbeitsstationen als virtuelle Maschinen definiert werden, die je nach Bedarf mit verschiedenster virtueller Hardware-Konfiguration ausgestattet werden können.

14.4.5.1 *Liste virtueller Maschinen*

In diesem Dialog werden angelegte virtuelle Gast-Maschinen angezeigt. Es können einzelne Maschinen hinzugefügt, bearbeitet oder bei Bedarf gelöscht werden.

Abschnitt *Hinweis*
Felder in diesem Abschnitt

- : Voraussetzung für die Benutzung der Virtualisierung ist Hardware mit Unterstützung von Intel VT oder AMD-V.

Spalten in der Tabelle

- *Name*: Name der hinzugefügten virtuellen Maschine.
- *Kommentar*: Weitere Informationen über die virtuelle Maschine.
- *CPUs*: Anzahl der zugeteilten virtuellen CPUs.
- *MEM*: Zugewiesener virtueller Hauptspeicher in MBytes.
- *NICs*: Anzahl der konfigurierten Netzwerkschnittstellen.
- *Disks*: Anzahl der konfigurierten Festplatten.
- *CDROMs*: Anzahl der konfigurierten CD-Laufwerke.
- *Boot*: Boot-Device der virtuellen Maschine.
- *VNC*: Zeigt an, ob Zugriff per VNC konfiguriert ist.
- *Autostart*: Zeigt an, ob die virtuelle Maschine wieder automatisch startet.
- *Priorität*: Zeigt die Priorität, mit der die virtuelle Maschine vom Virtualisierungsdienst angesteuert wird.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion öffnet sich der Dialog, um die virtuelle Maschine zu bearbeiten.
- *Löschen*: Mit dieser Aktion kann die virtuelle Maschine gelöscht werden.

Aktionen für dieses Formular

- *Hinzufügen*: Mit dieser Aktion öffnet sich der Dialog, um eine virtuelle Maschine hinzuzufügen.

14.4.5.2 *Bearbeiten*

Tab *Grundeinstellungen*, Abschnitt *Virtuelle Maschine*

Felder in diesem Abschnitt

- *Name*: Hier wird der Name der virtuellen Maschine angezeigt oder eingegeben.
- *Kommentar*: Weitere Informationen können in diesem Feld hinterlegt werden.
- *Autostart*: Wird diese Option aktiviert, startet die virtuelle Maschine sobald der Virtualisierungs-Host gestartet wird.
- *Verzögerung bei Autostart in Minuten (0-30)*: Für die Autostartfunktion ist es evtl. erforderlich, dass eine virtuelle Maschine mit Verzögerung startet, damit z.B. benötigte Verzeichnis oder Authentifizierungsserver vorher starten können. Die Verzögerungszeit wird nur beim automatischen Start der VM angewendet.
- *Boot-Reihenfolge*: Sind einem Gast-System mehrere Geräte zugewiesen, kann hier eingestellt werden, in welcher Reihenfolge das Gast-System von den Boot-Devices starten soll.

- *HDD-Caching*: Mit dieser Option kann der Caching-Modus der virtuellen Festplatten spezifiziert werden. Die korrekte Einstellung des Modus richtet sich nach dem Dateisystem der VM und dieser hat Einfluss darauf, ob bei einem Absturz oder direktem Ausschalten der VM Daten verloren gehen. Für moderne Dateisysteme und Collax Server ab Version 5.5.0 kann der Modus *Performance* eingestellt werden. Ansonsten soll die Einstellung *Datensicherheit* gewählt werden.
- *RTC Zeit*: Diese Einstellung hat Einfluss auf die Richtigkeit der Uhrzeit des Betriebsystems der virtuellen Maschine. Für Linux-basierende Systeme soll UTC, für Windows-Systeme lokale Zeit eingestellt werden.
- *Prozess-Priorisierung*: Hier wird angegeben mit welcher Priorität die virtuelle Maschine vom Virtualisierungsdienst angesteuert wird.
- *BIOS*: Hier soll die neueste BIOS-Version für das Starten der VM eingestellt sein. Falls Windows-VMs mit älteren Paravirtualisierungstreibern (Virtio) betrieben werden, sollte ebenso eine ältere BIOS-Version gewählt werden.
- *Virtio-Treiber-Diskette*: Hier kann der VM eine Diskette zugewiesen werden, auf der Virtio-Treiber für Festplatten von Windows Betriebssystemen vorhanden sind. Diese Option eignet sich für Neuinstallationen von Windows VMs, die paravirtualisierte Festplattentreiber nicht per CD-ROM-Laufwerk laden können.

Tab *Grundeinstellungen*, Abschnitt *CPU*
Felder in diesem Abschnitt

- *Anzahl virtueller CPUs*: Die Anzahl der CPUs berechnet sich aus der Anzahl der Sockel und der Kerne. Maximal können einer VM 64 CPUs zugewiesen werden. Um eine 100% Auslastung des Host-

Systems zu vermeiden, sollten den virtuellen Gästen insgesamt nicht mehr CPUs zugewiesen werden, als auf dem Host-System vorhanden sind.

- *Anzahl der CPU Sockel*: Gibt die Anzahl der CPU-Sockel für eine VM an. Diese Einstellung ist wichtig, falls das Betriebssystem der VM nur eine begrenzte Anzahl von CPU-Sockel berücksichtigt.
- *Anzahl der CPU Kerne*: Gibt die Anzahl der CPU-Kerne pro CPU-Sockel an.
- *Hinweis*: Zeigt an, falls mehr virtuelle CPUs verwendet werden, als physikalisch vorhanden sind.

Tab *Grundeinstellungen*, Abschnitt *Memory* Felder in diesem Abschnitt

- *RAM-Speicher (in MBytes)*: Hier wird der Hauptspeicher für den virtuellen Gast zugewiesen.

Tab *Grundeinstellungen*, Abschnitt *Grafik* Felder in diesem Abschnitt

- *VNC- und RDP-Konsole*: Um die Bildschirmkonsole der virtuellen Maschine zu erhalten, ist diese Option für Virtual Network Computing oder RDP zu aktivieren. Mit der Vergabe entsprechender Berechtigungen kann der Bildschirm einer virtuellen Maschine entweder mit einem VNC-Viewer oder über das im Collax GUI integrierte Java-VNC-Applet aufgerufen werden.

  VNC verwendet zur Kommunikation über TCP/IP die Dienst-Ports ab Port 5901 aufsteigend. Der Collax Server weist diese Ports automatisch zu und zeigt die verwendeten Ports in der Übersichtstabelle an. Beim Zugriff über Netzwerke muss sichergestellt sein, dass die entsprechenden VNC-Ports von dazwischenliegenden Router oder Firewalls erlaubt sind.

- *VNC- und RDP-Passwort*: Zur Erhöhung der Sicherheit beim Zugriff per VNC auf eine virtuelle Maschine kann hier ein Passwort angegeben werden. Soll das Passwort geändert werden, muss anschließend die virtuelle Maschine herunter und wieder hochgefahren werden.
- *Keymap*: Um den korrekten Einsatz einer Tastatur per VNC zu ermöglichen, kann hier das entsprechende Ländertastatur-Layout eingestellt werden.
- *VGA*: Hier kann die emulierte Grafikkarte für die VM eingestellt werden.

Tab *Hardware*, Abschnitt *Laufwerke*
Felder in diesem Abschnitt

- *Disk-Typ*: Für die Einbindung von virtuellen Disks können verschiedene Arten gewählt werden. „IDE“-Disks werden entsprechend dem Bus-System als vollvirtualisierte Platten emuliert und bringen keine Leistungssteigerung in der I/O-Virtualisierung.

  Der Disk-Typ „virtio“ bietet die volle Unterstützung des Kernel-Hypervisors für I/O-Virtualisierung. Innerhalb des Betriebssystems der VM müssen zur Unterstützung der Paravirtualisierung die „virtio“-Treiber installiert werden. Für Windows™-Betriebssysteme kann dazu die Option *Virtio-Treiber-Diskette* benutzt werden.
- *Festplatte*: Hier wird gewählt, auf welcher virtuellen Disk die virtuelle Maschine betrieben werden soll. Es können Logische Volumen oder vorhandene Disk-Images gewählt werden.
- *ISO image*: Wird ein CD-Rom eingebunden, kann hier ein ISO-Image als Datenträger gewählt werden.
- *Reihenfolge Festplatte*: Es können vier Disks gleichzeitig eingebunden werden. Die Reihenfolge gibt an, wie die Disks im System nacheinander erscheinen.

CD-ROMs können ausschließlich als erstes oder drittes Medium als Boot-Device verwendet werden.

Tab *Hardware*, Abschnitt *Netzwerkschnittstelle* Felder in diesem Abschnitt

- *MAC-Adresse*: Hier kann eine bestimmte MAC-Adresse für die virtuelle NIC gesetzt werden. Die Standardeinstellung generiert für jede Schnittstelle eine MAC-Adresse automatisch. In der Regel kann dieses Feld leergelassen werden.
- *Verbinde mit Switch Device*: Virtuelle Netzwerkschnittstellen können hier zu einer bestimmten Maschine hinzugefügt werden. Stehen hier noch keine Geräte zur Auswahl, können im Formular – *Virtuelle Netzwerk-Switches* Netzwerkschnittstellen verfügbar gemacht werden.
- *Treiber*: Wenn das Gast-System die leistungsfähige Paravirtualisierung für Netzwerkschnittstellen unterstützt, sollte hier Virtio gewählt werden. Alle Collax Server unterstützen dies. Für Windows-Systeme kann der auf dem Host mitgelieferte Treiber nachinstalliert werden (s. Option *Virtio-Treiber-Diskette*).

  Für andere Gastsysteme können Realtek 8139- oder Intel E1000-Netzwerkschnittstellen emuliert werden.

Tab *Hardware*, Abschnitt *PCI-Geräte* Felder in diesem Abschnitt

- *Gerät*: Wird ein PCI-Gerät hinzugefügt, stehen in diesem Feld die verfügbaren Geräte zur Auswahl. Verfügbar sind nur Geräte, die nicht vom Host-System oder von einer weiteren virtuellen Maschine in Benutzung sind.

Tab *Hardware*, Abschnitt *USB HUB/Port*
Felder in diesem Abschnitt

- *USB HUB/Port*: Hier können bestimmte USB-Ports ausgewählt werden, die der virtuellen Maschine zur Verfügung gestellt werden.

Tab *Hardware*, Abschnitt *Serielle Schnittstelle*
Felder in diesem Abschnitt

- *Name*: Serielle Schnittstellen, die vom Host-System nicht verwendet werden, können hier an eine virtuelle Maschine zugewiesen werden. Der Name einer benutzbaren seriellen Schnittstelle wird hier angezeigt.

Aktionen für jeden Abschnitt

- *Löschen*: Einzelne Hardware-Elemente können mit dieser Aktion gelöscht werden. Die Einstellungen zur virtuellen Maschine wird weiterhin angezeigt.

Aktionen in diesem Tab

- *Festplatte*: Mit dieser Aktion können Disk Images oder logische Volumes als Festplatte hinzugefügt werden. Es können bis zu vier Festplatten oder CD-ROMs zu einer virtuellen Maschine hinzugefügt werden.
- *CD-/DVD-ROM (ISO)*: Mit dieser Aktion wird ein virtuelles CD-/DVD-ROM-Laufwerk zur virtuellen Maschine hinzugefügt. Es kann direkt ein ISO-Image angegeben werden.
- *CD-/DVD-ROM*: Falls ein physisches CD-/DVD-Laufwerk zur Ver-

fügung steht, kann dieses zur virtuellen Maschine hinzugefügt werden. Das Laufwerk kann nur einer VM zugeteilt werden.
- *NIC*: Es können bis zu 16 Netzwerkschnittstellen zu einer virtuellen Maschine hinzugefügt werden. Für jede Schnittstelle muss ein Switch Device vorhanden sein.
- *PCI-Gerät*: PCI-Geräte, die nicht vom Host-System benutzt werden, können hier zur virtuellen Maschine hinzugefügt werden.
- *Serielle Schnittstelle*: Vom Host-System nicht verwendete serielle Schnittstellen können mit dieser Aktion zur virtuellen Maschine hinzugefügt werden.

Tab *Berechtigungen*
Felder in diesem Abschnitt

- *VNC-/RDP-Zugriff für ...*: Die Rechner und Netzwerke der ausgewählten Gruppen haben Zugriff per VNC oder RDP auf die definierten virtuellen Maschinen. Pro Maschine kann nur eine VNC-Verbindung aufgebaut werden.

14.4.5.3 Aktionen für dieses Formular

- *Abbrechen*: Bearbeitung abschließen, Änderungen werden verworfen.
- *Speichern*: Bearbeitung abschließen, Änderungen werden gespeichert.

14.4.6 *Virtuelle Festplatten*

(Dieser Dialog befindet sich unter *Einstellungen – Virtualisierung – Festplatten*

14.4.6.1 *Festplatten wählen*

In diesem Dialog wird die Liste der angelegten virtuellen Festplatten angezeigt. Sind noch keine Festplatten für virtuelle Maschinen vorhanden, können hier welche hinzugefügt werden.

Felder in dieser Tabelle

- *Typ*: Zeigt den Typ der virtuellen Festplatte.
- *Name*: Name der virtuellen Festplatte.
- *Info*: Weitere Informationen über die Festplatte sind hier angegeben.
- *Verwendung*: Angabe von welcher virtuellen Maschine die Festplatte genutzt wird.
- *Größe*: Größe der verwendeten Festplatte.

Aktionen für jeden Tabelleneintrag

- *Info*: Detailinformationen werden angezeigt.
- *Bearbeiten*: Durch diese Aktion kann die gewählte Festplatte einer virtuellen Maschine zugeordnet werden. Ist die Festplatte schon in Verwendung, kann hier der Typ der Schnittstelle und die Position der Festplatte festgelegt.
- *Aus der VM löschen*: Mit dieser Aktion kann die Zuordnung der Platte zu einer virtuellen Maschine direkt aufgehoben werden.

- *Vorlage generieren*: Eine angelegte Festplatte vom Typ „disk image“ kann als Vorlage für Klone virtueller Maschinen benutzt werden. Mit dieser Aktion kann aus der Festplatte eine Vorlage generiert werden. Um eine Vorlage zu definieren, darf die betreffende Festplatte nicht in Benutzung oder in Betrieb sein.
- *Vorlage freigeben*: Mit dieser Aktion wird die Festplatte nicht mehr als Vorlage genutzt, sie steht für nachfolgend für die Verwendung in virtuellen Maschinen zur Verfügung.
- *Festplatte erweitern*: Mit dieser Aktion kann die Größe einer Festplatte vom Typ „Logisches Volume“ oder „Diskimage“ vergrößert werden. Vorhanden Daten bleiben bei diesem Vorgang erhalten.
- *Löschen*: Hier kann die ausgewählte Festplatte gelöscht werden. Vorhanden Daten gehen bei diesem Vorgang verloren.

Aktionen für dieses Formular

- *Hinzufügen*: Mit dieser Aktion öffnet sich der Dialog, um eine Festplatte hinzuzufügen.

14.4.6.2 *Festplatte*

Felder in diesem Formular

- *Name*: Name der virtuellen Festplatte.
- *Info*: Weitere Beschreibung der virtuellen Festplatte.
- *Format*: Hier wird das Format des virtuellen Image angezeigt. Das systemeigene Format wird mit qcow2 bezeichnet.
- *Verwendung*: Hier wird angezeigt, von welcher Maschine das virtuelle Image, oder das logische Volumen benutzt wird.
- *Dateigröße*: Zeigt die Größe des virtuellen Images oder die Größe des logischen Volumens im Dateisystem.

- *Größe*: Zeigt die Gesamtgröße des virtuellen Images oder des logischen Volumens.

Aktionen für dieses Formular

- *Zurück*: Führt zurück zur Übersicht der virtuellen Festplatten.

14.4.6.3 *Festplatte anlegen*

Felder in diesem Abschnitt

- *Name*: Hier wird ein Name für die Festplatte eingetragen.
- *Typ*: Es stehen zwei Typen von virtuellen Festplatten zur Auswahl. *Disk image* bezeichnet eine Festplatte in Datei-Format. Ein *logisches Volume* ist eine logische Datenpartition, die für eine virtuelle Maschine in kompletter Größe genutzt werden kann.
- *Festplatten-Klon*: Hier kann eine vorhandene Festplatte vom Typ *disk image* als Basis-Image für die hier zu generierende Festplatte ausgewählt werden.
- *Vorlage verwenden*: Hier wird eine Auswahl an vorhandenen Vorlagen aufgelistet.
- *Größe*: Hier wird die gewünschte Größe der virtuellen Platte angegeben.

Abschnitt *Ausgabe*

Felder in diesem Abschnitt

- *Prozessausgabe*: Logausgabe, wenn Aktionen auf eine Disk ausgeführt werden.

Aktionen für dieses Formular

- *Abbrechen*: Bearbeitung beenden, Einstellungen werden verworfen.
- *Anlegen*: Mit dieser Aktion wird die Platte im System angelegt.

14.4.6.4 *Logisches Volume entfernen*

Felder in diesem Abschnitt

- *Volume-Gruppe*: Anzeige der Volume-Gruppe, zu der das gewählte logische Volume gehört.
- *Logisches Volume*: Name des logischen Volumes, das gelöscht werden soll.
- *Aktuelle Größe*: Momentan benutzte Größe des Volumes.

Abschnitt *Hinweis*
Felder in diesem Abschnitt

- : Hinweis, was beim Entfernen beachtet werden muss.

Aktionen für dieses Formular

- *Abbrechen*: Vorgang abbrechen, das Volume wird nicht gelöscht.
- *Löschen*: Vorgang fortsetzen, das Volume wird gelöscht.

Abschnitt *Ausgabe*
Felder in diesem Abschnitt

- : Ausgabe des Fortschritts der angestoßenen Aktion.

14.4.6.5 *Disk Image entfernen*

Felder in diesem Abschnitt

- *Name*: Name des Disk-Images, das gelöscht werden soll.

Abschnitt *Hinweis*
Felder in diesem Abschnitt

- : Hinweis, was beim Entfernen beachtet werden muss.

Aktionen für dieses Formular

- *Abbrechen*: Der Vorgang wird abgebrochen, das Disk-Image bleibt erhalten.
- *Löschen*: Der Vorgang wird durchgeführt, das Disk-Image und die darauf gespeicherten Daten werden gelöscht.

14.4.6.6 *Logisches Volume erweitern*

Felder in diesem Abschnitt

- *Volume-Gruppe*: Name der zugehörigen Volume-Gruppe.
- *Logisches Volume*: Name des gewählten Volumes.
- *Aktuelle Größe*: Momentane Größe des Volumes.
- *Verfügbarer Speicherplatz*: Noch verfügbarer Speicherplatz auf dem System.
- *Erweitern um*: Angabe des Speicherplatzes, um den das logische Volume erweitert werden soll.

Aktionen für dieses Formular

- *Abbrechen*: Der Vorgang wird abgebrochen, das logische Volume wird nicht erweitert.
- *Erweitern*: Die Erweiterung wird durchgeführt und es wird eine Ausgabe über den Fortschritt der Aktion angezeigt.

Abschnitt *Ausgabe*
Felder in diesem Abschnitt

- : Logausgabe der durchgeführten Aktion.
- *Zurück*: Diese Aktion führt zurück zur Liste der virtuellen Festplatten.

14.4.6.7 *Erweitern*
Abschnitt *Erweitern*
Felder in diesem Abschnitt

- *Name*: Hier steht der Name der zu bearbeitenden virtuellen Festplatte.
- *Info*: Hier steht der Gerätename der virtuellen Festplatte im System.
- *Aktuelle Größe*: Dieses Feld zeigt die aktuell konfigurierte Größe der virtuellen Festplatte an.
- *Verfügbarer Speicherplatz*: Um den hier angezeigten Speicherplatz kann die Festplatte maximal erweitert werden.
- *Erweitern um*: Hier wird festgelegt, um wie viel die virtuelle Festplatte vergrößert werden soll.

Aktionen für dieses Formular

- *Erweitern*: Mit dieser Aktion wird die Erweiterung der virtuellen Festplatte ausgeführt. Anschließend muss die Einstellung aktiviert werden.
- *Abbrechen*: Beendet den Dialog, die Einstellungen werden verworfen.

14.4.6.8 *Füge Festplatte der VM hinzu*
Abschnitt *Info*
Felder in diesem Abschnitt

- *Name*: Name der gewählten Festplatte.
- *Info*: Zeigt den Namen und den Typ der Festplatte.
- *Format*: Hier wird das Format des virtuellen Image angezeigt. Das systemeigene Format wird mit qcow2 bezeichnet.

- *Verwendung*: Hier wird angezeigt, von welcher Maschine das virtuelle Image, oder das logische Volumen benutzt wird.
- *Dateigröße*: Zeigt die Größe des virtuellen Images oder die Größe des logischen Volumens im Dateisystem.
- *Größe*: Zeigt die Gesamtgröße des virtuellen Images oder des logischen Volumens.

Abschnitt *Festplatte*

Felder in diesem Abschnitt

- *Virtuelle Maschine*: Ist die Festplatte nicht in Verwendung, kann in dieser Liste eine virtuelle Maschine gewählt werden, die diese Festplatte verwenden soll.
- *Festplatten-Typ*: Hier wird der Anschlusstyp der Festplatte gesetzt.
- *Festplatten Reihenfolge*: Es können vier Festplatten gleichzeitig von einer virtuellen Maschine verwendet werden. Diese Auswahl gibt an, an welcher Position die gewählte Festplatte in der virtuellen Maschine angeordnet wird.

Aktionen für dieses Formular

- *Abbrechen*: Dialog zum Hinzufügen einer Festplatte beenden, die Einstellungen werden verworfen.
- *Speichern*: Dialog zum Hinzufügen einer Festplatte beenden, die Einstellungen werden gespeichert.

14.4.7 *Netzwerk Bridge/Switch Schnittstellen*

(Dieser Dialog befindet sich unter *Einstellungen – Virtualisierung – Netzwerk Bridge/Switch*

14.4.7.1 *Netzwerk Bridge/Switch*

In dieser Tabelle werden vorhandene Netzwerk Bridge/Switch-Geräte aufgelistet.

Spalten in dieser Tabelle

- *Name*: Name der Netzwerk Bridge/Switch.
- *Verwendung*: Zeigt an, von welchen Netzwerk-Links oder virtuellen Maschinen diese Netzwerk Bridge/Switch verwendet wird.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion öffnet sich der Dialog, um die Netzwerk Bridge/Switch zu bearbeiten.
- *Löschen*: Mit dieser Aktion kann die Netzwerk Bridge/Switch gelöscht werden. Wird die Schnittstelle verwendet, kann diese Aktion nicht ausgeführt werden.

14.4.7.2 *Netzwerkschnittstellen*

In dieser Tabelle werden die vorhandenen virtuellen Netzwerkschnittstellen aufgelistet.

Spalten in dieser Tabelle

- *Name*: Name der Netzwerkschnittstelle.
- *Netzwerk Bridge/Switch*: Zeigt den Namen der Netzwerk Bridge/Switch, mit der diese Netzwerkschnittstelle verbunden ist.
- *Treiber*: Zeigt den Namen des verwendeten Treibers für die Schnittstelle.
- *Virtuelle Maschine*: Hier wird angezeigt, von welcher virtuellen Maschine die Netzwerkschnittstelle benutzt wird.
- *Info*: Diese Spalte zeigt weitere Informationen über die Netzwerkschnittstelle an.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion öffnet sich der Dialog, um die virtuelle NIC zu bearbeiten.
- *Löschen*: Mit dieser Aktion kann die Netzwerkschnittstelle gelöscht werden. Wird die Schnittstelle verwendet, kann diese Aktion nicht ausgeführt werden.

14.4.7.3 Aktionen für dieses Formular

- *Netzwerkschnittstelle hinzufügen*: Mit dieser Aktion öffnet sich der Dialog, um eine neue virtuelle NIC hinzuzufügen.
- *Netzwerk Bridge/Switch hinzufügen*: Mit dieser Aktion öffnet sich der Dialog, um ein neues Switch Device hinzuzufügen.

14.4.7.4 *Netzwerk Bridge/Switch bearbeiten*

In diesem Dialog können verschiedene Einstellungen eines Netzwerk Bridge / Switch bearbeitet werden.

Felder in diesem Formular

- *Name*: Hier wird der Name des Netzwerk Bridge / Switch angezeigt. Der Eintrag kann verändert werden.
- *Gerätename*: Zeigt den internen Gerätenamen.
- *Verbinde mit Netzwerkschnittstelle*: Diese Auswahl zeigt aktuell verwendete Netzwerkschnittstellen des Host-Systems. Änderungen können vorgenommen werden.
- *Verbinde mit Netzwerk-Links*: Diese Auswahl zeigt aktuell verwendete Netzwerk-Links des Host-Systems. Änderungen können vorgenommen werden.
- *Verbinde mit virtueller Netzwerkschnittstelle*: Diese Auswahl zeigt angelegte virtuelle Netzwerkschnittstellen. Änderungen können vorgenommen werden.

Aktionen für dieses Formular

- *Abbrechen*: Die Bearbeitung wird beendet, Änderungen werden verworfen.
- *Speichern*: Die Bearbeitung wird beendet, die Einstellungen werden gespeichert.

14.4.7.5 *Virtuelle Netzwerkschnittstelle bearbeiten*

In diesem Dialog können verschiedene Einstellungen der Netzwerkschnittstelle bearbeitet werden. Die Schnittstelle lässt sich in diesem Dialog für die Benutzung in schon vorhandenen virtuellen Maschinen zuweisen.

Felder in diesem Formular

- *Virtuelle Maschine*: Hier wird der Name der virtuellen Maschine angezeigt, der die Schnittstelle zugeordnet ist.
- *Name*: Zeigt den internen Namen der Schnittstelle.
- *Treiber*: Diese Auswahl zeigt den aktuell verwendeten Treiber der Schnittstelle. Änderungen können vorgenommen werden.
- *Verbunden mit Switch Device*: Diese Auswahl zeigt das aktuell verbundene Switch Device der Schnittstelle. Änderungen können vorgenommen werden. Soll die Schnittstelle nicht vom Betriebssystem verwendet werden, kann *Keine Verbindung* gewählt werden.

Aktionen für dieses Formular

- *Abbrechen*: Die Bearbeitung wird beendet, Änderungen werden verworfen.
- *Speichern*: Die Bearbeitung wird beendet, die Einstellungen werden gespeichert.

14.4.7.6 *Switch Device hinzufügen*

In diesem Dialog wird ein neues Switch Device hinzugefügt.

Felder in diesem Formular

- *Name*: Hier wird der Name des Switch Device festgelegt.
- *Verbinde mit Netzwerkschnittstelle*: Unbenutzte Ethernet-Anschlüsse des Hosts-Systems können auf das Switch Device gebunden werden.
- *Verbinde mit Netzwerk-Links*: Zur Verfügung stehende Netzwerk-Links des Host-Systems können auf das Switch Device gebunden werden.
- *Verbinde mit virtueller Netzwerkschnittstelle*: Hier wird definiert, welche virtuelle Netzwerkschnittstelle dieses Switch Device benutzen soll.

Aktionen für dieses Formular

- *Abbrechen*: Die Bearbeitung wird beendet, die Einstellungen werden verworfen.
- *Speichern*: Die Bearbeitung wird beendet, die Einstellungen werden gespeichert.

14.4.8 *USB-Geräte*

(Dieser Dialog befindet sich unter *Einstellungen – Virtualisierung – USB-Geräte*

Die hier gelisteten USB-Ports können einzelnen virtuellen Maschinen zugeordnet werden. Somit können USB-Sticks, -Platten, -Dongle

am Port ein- und ausgesteckt und diese dann von der virtuellen Maschine benutzt werden. Die Zuordnung bleibt bestehen, falls die virtuelle Maschine oder der Host neu gestartet wird. Die an einem USB-Port angeschlossenen USB-Geräte werden von den virtuellen Gastmaschinen als Geräte der Spezifikation USB 1.1 erkannt.

14.4.8.1 *Liste USB-Geräte*

In diesem Dialog werden USB-Geräte gelistet. Diese Geräte können den virtuellen Maschinen zugeordnet werden.

Felder in diesem Formular

- *Hub*: Zeigt die Nummer des USB-Hubs im Host.
- *Port*: Zeigt die Nummer des USB-Ports, der an dem angezeigten USB-Hub angeschlossen ist..
- *Eingestecktes Gerät*: Zeigt die Systeminformation oder Bezeichnung des eingesteckten USB-Geräts.
- *Verwendung*: Zeigt die virtuelle Maschine an, die das USB-Gerät momentan benutzt.

Aktionen für jeden Tabelleneintrag

- *An VM zuweisen*: Mit dieser Aktion kann der USB-Port zu einer vorhandenen virtuellen Maschine zugeordnet werden.
- *Von VM Lösen*: Mit dieser Aktion kann der USB-Port von einer vorhandenen virtuellen Maschine gelöst werden. Der Port steht anschließend anderen virtuellen Maschinen oder dem Host-System zur Verfügung.
- *Gerät einstecken*: Diese Aktion bewirkt dasselbe, wie wenn das

USB-Gerät am Port eingesteckt wird. Das Gastsystem meldet, dass ein USB-Gerät eingesteckt wurde. Die Aktion ist nur verfügbar, wenn ein USB-Port durchgereicht wurde.
- *Gerät entfernen*: Diese Aktion führt dazu, dass das Gastsystem meldet das Gerät sei entfernt worden. Unter Umständen kann diese Aktion nützlich sein, falls das Gerät im Gastsystem Probleme verursacht. Die Aktion ist nur verfügbar, wenn ein USB-Port durchgereicht wurde.

Aktionen für das Formular

- *Aktualisieren*: Hiermit kann die Ansicht der USB-Geräte aktualisiert werden. Dies ist kann erforderlich sein, falls USB-Geräte ein- oder ausgesteckt wurden, um die neuen Informationen anzuzeigen.

14.4.9 *USB Zuweisung*

14.4.9.1 Felder in diesem Formular

- *Info*: Zeigt Informationen über den USB-Port.
- *Hub ID*: Zeigt die Hub-Identifikationsnummer an.
- *Port*: Zeigt die Port-Identifikationsnummer an.
- *Eingestecktes Gerät*: Wenn ein USB-Gerät im Port eingesteckt ist, wird hier der Name oder die Herstellerbezeichnung und weitere Informationen angezeigt.
- *Virtuelle Maschine*: In dieser Auswahl kann festgelegt werden, an welche virtuelle Maschine der USB-Port zugewiesen wird. Ist

ein USB-Gerät eingesteckt, wird dieses ebenso in der virtuellen Maschine benutzbar.

14.4.9.2 Aktionen für diesen Abschnitt

- *Zuweisen*: Diese Aktion beendet den Dialog, die Zuweisung wird gespeichert.

14.4.9.3 Aktionen für dieses Formular

- *Zurück*: Der Dialog wird beendet, die Änderungen weren verworfen.

14.4.10 *PCI-Geräte*

(Dieser Dialog befindet sich unter *Einstellungen – Virtualisierung – PCI-Gerät*

Geräte, die am PCI-Bus des V-Cube angeschlossen sind, können für virtuelle Maschinen freigegeben werden. In diesem Dialog sind die verfügbaren PCI-Geräte aufgelistet, diese können direkt zu einer virtuellen Maschine zugeordnet werden.

14.4.10.1 *Liste PCI Geräte*

In dieser Liste werden angeschlossene PCI-Geräte gelistet.

Felder in diesem Formular

- *Bus-Adresse*: Busadresse des PCI-Geräts.
- *Info*: Systeminformationen des PCI-Geräts.
- *Verwendung*: Die Benutzung des PCI-Geräts erfolgt entweder durch das Host-System oder durch eine virtuelle Maschine.

Aktionen für jeden Tabelleneintrag

- *Dem System zuweisen*: Ist ein Gerät vom Host-System freigegeben kann es mit dieser Aktion einer virtuellen Maschine zugewiesen werden. Ein entsprechender Dialog wird geöffnet. Diese Aktion steht nicht zur Verfügung, wenn das Gerät vom System benutzt wird.

  Ein Bandlaufwerk, das bei der Systeminstallation des V-Cube am PCI-Bus angeschlossen ist, wird automatisch durch das lokale Backup-System als Sicherungsziel verwendet. Vor der Zuweisung des entsprechenden PCI-Geräts zu einer virtuelle Maschine, muss dieses Sicherungsziel gelöscht werden.
- *Von VM Lösen*: Soll ein PCI-Gerät nicht mehr von einer virtuellen Maschine benutzt werden, kann es mit dieser Aktion getrennt werden. Anschließend steht das Gerät anderen virtuellen Maschinen oder dem Host-System wieder zur Benutzung wieder zur Verfügung.
- *Verbinden*: Hier kann eingestellt werden, ob das PCI-Gerät vom V-Cube benutzt werden soll. Wird das PCI-Gerät dem V-Cube zugeordnet, steht es keinen virtuellen Maschinen mehr zur Verfügung.
- *Von System lösen*: Mit dieser Aktion wird das Gerät vom Host-System getrennt und steht dann für die Zuweisung zu einer virtuellen Maschine bereit.
- *Treiber testen*: Wurde das Gerät zuvor von einer virtuellen Ma-

schine getrennt, kann es wieder an das Host-System gebunden werden. Hierfür wird der korrekte Treiber für das Gerät getestet und dann das Gerät ins Host-System eingebunden.

14.4.10.2 *Bearbeiten*

Felder in diesem Abschnitt

- *Bus-Adresse*: Hier wird die Bus-Adresse des PCI-Geräts angezeigt.
- *Info*: Zeigt Detailinformationen über das Gerät an.
- *Verwendung*: Hier wird angezeigt, ob das Gerät von einer virtuellen Maschine oder vom Host-System verwendet wird.
- *Treiber*: Zeigt den verwendeten Treiber für das Gerät an.

Felder in diesem Abschnitt

- *Ausgabe*: Hier wird der Fortschritt der Aktion angezeigt.

Aktionen für dieses Formular

- *Zurück*: Beenden der Bearbeitung.
- *Verbinden*: Mit dieser Aktion wird das PCI-Gerät ans Host-System gebunden und steht für die Verwendung in virtuellen Maschinen nicht zur Verfügung.
- *Trennen*: Mit dieser Aktion wird das PCI-Gerät vom Host-System getrennt und steht für die Verwendung in virtuellen Maschinen wieder zur Verfügung.
- *Treiber testen*: Wurde das Gerät zuvor von einer virtuellen Maschine getrennt, kann es wieder an das Host-System gebunden

werden. Hierfür wird der korrekte Treiber für das Gerät getestet und dann das Gerät ins Host-System eingebunden.

14.4.10.3 *Bearbeiten*

Felder in diesem Formular

- *Name*: Name des PCI-Geräts.
- *Info*: Zeigt Detailinformationen über das Gerät an.
- *Virtuelle Maschine*: Ist ein Gerät vom Host-System freigegeben kann es mit dieser Aktion einer virtuellen Maschine zugewiesen werden.

Aktionen für dieses Formular

- *Zurück*: Beenden der Bearbeitung, die Einstellungen werden nicht übernommen.
- *Zuweisen*: Beenden der Bearbeitung, das Gerät wird der virtuellen Maschine zugewiesen.
- *Lösen*: Beenden der Bearbeitung, das Gerät wird von virtuellen Maschine gelöst.

14.4.11 GUI-Referenz: *Virtuelle Maschinen*

(Dieser Dialog befindet sich unter *Einstellungen – Virtualisierung – Virtuelle Maschinen*

14.4.11.1 Abschnitt *Hinweis*

Felder in diesem Abschnitt

- *VT-Hardware*: Voraussetzung für die Benutzung der Virtualisierung ist Hardware mit Unterstützung von Intel VT oder AMD-V.
- *Virtualisierungsdienst*: Der Virtualisierungsdienst wurde gestoppt oder steht aus unbekanntem Grund nicht zur Verfügung.

14.4.11.2 *Liste virtueller Maschinen*

Virtuelle Maschine wählen

Spalten in der Tabelle

- *Name*: Hier erscheint der definierte Name der virtuellen Maschine.
- *Kommentar*: Hier erscheint der Kommentar.
- *Status*: Der Status einer virtuellen Maschine kann *running* , *paused* oder *shutoff* sein.

  running bedeutet, dass die virtuelle Maschine gestartet ist, oder dass vom Ruhezustand in den gestarteten Zustand gewechselt wurde.

  Wurde die virtuelle Maschine angehalten , so befindet sie sich im *paused*. In diesem Zustand werden laufende Daten im Speicher gehalten, damit der aktive Betrieb sehr schnell fortgesetzt werden kann. Diese laufenden Daten gehen verloren, wenn das Host-System neu gestartet wird. Passiert dies, ist danach der Status der virtuellen Maschine *shutoff*

  Wird die virtuelle Maschine heruntergefahren oder ausgeschaltet, wird ebenso der Status *shutoff* eingenommen.
- *CPUs*: Zeigt die Anzahl der zugeteilten virtuellen CPUs.

- *Speicher*: Zeigt den zugewiesenen Menge an Hauptspeicher in MBytes.
- *Snapshots*: Zeigt die Anzahl der erstellten Snapshots dieser virtuellen Maschine an.
- *VNC*: Zeigt an, ob Zugriff per VNC möglich ist.
- *Konsole*: Ist die virtuelle Maschine gestartet, wird in diesem Feld ein Link angezeigt, der nach dem anklicken die Bildschirmkonsole der entsprechenden virtuellen Maschine öffnet. Dazu wird ein neuer Browser-Reiter oder ein neues Fenster geöffnet.
- *Clustered*: Zeigt an, ob die VM im Cluster-Verbund verwaltet wird.
- *Priorität*: Zeigt an, welche Priorität der virtuellen Maschine vergeben wurde.

Aktionen für jeden Tabelleneintrag

- *Detail*: Mit dieser Aktion können Details über die verwendeten Laufwerke, die Konsole oder die Logausgabe der virtuellen Maschine eingesehen werden.
- *Konsole*: Mit dieser Aktion öffnet sich die Bildschirmkonsole der gewählten virtuellen Maschine in einem neuen Reiter oder Fenster des Browsers.
- *Einschalten*: Ist die virtuelle Maschine ausgeschaltet, kann sie mit dieser Aktion angeschaltet werden. Die Maschine bootet daraufhin vom angegebenen Boot-Laufwerk.
- *Reset*: Führt einen Kaltstart der virtuellen Maschine durch.
- *Reboot*: Mit dieser Aktion wird die virtuelle Maschine heruntergefahren und neu gestartet.
- *Herunterfahren*: Diese Aktion sorgt dafür, dass die virtuelle Maschine über das darauf laufende Betriebssystem heruntergefahren wird. Hierbei gehen keine Daten verloren, da Prozesse auf der virtuellen Maschine korrekt beendet werden. Im Arbeitsspei-

cher befindliche Daten werden entsprechend auf die Festplatten geschrieben.

- *Ausschalten*: Lässt sich eine virtuelle Maschine nicht korrekt herunterfahren, kann sie mit dieser Aktion einfach ausgeschaltet werden. Dabei können im virtuellen Arbeitsspeicher befindliche Daten verloren gehen.
- *Pausieren*: Mit dieser Aktion wird die virtuelle Maschine in einen Zustand versetzt, in dem sie wenige Ressourcen in Anspruch nimmt. Daten im zugewiesenen Arbeitsspeicher werden nicht auf Festplatte gespeichert. Die Informationen über die Sitzung gehen durch das Herunterfahren des Virtualisierungs-Host verloren. Die virtuelle Maschine kann nach *Suspend (RAM)* durch die Aktion *Aufwecken*
  wieder gestartet werden.
- *Aufwecken*: Befindet sich die virtuelle Maschine im Ruhezustand kann mit dieser Aktion der aktive Betrieb wieder aufgenommen werden.
- *Snapshots*: Ruft den Dialog zum Verwalten der Snapshots auf.
- *Storage Migration*: Ermöglicht das Verschieben von virtuellen Maschinen in einen Collax Cluster.
- *Bearbeiten*: Mit dieser Aktion öffnet sich der Dialog, um die virtuelle Maschine zu bearbeiten.
- *Löschen*: Mit dieser Aktion kann die virtuelle Maschine gelöscht werden.

Aktionen für dieses Formular

- *Neue VM anlegen*: Diese Aktion öffnet den Dialog zum Anlegen einer weiteren virtuellen Maschine.
- *Aktualisieren*: Hier kann die Ansicht des Formulars aktualisiert werden.

14.4.11.3 *Virtuelle Maschine ()*

Tab *Steuerung*, Abschnitt *Info*
Felder in diesem Abschnitt

- *Name*: Name der virtuellen Maschine.
- *Status*: Aktueller Betriebsstatus der virtuellen Maschine.
- *Clustered*: Zeigt an, ob die VM im Cluster-Verbund verwaltet wird.
- *Boot-Reihenfolge*: Zeigt das Laufwerk von dem gestartet wird.
- *Prozess-Priorität*: Zeigt die Priorität der virtuellen Maschine an.
- *Bildschirmvorschau*: Hier wird ein Miniatur-Bild der Bildschirmkonsole dargestellt.
- *VNC-Verbindung von*: Wurde ein Fernzugriff mittels eines VNC-Clients aufgebaut, wird in diesem Feld die IP-Adresse der verbundenen Arbeitsstation angezeigt.
- *CD-/DVD-ROM Info*: Hier wird angezeigt, ob in das CD-/DVD-ROM-Laufwerk ein ISO-Medium eingelegt wurde.

Tab *Steuerung*, Abschnitt *CD-/DVD-ROM Media*
Felder in diesem Abschnitt

- *Eingelegtes ISO-Image*: Hier wird angezeigt, welches ISO-Image im CD-/DVD-ROM eingelegt ist.
- *Verfügbare ISO-Images*: In dieser Auswahl werden die verfügbaren ISO-Images aufgelistet. Mit den nachfolgenden Aktionen, kann ein gelistetes ISO-Image in das virtuelle CDROM-Laufwerk eingelegt werden.

Aktionen für diesen Abschnitt

- *Treiber-ISO einlegen*: Hier kann ein ISO-Image, das Hardware-Treiber beinhaltet, eingelegt werden.
- *Auswerfen*: Hier kann ein eingelegtes ISO-Image aus dem CDROM-Laufwerk ausgeworfen werden.
- *ISO einlegen*: Mit dieser Aktion kann das gewählte ISO-Image ins CDROM-Laufwerk eingelegt werden.

Tab *Steuerung*, Abschnitt *Prozess-Priorisierung*
Felder in diesem Abschnitt

- *Priorität*: Hier wird die aktuelle Prioritätsstufe der virtuellen Maschine angezeigt. In der Auswahlliste kann bei Bedarf eine andere Priorität eingestellt werden.

Aktionen für diesen Abschnitt

- *Setzen*: Mit dieser Aktion wird die Einstellung gespeichert.

Aktionen für diesen Dialog

- *Einschalten*: Die virtuelle Maschine wird mit dieser Aktion gestartet.
- *Reboot*: Mit dieser Aktion wird die virtuelle Maschine heruntergefahren und neu gestartet.
- *Suspend (RAM)*: Mit dieser Aktion wird die virtuelle Maschine in einen Zustand versetzt, in dem sie wenige Ressourcen in Anspruch nimmt. Daten im zugewiesenen Arbeitsspeicher werden nicht auf Festplatte gespeichert. Die Informationen über die Sitzung gehen durch das Herunterfahren des Virtualisierungs-

Host verloren. Die virtuelle Maschine kann nach *Suspend (RAM)* durch die Aktion *Aufwecken*
wieder gestartet werden.

- *Aufwecken*: Befindet sich die virtuelle Maschine im Ruhezustand kann mit dieser Aktion der aktive Betrieb wieder aufgenommen werden.
- *Herunterfahren*: Diese Aktion sorgt dafür, dass die virtuelle Maschine über das darauf laufende Betriebssystem heruntergefahren wird. Hierbei gehen keine Daten verloren, da Prozesse auf der virtuellen Maschine korrekt beendet werden. Im Arbeitsspeicher befindliche Daten werden entsprechend auf die Festplatten geschrieben.
- *Ausschalten*: Lässt sich eine virtuelle Maschine nicht korrekt herunterfahren, kann sie mit dieser Aktion einfach ausgeschaltet werden. Dabei können im virtuellen Arbeitsspeicher befindliche Daten verloren gehen.

Tab *Konsole*
Felder in diesem Abschnitt

- : Sobald eine virtuelle Maschine startet, wird in diesem Reiter die Bildschirmkonsole angezeigt

  In diesem Abschnitt wird die Bildschirmkonsole einer gestarteten virtuellen Maschine angezeigt. Es stehen verschiedene Einstellungsmöglichkeiten zur Verfügung, um das Fenster anzupassen oder vom Browser abzulösen. Die Bildschirmkonsole wird über ein VNC-Java-Applet erzeugt. Ist ein Passwort für VNC-Verbindungen gesetzt, muss vor der Darstellung dieses Passwort eingegeben werden.

Tab *Statistik*
Felder in diesem Abschnitt

- : Hier werden ein graphische Statistik über die Ressourcen der virtuellen Maschine dargestellt. Darunter kann der die Nutzung von CPU, Arbeitsspeicher und Laufwerken innerhalb der letzten 4 Stunden eingesehen werden.

Tab *Log*, Abschnitt *Ausgabe*
Felder in diesem Abschnitt

- *Ausgabe*: Hier werden Details der Systemprozesse ausgeben. Sie dienen zur Kontrolle oder zum erkennen von fehlerhaften Einstellungen.

Aktionen für dieses Formular

- *Aktualisieren*: Mit dieser Aktion werden die Informationen über die virtuelle Maschine aktualisiert. Das Formular baut sich anschließend neu auf.
- *Zurück*: Bearbeiten des Formulars abbrechen, Einstellungen werden nicht übernommen.

14.4.11.4 *Snapshots*

Abschnitt *Disk Info*
Felder in diesem Abschnitt

- : Zeigt Informationen über den Festplattenbereich an, auf den Snapshots abgelegt werden.

Abschnitt *Aktueller Zustand*
Felder in diesem Abschnitt

- *Virtuelle Maschine*: Zeigt den Namen der virtuellen Maschine.
- *Status*: Zeigt den aktuellen Betriebsstatus der virtuellen Maschine.
- *Momentanes Disk-Delta*: Zeigt den Größenunterschied zum letzten Snapshot.
- *Hardware*: Zeigt zusätzliche Informationen zur virtuellen Hardwarekonfiguration.

Abschnitt *Snapshot*
Felder in diesem Abschnitt

- *Aktion*: Hier können Aktionen zum Erstellen, Zusammenführen, Löschen und Wiederherstellen von Snapshots ausgewählt werden. Das *Erstellen* eines Snapshots unterscheidet zwischen Online- und Offline-Snapshot. Ein Online-Snapshot speichert, neben dem Erstellen einer abgezweigten Snapshot-Disk, den aktuellen Speicherzustand der Maschine im laufenden Betrieb. Durch das *Zusammenführen* werden alle Snapshots bis zum dem gewählten Zeitpunkt vereinigt, die virtuelle Maschine behält ihren aktuellen Zustand. Anders verhält es sich bei den Aktionen *Wiederherstellen* oder *Löschen*. Hier werden Zustände jüngerer als des gewählten Snapshots nicht erhalten, sondern gelöscht.

- *Live*: Beim Erstellen oder beim Zusammenführen wird die VM nicht mehr angehalten, sondern der Vorgang wird während des Betriebs unmerklich für Anwender durchgeführt.
- *Kommentar*: Für jeden Snapshot kann eine kurze Information hinterlegt werden.
- *Snapshot*: Hier wird die Liste der Snapshots angezeigt.

Aktionen für diesen Abschnitt

- *Ausführen*: Führt die gewählte Aktion aus.

Abschnitt *Bestätigen*
Felder in diesem Abschnitt

- : Soll ein Snapshot erzeugt, gelöscht oder zusammengeführt werden, wird hier eine entsprechende Bestätigung erforderlich.

Abschnitt *Verfügbare Snapshots*
Felder in diesem Abschnitt

- : Hier werden die verfügbaren Snapshots mit weiteren Details aufgelistet.

Abschnitt *Ausgabe*
Felder in diesem Abschnitt

- *Ausgabe*: Zeigt den Prozessausgabe der initiierten Aktion.

Aktionen für dieses Formular

- *Herunterfahren*: Fährt die virtuelle Maschine herunter.
- *Ausschalten*: Schaltet die virtuelle Maschine aus.
- *Einschalten*: Schaltet die virtuelle Maschine ein.
- *Zurück*: Führt zurück zur Übersicht.

14.4.12 *Storage Migration*

Durch die Storage Migration können einerseits virtuelle Maschinen und deren Inhalt in die Verwaltung des Clusters verschoben werden. Zum anderen ist es möglich nur die Festplatten einer virtuellen Maschine auf Festplatten im Cluster zu migrieren.

14.4.12.1 Abschnitt *Ziel Typ*

Felder in diesem Abschnitt

- *Aktion*: Wenn eine oder mehrere Festplatten einer VM mit Inhalt zu einem anderen Festplattentyp migriert werden sollen, kann die Aktion Festplatte verschieben gewählt werden. Für die Migration in den Hochverfügbarkeits-Cluster kann die Aktion VM in Cluster verschieben gewählt werden.

14.4.12.2 Abschnitt *Allgemein*

Felder in diesem Abschnitt

- *VNC-Zugriff für ...*: Wird eine VM in den Cluster migriert, kann hier die Voreinstellung für die VNC-Gruppen gesetzt werden.

14.4.12.3 Abschnitt *Festplatte*
Felder in diesem Abschnitt

- *Inhalt von ...*: Zeigt den Namen der Festplatten, die migriert werden soll.
- *Auf vorhandene Festplatte migrieren*: Aus dieser Liste wird die Festplatte gewählt, auf die die Daten der oben genannten Festplatte kopiert werden sollen.
- *Auf neue Festplatte migrieren*: Aus dieser Liste wird die Festplatte gewählt, auf die die Daten der oben genannten Festplatte kopiert werden sollen.
- *Festplatte im Cluster*: In diesem Feld werden bestehende Festplatten des Cluster-Verbunds aufgelistet.

14.4.12.4 Abschnitt *Netzwerkkarte der VM*
Felder in diesem Abschnitt

- *Name*: In diesem Feld wird die lokale Netzwerkverbindung der VM angezeigt.
- *Verbinden mit virtuellem Switch im Cluster*: Hier kann angegeben werden, mit welchem virtuellen Netzwerkswitch die VM im Cluster verbunden werden soll. Diese Einstellung kann auch nach der Migration in der Cluster Administration bearbeitet werden.

14.4.12.5 Abschnitt *Status*
Felder in diesem Abschnitt

- *Ausgabe*: Zeigt Details über den Migrationsfortschritt.

14.4.12.6 Abschnitt *Festplatte*
Felder in diesem Abschnitt

- *Inhalt von ...*: Hier wird die Festplatte angezeigt, die migriert werden soll.
- *Umziehen auf ...*: Hier wird eine bestehende lokale Festplatte angegeben, auf die migriert werden soll.

14.4.12.7 Abschnitt *Convert Status*
Felder in diesem Abschnitt

- *Ausgabe*: Zeigt Details über den Migrationsfortschritt.

14.4.12.8 Aktionen für dieses Formular

- *Abbrechen*: Beendet den Dialog und führt zurück zur Übersicht.
- *Migration starten*: Die Storage Migration wird gestartet. Einzelne Snapshots der Festplatten werden auf der Zielfestplatte zusammengeführt. Der aktuelle Zustand bleibt also erhalten, die älteren Snapshot-Zustände werden gelöscht. Ein Ausgabefenster mit Details wird eingebendet.

14.4.13 GUI-Referenz: *V-Recovery*

(Dieser Dialog befindet sich unter *Einstellungen – Virtualisierung – V-Recovery*

Mit V-Recovery können die Daten von gesicherten virtuellen Maschinen auf drei Arten behandelt werden. Durch die Verifizierung

kann die Integrität der Sicherungsdaten geprüft werden. Werden einzelne Dateien aus der virtuellen Maschine benötigt, kann das Dateisystem einer VM mit der Funktion File-Restore exportiert und daraus einzelne Dateien über FTP kopiert werden, ohne dass die VM gestartet werden muss. Um vorübergehend eine VM direkt in Betrieb zu nehmen, kann die Funktion Instant-VM benutzt werden. Instant-VM sorgt dafür, dass eine separate VM-Instanz hergestellt wird, welche nicht mit der original VM kollidiert. Standardmäßig werden hierbei auch Kollisionen im Netzwerk vermieden.

14.4.13.1 *Temporär wiederhergestellte VMs*

In dieser Liste werden wiederhergestellte Daten von gesicherten virtuellen Maschinen angezeigt, die vorübergehend benutzt werden können.

Abschnitt *Info*
XXX missing title found

- : Hinweis, wohin eine Rücksicherung stattfinden kann.

Abschnitt *Keine Daten*
XXX missing title found

- : Die Liste ist leer, wenn keine VM-Daten temporär wiederhergestellt wurden.

XXX missing title found
Spalten in der Tabelle

- *Nr.*: Zeigt eine aufsteigende Nummerierung der wiederhergestellten Daten einer virtuellen Maschine.
- *Zeit/Datum*: Zeigt den Zeitpunkt, wann die Daten temporär wiederhergestellt wurden.
- *VM*: Zeigt den Namen der virtuellen Maschine.
- *Ort*: Zeigt an, in welchem Verzeichnis die Daten liegen.
- *Dateien*: Zeigt die Anzahl der wiederhergestellten Dateien an, die zu der virtuellen Maschine gehören.
- *V-Recovery Status*: Zeigt an, wie die Daten momentan durch die Funktionen von V-Recovery verwendet werden. Wenn diesselben VM-Daten mehrfach wiederhergestellt wurden, zeigt das Feld an, welche Einträge überschrieben wurden und somit möglicherweise nicht mehr verwendbar sind.

Aktionen für jeden Tabelleneintrag

- *Verifizierung*: Mit dieser Aktion können die temporären Daten einer Verifizierung unterzogen werden. Details werden in einem separaten Formular angezeigt.
- *File-Recovery*: Öffnet ein Formular, in dem die Festplatten der virtuellen Maschine und deren Inhalt im Netzwerk zur Verfügung gestellt werden können. Dadurch erhält man Zugriff auf das Dateisystem und damit auf einzelne Dateien der gewählten virtuellen Maschine, ohne dass die VM gestartet werden muss. Unterstützt werden die Dateisysteme VFAT, NTFS, Linux Ext, ReiserFS und XFS. Dateisysteme in Dynamic Disks (SFS) oder in Logischen Volumes (LVM) werden derzeit nicht unterstützt.
- *File-Recovery beenden*: Der Export des Dateisystems der VM

wird beendet. Unter Umständen kann der Export nicht beendet werden, solange noch eine Verbindung von einem Client, zum Beispiel von einem Browser, besteht. In dem Fall muss der Timeout der Verbindung abgewartet werden bevor das File-Recovery beendet werden kann.

- *Instant-VM*: Diese Aktion öffnet einen Dialog, um die VM zur Liste von *Virtuellen Maschinen* hinzuzufügen.
- *Instant-VM beenden*: Die Instant-VM wird aus der Liste von *Virtuellen Maschinen* entfernt.
- *Löschen*: Die temporär wiederhergestellten Daten der jeweiligen virtuellen Maschine werden von der Festplatte gelöscht und der Eintrag aus der Liste entfernt.

14.4.13.2 *Verifizierung*

Abschnitt *Verifizierung*
Felder in diesem Abschnitt

- *Alle Dateien vorhanden?*: Hier wird angezeigt, ob alle Daten die ursprünglich gesichert wurden, für weitere Aktionen in korrektem Zustand vorhanden sind.
- *VM-Zustand/Snapshot*: Zeigt die Liste von Snapshots der gewählten VM an.

Abschnitt *Nutzung*
Felder in diesem Abschnitt

- *Art*: In diesem Feld wird angezeigt, ob die temporären Daten der VM gerade für File-Recovery oder als Instant-VM genutzt werden.

Ebenso wird angezeigt, wenn die Daten nicht benutzt werden.

Abschnitt *Festplatte*
Felder in diesem Abschnitt

- *Arbeitsdatei*: Zeigt an welche Systemdatei als Festplatte verwendet wird.
- *Zustand der Backing files*: Zeigt den Zustand der Backing-Dateien an.

Abschnitt *Backing*
Felder in diesem Abschnitt

- *Arbeitsdatei*: Zeigt an welche Systemdatei als Festplatte des Backing verwendet wird.
- *Backing*: Zeigt das Backing.
- *Zustand*: Zeigt den Zustand.

XXX missing title found
Felder in diesem Abschnitt

- *Fehlerzustand*: Zeigt Fehler an, wenn es welche gibt.

Aktionen für dieses Formular

- *Zurück*: Führt zurück zur Übersicht.

14.4.13.3 *File-Recovery*

Von dieser Funktion werden die Dateisysteme VFAT, NTFS, Linux Ext, ReiserFS und XFS unterstützt.

Abschnitt *Verifizierung*
Felder in diesem Abschnitt

- *Alle Dateien vorhanden?*: Hier wird angezeigt, ob alle Daten die ursprünglich gesichert wurden, für weitere Aktionen in korrektem Zustand vorhanden sind.
- *VM-Zustand/Snapshot*: Zeigt die Liste von Snapshots der gewählten VM an.

Abschnitt *VM Daten exportieren über*
Felder in diesem Abschnitt

- *Exportmethode*: Hier kann gewählt werden, über welchen Netzwerkdienst die Daten für den Zugriff bereitgestellt werden sollen. Der Zugriff auf die Daten über FTP sollte mit einem FTP-Clientprogramm oder dem Windows Explorer erfolgen.

Abschnitt *Ausgabe*
Felder in diesem Abschnitt

- *Ausgabe*: Zeigt Details der ausgeführten Aktion an.

Aktionen für dieses Formular

- *Starten*: Diese Aktion stellt die Daten im Netzwerk zur Verfügung.
- *Zurück*: Führt zurück zur Übersicht.

14.4.13.4 *File-Recovery beenden*

Fehler
Felder in diesem Abschnitt

- : Zeigt einen Hinweis, falls das File-Recovery nicht beendet werden kann.

Abschnitt *Ausgabe*
Felder in diesem Abschnitt

- *Ausgabe*: Zeigt Details.

Aktionen für dieses Formular

- *Zurück*: Führt zurück zur Übersicht.

14.4.13.5 *Instant-VM*

Abschnitt *Verifizierung*
Felder in diesem Abschnitt

- *Alle Dateien vorhanden?*: Hier wird angezeigt, ob alle Daten die ursprünglich gesichert wurden, für weitere Aktionen in korrektem Zustand vorhanden sind.
- *VM-Zustand/Snapshot*: Zeigt die Liste von Snapshots der gewählten VM an.

Abschnitt *Info*
Felder in diesem Abschnitt

- : Informationsfeld.

Abschnitt *Netzwerk*
Felder in diesem Abschnitt

- *Netzwerk aktivieren*: Um Netzwerkkollisionen zu vermeiden, kann hier gewählt werden, ob die Instant-VM mit Netzwerkgerät starten soll oder nicht.
- *Zufällige MAC-Adresse*: Hier kann eine zufällige MAC-Adresse erzeugt automatish werden. Das ist sinnvoll, wenn die virtuelle Maschine ursprünglich DHCP verwendet hat.

Abschnitt *NIC*
Felder in diesem Abschnitt

- *Treiber*: Zeigt den Treiber des Netzwerkgeräts an.
- *Verbinde mit Switch-Device*: Hier kann der virtuelle Switch gewählt werden, mit dem die Instant-VM verbunden werden soll.

Abschnitt *Konsolen-Zugriff*
Felder in diesem Abschnitt

- *VNC-Zugriff*: Hier wird der Konsolenzugriff per VNC aktiviert.
- *Keymap*: Das entsprechende Tastaturlayout wird hier gewählt.
- *Passwort*: Zur Sicherheit kann hier ein Passwort für den VNC-Zugriff gesetzt werden.

Abschnitt *Info*
Felder in diesem Abschnitt

- : Informationsfeld.

Abschnitt *Info*
Felder in diesem Abschnitt

- : Informationsfeld.

Abschnitt *Ausgabe*
Felder in diesem Abschnitt

- *Ausgabe*: Zeigt Details nach Ausführen der Aktion.

Aktionen für dieses Formular

- *Instant-VM herstellen*: Erzeugt die Instant-VM in der Maschinenkontrolle. Die VM kann anschließend in der Maschinenkontrolle gestartet werden.
- *Zurück*: Führt zurück zur Übersicht.

15 Cluster und Cluster Management

15.1 Hochverfügbarkeit

In der Informationstechnologie beschreibt der Begriff „Cluster“ recht abstrakt eine Menge von Computern, die ihre Eigenschaften bündeln, um eine gemeinsame Arbeit zu verrichten. Vorrangig dient das dazu, die Arbeitsgeschwindigkeit von Abläufen zu erhöhen, die Last von Server-Diensten auf mehrere Schultern zu verteilen, oder um die Ausfallsicherheit zu erhöhen, also einen bestimmten Grad von Hochverfügbarkeit zu erhalten.

Collax stellt eine Hochverfügbarkeitslösung auf Basis der etablierten Collax-Plattform bereit. Durch redundante Server kann eine hohe Verfügbarkeit („High Availability“, „HA“) von Servern garantiert werden. Alle x86-Betriebssysteme lassen sich virtualisiert und hoch verfügbar betreiben.

Mit dem V-Cube wurde die innovative, auf KVM basierende Virtualisierungstechnologie eingeführt. Diese liegt ebenso dem Cluster zugrunde. Ein Cluster-Backend sowie eine zentrale, ausfallsichere Steuerung erweitern das gesamte Konzept. Im klassischen Fall mit zwei Cluster Nodes bedeutet das, dass die virtuellen Server, die auf dem ersten Hardware-Node laufen, im Falle ihres Ausfalls vom zweiten Node automatisch übernommen werden.

Damit die virtuellen Maschinen auf unterschiedlicher Hardware gestartet werden können, ist zwingend ein gemeinsamer Speicherplatz („Shared Storage“) erforderlich, auf dem die Festplatten-Abbilder der Virtuellen Maschinen liegen. Hierfür bietet die Collax-Lösung ein *Embedded SAN* , bei dem sich Festplatten der beteiligten Server über das Cluster Netzwerk ohne Verzögerung synchronisieren, so dass

auf den Maschinen identische Daten – und somit ein gemeinsamer Speicher – befinden.

15.2 Cluster-Domain

Um eine einfache und vor allem konsistente Konfiguration der Cluster-Knoten zu ermöglichen, verfügt der Collax-Cluster über eine Domänensteuerung. Dies ist eine Oberfläche, die das Verhalten aller Nodes im Cluster steuert.

In der Cluster Administration können einige Objekttypen angelegt und bearbeitet werden, die aus der üblichen Administrationsoberfläche bekannt sind. Dazu gehören Netze und Berechtigungen, und, für die eigentliche Cluster-Funktionalität essenziell, die virtuellen Maschinen.

15.3 Shared Storage

Unter Shared Storage versteht man hier Speicher, der sich im Zugriff aller beteiligter Maschinen befindet. Gemeinsamer Speicherplatz ist zwingend erforderlich, um virtuelle Maschinen auf unterschiedlichen Hardware-Nodes starten zu können.

Collax stellt die Möglichkeit zur Verfügung, gemeinsamen Speicherplatz ohne den Einsatz eines teuren SANs zu betreiben. Die Technik von verteilten, replizierten Blockgeräten (eSAN) kann für den Einsatz eines Zwei-Node-Clusters genutzt werden.

15.4 Erstkonfiguration eines Clusters

Nachfolgend werden die Administrationspunkte beschrieben, die erforderlich sind, einen Cluster-Verbund einzurichten, oder eine Maschine einem Cluster-Verbund beitreten zu lassen.

15.4.1 GUI-Referenz: *Lokaler Node*

(Dieser Dialog befindet sich unter *Einstellungen – Cluster – Lokaler Node – Allgemein*)

Diese Dialog zeigt Informationen über den Status der lokalen Maschine in Bezug auf eine Cluster-Domäne an.

15.4.1.1 Tab *Einstellungen*, Abschnitt *Cluster-Dienst*

Felder in diesem Abschnitt

- *Aktiviert*: Hier wird angezeigt, ob der Cluster-Dienst gestartet ist. Nach dem Beitritt zu einem Cluster wird der Cluster-Dienst gestartet. Ist der Host noch keinem Cluster beigetreten, bleibt der Dienst deaktiviert.

15.4.1.2 Tab *Einstellungen*, Abschnitt *Lokaler Node*

Felder in diesem Abschnitt

- *Node-ID*: Hier wird die Identifikationsnummer von diesem Node im Clusterverbund angezeigt.

15.4.1.3 Tab *Einstellungen*, Abschnitt *Netzwerk*
Felder in diesem Abschnitt

- *Cluster Interconnect Link*: Zeigt den Namen des Links an, über den der Node im Cluster kommuniziert.
- *Cluster Interconnect Network*: Zeigt das Netzwerk an, über das der Node im Cluster kommuniziert.
- *Interface für Verknüpfung von virtuellen Switches innerhalb des Clusters*: Standardmäßig sind neu hinzugefügte virtuelle Switches im Cluster zunächst nicht verknüpft. Damit virtuelle Maschinen, die auf verschiedene Cluster Nodes verteilt sind, über diese virtuellen Switches kommunizieren können, ist es erforderlich eine physikalische Verknüpfung herzustellen. Diese Verknüpfung wird anhand der hier gewählten Netzwerkschnittstelle vorbereitet. Unter der Annahme, dass Cluster-Nodes über diesselbe Hardware-Ausstattung verfügen, sollte auf jedem Node dasselbe Interface gesetzt sein.

  Voreingestellt (leere Auswahl) ist das Interface des Cluster-Interconnect, was in den meisten Konfigurationen die optimale Einstellung ist.

  Die eigentliche Verknüpfung wird mit der Option Virtuellen Switch innerhalb des Clusters verbinden (S. 466) aktiviert.

15.4.1.4 Tab *Einstellungen*, Abschnitt *Domäneneinstellungen*
Felder in diesem Abschnitt

- *Domäne*: Zeigt den Namen der Cluster-Domäne an.
- *Base-DN*: Zeigt die LDAP-Base-DN an.
- *Bind-DN*: Zeigt die LDAP-Bind-DN an.

15.4.1.5 Tab *Berechtigungen*
Felder in diesem Abschnitt

- *Cluster Backend*: Netzwerke und Hosts der angehakten Gruppen haben Zugriff auf verschiedene Dienste.

15.4.1.6 Aktionen für dieses Formular

- *Abbrechen*: Der Dialog wird beendet und die Änderungen verworfen.
- *Speichern*: Der Dialog wird beendet und die Änderungen gespeichert.

15.4.2 *Assistent für das Cluster-Netzwerk*

(Dieser Dialog befindet sich unter *Einstellungen – Cluster – Lokaler Node – Cluster Netzwerk*)

Der Assistent zur Einrichtung des Cluster-Netzwerks für diesen Node richtet in wenigen Schritten eine Cluster-Interconnect-Verbindung ein. Zusätzlich hilft der Assistent dabei, festzulegen, über welche Schnittstellen oder Verbindung später die virtuellen Maschinen erreichbar sein sollen. Dies kann über den LocalNet-Link oder über separate physikalische Schnittstellen geschehen.

15.4.2.1 Felder in diesem Formular

- *Ablauf*: Im Schritt Eins wird die Verbindung zwischen den Cluster-Nodes definiert. Der Assistent zeigt an, wenn hier mehrere

Netzwerkschnittstellen zur Bündelung verfügbar sind. Es können dann Vorgaben zu Schnittstellen oder Verkabelung getroffen werden. Für diesen Cluster Interconnect Link ist eine Nummer für das Virtuelle LAN (VLAN) anzugeben. Die Aktivierung von Jumbo-Frames erhöht die Durchsatzrate zwischen den Cluster Nodes. Voraussetzung ist, dass die Netzwerkschnittstellen die Paketgröße von 9000 Bytes verarbeiten können. Anschließend werden Einstellungen für das Cluster Interconnect Netzwerk vorgenommen. Hier können die vorgeschlagenen Werte übernommen werden, sofern diese sich nicht mit vorhandenen Netzwerken überschneiden.

Damit zukünftig virtuelle Maschinen im Netzwerk erreichbar sind, wird im zweiten Schritt eine freie Schnittstelle definiert. Wenn mehrere Schnittstellen gebündelt werden können, zeigt der Assistent dies an. Wenn genügend Schnittstellen zur Verfügung stehen ist es von Vorteil hier nur unverwendete Schnittstellen auszuwählen.

In der Zusammenfassung können die Einstellungen des Assistenten nochmal geprüft und geändert werden. Mit der Aktion Fertigstellen werden die Einstellungen übernommen. Ein grafisches Schema des Cluster-Netzwerks kann unter *Ethernet-Status* eingesehen werden.

- *Konfiguration*: Beim Fertigstellen des Assistenten wird der zusätzliche Link ClusterLink mit der angegeben IP-Adresse und VLAN-Nummer angelegt. Die ausgewählten Schnittstellen des Cluster-Links werden immer für Ethernet-Bündelungen vorbereitet. So ist es sehr leicht möglich, später höhere Ausfallsicherheit und Bandbreite mit zusätzlichen Schnittstellen zu gewährleisten.

  Durch die Auswahl der Schnittstelle für die virtuellen Maschinen wird ein virtueller Switch erzeugt, an den die Maschinen später angeschlossen werden können. Auch auf diesem Switch

kann später eine höhere Ausfallsicherheit oder Bandbreite durch hinzufügen von Schnittstellen gewährleistet werden.

15.4.3 *Assistent zur Einrichtung eines Clusters*

(Dieser Dialog befindet sich unter *Einstellungen – Cluster – Lokaler Node – Cluster initiieren/beitreten*)

Der Assistent zur Einrichtung eines Clusters initiiert in wenigen Schritten den Server als Cluster Node und generiert eine Cluster Domain oder lässt den Server in eine Cluster Domain beitreten.

15.4.3.1 Abschnitt *Hinweis*
Felder in diesem Abschnitt

- *Information*: Der Assistent kann ausgeführt werden, wenn der Host noch keinem Cluster beigetreten ist.

15.4.3.2 Felder in diesem Formular

- *Ablauf: Cluster initiieren*: Soll ein neuer Cluster-Verbund initiiert werden, ist im Schritt Eins die entsprechende Option zu wählen.

  Im zweiten Schritt ist die Domäne des Clusters anzugeben. Um den Cluster zu initiieren, muss das Passwort des lokalen Administrators angegeben werden.
- *Konfiguration*: Beim Fertigstellen des Assistenten wird mit der Cluster-Domäne das LDAP-Verzeichnis neu initialisiert, der KDC-Dienst eingerichtet und gestartet. Durch das Fertigstellen werden alle erforderlichen Cluster-Dienste und der Dienst zur Synchronisation der Cluster-Konfiguration gestartet.

Zeigt der Logauszug die Meldung „Done“, kann nun die Cluster-Administration durch Einloggen auf der URL https://serverip:8001 aufgerufen werden.

- *Ablauf: Cluster beitreten*: Soll der Server einem bestehenden Cluster beitreten, muss im ersten Schritt die entsprechende Option gewählt werden.

  Im zweiten Schritt ist die IP-Adresse eines Hosts anzugeben, der schon Mitglied im gewünschten Cluster-Verbund und im Cluster Interconnect-Netzwerk ist. Für den Beitritt zu einer Cluster-Domäne ist das Passwort des Administrators im Cluster anzugeben.

  Konnten Informationen der vorhandenen Cluster-Domäne abgerufen werden, wird die Zusammenfassung angezeigt. Für den letztendlichen Beitritt ist die Aktion Fertigstellen auszuführen.
- *Konfiguration*: Beim Fertigstellen des Assistenten wird das LDAP-Verzeichnis neu initialisiert und der Kerberos-Dienst eingerichtet. Durch das Fertigstellen werden die Cluster-Dienste und der Dienst zur Synchronisation der Cluster-Konfiguration gestartet. Zeigt der Logauszug die Meldung „The join of this node has been finished“, kann die Cluster-Administration durch Einloggen auf der URL https://serverip:8001 aufgerufen werden.

15.5 Konfiguration der Cluster-Domain

15.5.1 GUI-Referenz: *Infrastruktur*

(Dieser Dialog befindet sich unter *Cluster-Administration – Allgemein – Infrastruktur*

Im folgenden Dialog werden die Grundeinstellungen der benötigten Infrastruktur des Clusters angezeigt. Die wichtigsten Einstellungen sind die Angabe der NTP-Server sowie die Angabe eines E-Mailservers für den Empfang von Status-E-Mails oder ein funktionstüchtiger DNS-Server um korrekte Namensauflösung für die angegebenen NTP-Server und E-Mailserver durchzuführen.

Diesbezügliche Einstellungen, die nicht über die Cluster-Administration vorgenommen werden, können das gesamte Cluster-System außer Funktion setzen. Änderungen sollen also an dieser Stelle gemacht werden.

15.5.1.1 Abschnitt *DNS*

Die DNS-Einstellungen dienen zur Interpretation von unqualifizierten Host-Namen im lokalen Netzwerk. Wenn erforderlich kann hier eine entsprechende Suchliste und ein DNS-Forwarder eingetragen werden, um Namensauflösung auf den Cluster-Nodes zu gewährleisten.

Felder in diesem Abschnitt

- *Suchliste*: Hier werden DNS-Suffixe eingetragen, die an Hostnamen angehängt werden. Falls nicht klar ist, für was diese Liste gebraucht werden kann, kann die Liste leergelassen werden. Mehrere Einträge werden durch Leerzeichen getrennt. Es werden maximal sechs Domains und 256 Zeichen unterstützt.
- *Forwarder*: Der hier gewählte Server übernimmt die Auflösung fremder DNS-Zonen. DNS-Anfragen werden an diesen Server weitergeleitet.

15.5.1.2 Abschnitt *NTP*

Felder in diesem Abschnitt

- *Server*: Hier kann ein NTP-Server für den korrekten Zeitabgleich eingetragen werden. Als Standard ist hier mindestens ein NTP-Server eingetragen.

15.5.1.3 Abschnitt *Mail*

Felder in diesem Abschnitt

- *Administrative E-Mail-Adresse*: Hier wird die E-Mail-Adresse des Systemverantwortlichen eingetragen. An diese Adresse werden Meldungen des Systems gesendet.
- *E-Mail-Domain*: Diese E-Mail-Domain wird bei abgehenden E-Mails angehängt, wenn E-Mails vom System versendet werden.

  Wird hier keine E-Mail-Domain angegeben, wird der Name des Systems (FQDN) verwendet. Dies kann jedoch zu Problemen führen, wenn E-Mails an externe Empfänger weitergeleitet werden.

- *Relay-Host*: Soll ein Relay-Server verwendet werden, wird hier der Server, an den E-Mail weitergeleitet werden sollen, ausgewählt.
- *Benutzerkennung für Relay-Host*: Verlangt der Relay-Server Authentifizierung kann hier die entsprechende Benutzerkennung (Login) eingetragen werden.
- *Passwort*: Verlangt der Relay-Server Authentifizierung kann hier das entsprechende Passwort zur Benutzerkennung eingetragen werden.

15.5.1.4 Aktionen für dieses Formular

- *Abbrechen*: Dialog der Grundeinstellungen beenden, die Einstellungen werden verworfen.
- *Speichern*: Dialog der Grundeinstellungen beenden, die Einstellungen werden gespeichert.

15.5.2 GUI-Referenz: *Storage*

15.5.2.1 Abschnitt *eSAN*
Felder in diesem Abschnitt

- *Node 1*: Um verteilte, replizierte eSAN-Festplatten im Cluster benutzen zu können, muss hier einer der Cluster-Nodes angegeben werden.
- *Node 2*: Um verteilte, replizierte eSAN-Festplatten im Cluster benutzen zu können, muss hier einer der Cluster-Nodes angegeben werden.

- Zeigt an, auf welche Cluster Nodes die eSAN-Festplatten verteilt sind.

15.5.2.2 Abschnitt *iSCSI-Inititator*

Um iSCSI-LUNs eines SAN als Festplatten benutzen zu können, ist der iSCSI Initiator zu aktivieren. Der Initiator funktioniert wie ein physikalischer SCSI Bus-Adapter, allerdings sendet er SCSI-Kommandos nicht über SCSI-Kabel, sondern verpackt diese in TCP/IP-Pakete.

Felder in diesem Abschnitt

- *Aktivieren*: Mit dieser Option wird der iSCSI Initiator aktiviert. Die Aktivierung ist erforderlich, um externe iSCSI-LUNs ins System einzubinden.
- *Authentifizierung für iSCSI-Discovery*: Um iSCSI Targets zu ermitteln, kann es aus Sicherheitsgründen erforderlich sein, dass dafür Authentifizierungsdaten anzugeben sind. Die Option kann aktiviert werden, falls ein iSCSI discovery login erforderlich ist.
- *Benutzer*: Hier wird der Benutzer-Login für die Authentifizierung angegeben.
- *Passwort*: Hier wird das Passwort zum Benutzer-Login angegeben.

15.5.2.3 Abschnitt *Cluster-Share*

Um bestimmte Funktionen wie Live Migration und Snapshots für virtuelle Maschinen bereit stellen zu können, ist es erforderlich einen

Datenbereich zu benennen, auf den von PC-Arbeitsstationen oder von beiden Cluster-Nodes aus gelesen oder geschrieben werden kann. Dieser Datenbereich wird durch das Cluster-Share definiert und basiert immer auf einer Disk, die per iSCSI oder Embedded SAN eingerichtet wurde. Es gibt im Collax Cluster genau ein Cluster Share.

Felder in diesem Abschnitt

- *Name*: Zeigt den Freigabenamen des Cluster-Shares an.
- *Disk für Cluster-Daten/-Share*: Hier wird eine vorhandene Festplatte gewählt, die noch nicht von einer VM oder andersweitig verwendet wird. Enthält die Festplatte noch kein Cluster-Dateisystem wird dies automatisch erzeugt. Dadurch gehen alle vorhandene Daten verloren. Diese Festplatte kann als Typ iSCSI oder eSAN definiert sein und dient dazu, um Snapshots von VMs, oder VM-Image- oder ISO-Dateien zentral zu lesen oder zu speichern.
- *Exportiere über*: In dieser Liste sind alle Dienste und Protokolle aufgeführt, über die das Verzeichnis im Netzwerk exportiert werden kann. Wenn das Share per SMB/CIFS exportiert wird, müssen die Passwörter der Benutzer nach der Aktivierung neu gesetzt werden, damit die Authentifizierung funktioniert.
- *Leseberechtigung für*: Gibt die Gruppen und Netzwerke an, die auf das Cluster Share Leseberechtigung erhalten.
- *Schreibberechtigung für*: Gibt die Gruppen und Netzwerke an, die auf das Cluster Share Schreibberechtigung erhalten.

15.5.2.4 Aktionen für dieses Formular

- *Abbrechen*: Beendet den Dialog, die Änderungen werden verworfen.
- *Speichern*: Auf der oben gewählten Festplatte wird während der Aktivierung ein Cluster-Dateisystem angelegt. *Alle Daten auf der Festplatte gehen dadurch verloren.* Diese Aktion beendet diesen Dialog, die Änderungen werden gespeichert.

15.5.3 *Überwachungstests*

Hier können Tests zur Überwachung von Hosts und virtuellen Maschinen definiert werden. Zur Auswahl stehen einfache Protokolltests und auch NRPE-Tests, mit welchen Überwachungstests auf Hosts oder virtuellen Maschinen ausgeführt werden können.

15.5.3.1 GUI-Referenz: *Überwachungstests*

(Dieser Dialog befindet sich unter *Cluster-Administration – Allgemein – Überwachungstests*)

Felder in dieser Tabelle

- *Name*: Hier wird der Name des Tests angezeigt.
- *Überwachter Dienst*: Zeigt an, welcher Dienst überwacht wird.
- *Kommentar*: Hier werden weitere Informationen angezeigt.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Öffnet den Dialog zum Bearbeiten eines Eintrags.
- *Löschen*: Entfernt den gewählten Eintrag aus der Liste.

Aktionen für dieses Formular

- *Hinzufügen*: Öffnet den Dialog, um einen Überwachungstest hizuzufügen.

15.5.3.2 *Eintrag Bearbeiten*

Tab *Grundeinstellungen*, Abschnitt *Grundeinstellungen*

Felder in diesem Abschnitt

- *Name*: Hier wird ein Name für den Test angegeben oder angezeigt.
- *Kommentar*: Weitere Informationen können hier eingegeben werden.
- *Überwachter Dienst*: Aus der Liste können entsprechende Dienste gewählt werden, die nachfolgend auf zu bestimmenden Hosts getestet werden.
- *Port*: Für Dienste die unspezifizierte Netzwerk-Ports benutzen kann hier der entsprechende Port angegeben werden.
- *Host*: Werden Dienste getestet, welche andere unbekannte Hosts ansteuern oder auswerten (Z.Bsp.: DNS), kann hier der Host angegeben werden.
- *URL*: Für Dienste die URLs auswerten, kann in diesem Feld die URL angegeben werden.
- *Benutzer*: Falls der überwachte Dienst Authentifizierung verlangt, kann hier der Benutzer angegeben werden.

- *Passwort*: Falls der überwachte Dienst Authentifizierung verlangt, kann hier das Passwort zum zuvor angegebenen Benutzer angegeben werden.
- *Parameter*: Für die Tests, die entfernt Skripte ausführen (NRPE/NSClient++) werden in diesem Feld die entsprechenden Parameter angegeben. Im einfachen Fall, dass ein Kommando ausgeführt werden soll wird hier „-c KOMMANDO“ angegeben. Wird ein Collax Server überwacht, kann zum Beispiel „-c System_Load“ angegeben werden, um dessen Systemauslastung zu testen und auszuwerten.
- *Prozess*: Für Microsoft Windowssysteme kann hier ein bestimmter Prozess überprüft werden. Angegeben wird der Prozess inklusive der Endung (Z.B. Explorer.exe).

Tab *Grundeinstellungen*, Abschnitt *Hinweis*
Felder in diesem Abschnitt

- : Für die Benutzung von NRPE und NSClient erscheint hier ein Hinweis.

Tab *Hosts*, Abschnitt *Hosts*
Felder in diesem Abschnitt

- *Einstellungen*: Hosts, die mit diesem Test überwacht werden.

Aktionen für dieses Formular

- *Abbrechen*: Bearbeiten der Überwachungstests beenden. Die Änderungen werden verworfen.
- *Speichern*: Bearbeiten der Überwachungstests beenden. Die Änderungen werden gespeichert.

15.5.4 *Gruppen*

(Dieser Dialog befindet sich unter *Cluster-Administration – Richtlinien – Gruppen*

Über die Gruppen wird der Zugriff auf alle Dienste im Cluster geregelt. In diesem Dialog werden Gruppen angelegt und deren Rechte verwaltet. Eine Gruppe kann dabei aus Benutzern, Rechnern und Netzwerken bestehen.

Dieser Dialog besteht aus mehreren untergeordneten Dialogen.

15.5.4.1 *Gruppe wählen*

In dieser Liste werden die bestehenden Gruppen angezeigt.

Felder in diesem Formular

- *Name*: Der Name der Gruppe.
- *Kommentar*: Ein Kommentartext zur Gruppe.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion wird die Konfiguration der ausgewählten Gruppen bearbeitet.
- *Benutzer*: Mit dieser Aktion werden alle Benutzer und ihre Mitgliedschaft in der Gruppe angezeigt. Der Mitgliedschaftsstatus kann geändert werden.

  In eine importierte Netzwerkgruppe können keine Benutzer aufgenommen werden. Diese Aktion wird daher nur für lokal angelegte Gruppen angezeigt.
- *Rechner*: Mit dieser Aktion werden alle Rechner und ihr Mitglied-

status in der Gruppe angezeigt. Der Mitgliedschaftsstatus kann geändert werden.
- *Netze*: Mit dieser Aktion werden alle Netzwerke und ihr Mitgliedstatus in der Gruppe angezeigt. Der Mitgliedschaftsstatus kann geändert werden.
- *Löschen*: Diese Aktion löscht die ausgewählte Gruppe.

Aktionen für dieses Formular

- *Gruppe anlegen*: Mit dieser Aktion wird eine neue Gruppe angelegt.

15.5.4.2 *Cluster-Gruppe bearbeiten*

In diesem Dialog wird eine zuvor ausgewählte Gruppe bearbeitet.

Felder in diesem Formular

- *Name der Gruppe*: Name der Gruppe.
- *Kommentar*: In diesem Feld kann ein Kommentartext zu dieser Gruppe erstellt werden.

Aktionen für dieses Formular

- *Abbrechen*: Bearbeiten der Gruppen-Konfiguration beenden. Die Änderungen werden verworfen.
- *Speichern*: Bearbeiten der Gruppen-Konfiguration beenden. Die Änderungen werden gespeichert.

15.5.4.3 *Berechtigungen*

In diesem Dialog sind alle Berechtigungen sichtbar. Berechtigungen, die der zu bearbeitenden Gruppe erteilt sind, sind markiert.

Die Berechtigungen sind additiv, d. h., wenn ein Gruppenmitglied zu mehreren Gruppen gehört, in denen dieselbe Berechtigung in einigen aktiviert und in anderen deaktiviert ist, ist die Berechtigung für dieses Mitglied aktiviert. Es reicht aus, wenn eine Berechtigung für das Mitglied in einer einzigen Gruppe aktiviert ist.

Aktionen für dieses Formular

- *Abbrechen*: Bearbeiten der Gruppen-Berechtigungs-Konfiguration beenden. Die Änderungen werden verworfen.
- *Speichern*: Bearbeiten der Gruppen-Berechtigungs-Konfiguration beenden. Die Änderungen werden gespeichert.

15.5.4.4 *Benutzer*

In diesem Dialog sind alle angelegten Benutzer sichtbar. Benutzer, die zu der bearbeiteten Gruppe gehören, sind markiert.

In diesem Dialog werden die Mitglieder der Gruppe ausgewählt.

Felder in diesem Formular

- *Name der Gruppe*: Name der Gruppe, der die Benutzer angehören.

Aktionen für dieses Formular

- *Abbrechen*: Bearbeiten der Gruppen-Konfiguration beenden. Die Änderungen werden verworfen.
- *Speichern*: Bearbeiten der Gruppen-Konfiguration beenden. Die Änderungen werden gespeichert.

15.5.4.5 *Rechner*

In diesem Dialog sind alle angelegten Rechner sichtbar. Rechner, die zu der bearbeiteten Gruppe gehören, sind markiert.

In diesem Dialog werden die Rechner ausgewählt, die zu der Gruppe gehören sollen.

Felder in diesem Formular

- *Name der Gruppe*: Hier wird der Name der Gruppe angezeigt, der die Rechner angehören.

Aktionen für dieses Formular

- *Abbrechen*: Bearbeiten der Gruppen-Konfiguration beenden. Die Änderungen werden verworfen.
- *Speichern*: Bearbeiten der Gruppen-Konfiguration beenden. Die Änderungen werden gespeichert.

15.5.4.6 GUI-Referenz: *Netzwerke*

In diesem Dialog sind alle angelegten Netzwerke sichtbar. Netze, die zu der bearbeiteten Gruppe gehören, sind markiert.

In diesem Dialog werden die Netzwerke ausgewählt, die zu der Gruppe gehören sollen.

Felder in diesem Formular

- *Name der Gruppe*: Hier wird der Name der Gruppe angezeigt.

Aktionen für dieses Formular

- *Abbrechen*: Bearbeiten der Gruppen-Konfiguration beenden. Die Änderungen werden verworfen.
- *Speichern*: Bearbeiten der Gruppen-Konfiguration beenden. Die Änderungen werden gespeichert.

15.5.5 *Benutzer*

(Dieser Dialog befindet sich unter *Cluster-Administration – Richtlinien – Benutzer*)

In diesem Dialog werden die Benutzer der Cluster-Domain verwaltet.

15.5.5.1 *Benutzer auswählen*

Hier werden alle in der Cluster-Domain angelegten Benutzer angezeigt. Neue Benutzer können hier hinzugefügt, bestehende Benutzer können hier bearbeitet oder gelöscht werden.

Spalten in der Tabelle

- *Login*: Der Login-Name des Benutzers. Dieser wird zur Authentifizierung an den Diensten genutzt. Für den Login-Namen sollten nur Kleinbuchstaben verwendet werden.
- *Vorname*: Zeigt den Vornamen den Benutzers.
- *Nachname*: Zeigt den Nachnamen des Benutzers.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion wird das Benutzerkonto bearbeitet.
- *Passwort setzen*: Diese Aktion kann ausgeführt werden, wenn der Benutzer auf allen Cluster-Nodes existiert. Durch diese Aktion wird ein weiterer Dialog zum Setzen des Passwörters geöffnet.
- *Löschen*: Durch diese Aktion wird das Benutzerkonto gelöscht.

Aktionen für dieses Formular

- *Benutzer anlegen*: Mit dieser Aktion wird ein neues Benutzerkonto erstellt.

15.5.5.2 *Benutzer bearbeiten*

In diesem Dialog können die Einstellungen des Benutzerkontos bearbeitet werden.

Tab *Grundeinstellungen*, Abschnitt *Grundeinstellungen* Felder in diesem Abschnitt

- *Login-Name*: Der Login-Name des Benutzers wird zur Authentifizierung bei den verschiedenen Diensten der Cluster-Domäne eingesetzt.

  Der Login-Name sollte in Kleinbuchstaben angegeben werden. Erlaubt sind nur die Buchstaben „a“ bis „z“ (keine Umlaute o. ä.), Ziffern, der Unterstrich „_“ sowie (nicht empfohlen) die Großbuchstaben „A“ bis „Z“. Der Login-Name darf nicht mit einer Ziffer beginnen.

  Das Eingabefeld erscheint nur, wenn ein neues Benutzerkonto angelegt wird. Besteht der Benutzer schon, wird der Login-Name angezeigt und kann nicht verändert werden.
- *Shell des Benutzers*: Hier kann eingestellt werden, ob ein Benutzer sich per Konsole auf dem Server anmelden kann.

  Wollen Sie einen User, der nur über die Weboberfläche Zugriff auf das System hat, dann wählen sie „Keine“.

  Wollen Sie einen User, der sowohl über die Weboberfläche, als auch per Konsole Zugriff auf das System hat, dann wählen sie „Bash“.
- *Primäre Gruppe*: Jeder Benutzer in Linux-Systemen gehört einer primären Gruppe an. In dieser Auswahl kann diese primäre Gruppe aus den bestehenden festgelegt werden.
- *Vorname*: Der Vorname des Benutzers.
- *Nachname*: Der Nachname des Benutzers.
- *Tätigkeit*: Die Tätigkeit des Benutzers.
- *E-Mail-Adressen*: In diesem Eingabefeld können E-Mail-Adressen für den Benutzer angegeben werden, die als E-Mail-Alias angelegt werden. Wird dabei die Maildomain nicht angegeben, erhält der Benutzer den Alias in der Default-E-Mail-Domain die unter *Cluster-*

Administration – Allgemein – Grundeinstellungen angegeben ist.

An diese E-Mail-Adresse werden ausschließlich Benachrichtigungen versendet, der Benutzer erhält dadurch kein Postfach auf diesem System.

Pro Zeile wird eine Adresse eingegeben, ein Trennzeichen ist nicht erforderlich.

- *Telefon*: Hier können eine oder mehrere Telefonnummern für den Benutzer angegeben werden. Pro Zeile wird eine Nummer eingegeben, ein Trennzeichen ist nicht erforderlich.

Tab *Gruppenzugehörigkeit*, Abschnitt *Gruppenzugehörigkeit*

Felder in diesem Abschnitt

- *Gruppen*: Hier kann konfiguriert werden, zu welchen Gruppen der Benutzer gehört.

Aktionen für dieses Formular

- *Abbrechen*: Bearbeiten des Benutzerkontos beenden. Die Änderungen werden verworfen.
- *Speichern*: Bearbeiten des Benutzerkontos beenden. Die Änderungen werden gespeichert.

15.5.5.3 *Passwort ändern*

In diesem Dialog kann, nachdem der Benutzer auf allen Cluster-Nodes existiert, das Passwort gesetzt oder geändert werden.

Felder in diesem Formular

- *Benutzer*: Zeigt den vollständigen Namen des Benutzers.
- *Login*: Zeigt das Login des Benutzers.
- *Neues Passwort*: Das Passwort des Benutzers.
- *Passwort (Wiederholung)*: Da das Passwort aus Sicherheitsgründen bei der Eingabe nicht angezeigt wird, muss es hier zur Kontrolle ein zweites Mal eingegeben werden.

Aktionen für dieses Formular

- *Abbrechen*: Bearbeiten der Passwortänderung beenden. Die Änderungen werden verworfen.
- *Ändern*: Bearbeiten der Passwortänderung beenden. Die Änderungen werden gespeichert und steht ohne Aktivierung auf allen Cluster-Nodes zur Verfügung.

15.5.6 *Hosts*

Als „Host“ werden einzelne Rechner bezeichnet, die in der Cluster-Domain bekannt sind. Im einfachsten Fall muss nur die IP-Adresse eingetragen werden. Damit kann ein Host überwacht oder in den *Benutzungsrichtlinien* einer Gruppe zugeordnet werden.

Ein Host als existierendes Element ist Voraussetzung für verschiedene Einstellungen, welche die Dienste betreffen. So muss zur Angabe eines NTP, DNS oder SMTP-Server im Dialog Grundeinstellungen zuvor der entsprechende Host in diesem Dialog hinzugefügt worden sein.

15.5.6.1 *Host wählen*

(Dieser Dialog befindet sich unter *Cluster-Administration – Richtlinien – Hosts*)

In dieser Liste werden alle dem System bekannten Hosts im lokalen Netz angezeigt.

Spalten in der Tabelle

- *Name*: Zeigt den Namen des Hosts.
- *Kommentar*: Zeigt weitere Informationen an.
- *FQDN*: Zeigt den FQDN des Hosts an.
- *IP-Adressen*: Hier wird die IP-Adresse des Hosts angezeigt.
- *MAC-Adressen*: Hier werden die MAC-Adressen angezeigt.
- *Domänenmitglied*: Zeigt an, ob der Host Mitglied in der Cluster-Domäne ist.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion können die Einstellungen zu einem Host bearbeitet werden.
- *Löschen*: Mit dieser Aktion wird ein Host gelöscht.

Aktionen für dieses Formular

- *Host anlegen*: Mit dieser Aktion wird ein neuer Eintrag für einen Host erzeugt.

15.5.6.2 *Host bearbeiten*

In diesem Dialog werden die Einstellungen zu einem einzelnen Host bearbeitet.

Tab *Grundeinstellungen*, Abschnitt *Grundeinstellungen*
Felder in diesem Abschnitt

- *Name*: Hier wird der Name eines Hosts angezeigt oder eingegeben. Der Name entspricht einer kurzen Bezeichnung, um den Host zu identifizieren und wird auch in weiteren Dialogen angezeigt.
- *Kommentar*: Hier kann eine weitere Beschreibung des Hosts eingegeben werden.
- *FQDN*: Hier wird der vollständig qualifizierte Domain-Name des Hosts angegeben. Ist der Domain-Anteil Bestandteil der Cluster-Domain, wird eine entsprechender Eintrag in der Forward-Zone des lokalen DNS-Dienstes eingetragen.

  Wird der FQDN im Netzwerk nicht benutzt oder wird der FQDN im Netzwerk nicht aufgelöst, kann dieses Feld auch leergelassen werden.
- *Aliase*: Ist der Host unter weiteren Namen bekannt, können diese Aliasnamen hier eingetragen werden.
- *IP-Adressen*: Hier kann die IP-Adresse des Hosts eingetragen werden. Es können im speziellen Fall mehrere Adressen angegeben werden. Existiert ein Netzwerk mit einer Reverse-Zone und fällt eine der IP-Adressen in ein solches Netzwerk wird ein entsprechender Eintrag in der Reverse-Zone generiert.

  Sind einem Host mehrere IP-Adressen zugewiesen, und soll ein Dienst dieses Hosts benutzt werden, z. Bsp. SMTP- oder DNS-Dienst, wird die passende IP-Adresse automatisch für eine Verbindung ausgesucht.

- *MAC-Adressen*: Hier können die MAC-Adressen des Hosts eingetragen werden.

Tab *Gruppenzugehörigkeit*, Abschnitt *Gruppenzugehörigkeit*
Felder in diesem Abschnitt

- *Einstellungen*: Ein Host kann direkt als Mitglied in ausgewählte Gruppen aufgenommen werden. Damit erhält er Zugriffsrechte auf verschiedene Dienste.

Tab *Überwachung*, Abschnitt *Überwachungstests*
Felder in diesem Abschnitt

- *Einstellungen*: Für diesen Host können in diesem Abschnitt definierte Überwachungstests gewählt werden.

Aktionen für dieses Formular

- *Abbrechen*: Bearbeiten des Host abbrechen. Die Änderungen werden verworfen.
- *Speichern*: Bearbeiten des Host beenden. Die Änderungen werden gespeichert.

15.5.7 *Netzwerke*

(Dieser Dialog befindet sich unter *Cluster-Administration – Richtlinien – Netzwerke*)

15.5.7.1 *Netzwerk wählen*

In diesem Dialog können ein Netzwerk zum Bearbeiten oder Löschen ausgewählt und weitere Netzwerke anlegt werden.

Spalten in der Tabelle

- *Bezeichnung*: Hier wird die Bezeichnung des Netzwerks angezeigt.
- *Netzwerkadresse*: In diesem Feld wird die zugehörige Netzwerkadresse angezeigt.
- *Netzmaske*: Über die hier angezeigte Netzmaske ergibt sich die Größe des Netzwerkbereichs.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion können die Einstellungen für ein Netzwerk geändert werden.
- *Löschen*: Mit dieser Aktion wird das angezeigte Netzwerk gelöscht.

Aktionen für dieses Formular

- *Netzwerk anlegen*: Mit dieser Schaltfläche wird der Dialog zum Anlegen eines neuen Netzwerks geöffnet.

15.5.7.2 *Netzwerk bearbeiten*

Tab *Grundeinstellungen*, Abschnitt *Grundeinstellungen*
Felder in diesem Abschnitt

- *Bezeichnung des Netzwerks*: Hier wird die Bezeichnung für das Netzwerk angegeben. Unter diesem Namen wird das Netzwerk in verschiedenen anderen Dialogen zur Auswahl angeboten.

  Diese Bezeichnung kann nachträglich nicht mehr geändert werden.
- *Bezeichnung*: Wird ein bereits angelegtes Netzwerk bearbeitet, wird das Feld *Bezeichnung* nur angezeigt, es kann nicht geändert werden.
- *Netzwerkadresse*: In diesem Feld wird die Adresse des Netzwerks festgelegt.
- *Netzmaske*: In diesem Feld wird die zugehörige Netzmaske für das Netzwerk eingestellt. Dabei können beide Schreibweisen (*255.255.255.0* und */24*) ausgewählt werden.
- *Reverse-Zone im DNS anlegen*: Wenn dieses Häkchen gesetzt ist, wird es in diesem Netzwerk ermöglicht IP-Adressen zu Hostnamen aufzulösen. Dies wird von manchen Netzwerkdiensten benötigt, um korrekt zu funktionieren.

Tab *Gruppenzugehörigkeit*, Abschnitt *Gruppenzugehörigkeit*
Felder in diesem Abschnitt

- *Einstellungen*: Das bearbeitete Netz ist Mitglied in allen aktivierten Gruppen. Über die Gruppen werden in den *Benutzungsrichtlinien* Berechtigungen für Systeme aus den einzelnen Netzwerkbereichen vergeben.

Aktionen für dieses Formular

- *Abbrechen*: Bearbeiten der Netzwerkkonfiguration beenden. Die Änderungen werden verworfen.
- *Löschen*: Diese Aktion löscht die Netzwerkkonfiguration.
- *Speichern*: Bearbeiten der Netzwerkkonfiguration beenden. Die Änderungen werden gespeichert.

15.5.8 *Berechtigungen*

(Dieser Dialog befindet sich unter *Cluster-Administration – Richtlinien – Berechtigungen*)

Durch diesen Dialog können Berechtigungen innerhalb der Cluster-Domain gesteuert und verändert werden. Berechtigungen können Cluster Gruppen zugewiesen werden. Mit der Aktivierung der Einstellungen stehen die Berechtigungen allen Cluster-Mitgliedern (Cluster Nodes) zur Verfügung.

15.5.8.1 *Berechtigung wählen*

Die Liste zeigt alle Berechtigungen, die innerhalb der Cluster-Domain für die Nodes verwaltbar sind. Hier können Berechtigungen nur ausgewählt und editiert werden.

Felder in diesem Formular

- *Berechtigung*: Hier wird der Name der Berechtigung angezeigt.
- *Gruppen mit dieser Berechtigung*: Alle angezeigten Gruppen erhalten diese Berechtigung.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion wird die Konfiguration der ausgewählten Berechtigung bearbeitet.

15.5.8.2 *Berechtigung*

In diesem Formular wird festgelegt, für welche Gruppe die ausgewählte Berechtigung gültig ist.

Abschnitt *Bearbeiten*
Felder in diesem Abschnitt

- *ID*: Hier wird die interne ID der Berechtigung angezeigt.
- *Kommentar*: Hier ist eine kurze Beschreibung eingetragen.

Abschnitt *Gruppen*
Felder in diesem Abschnitt

- *Berechtigung für Gruppen*: Hier wird eingestellt, für welche Gruppe die Berechtigung gelten soll.

Aktionen für dieses Formular

- *Abbrechen*: Bearbeiten der Berechtigung beenden. Die Änderungen werden verworfen.
- *Speichern*: Bearbeiten der Berechtigung beenden. Die Änderungen werden übernommen.

15.5.9 GUI-Referenz: *Fencing Devices*

(Dieser Dialog befindet sich unter *Cluster-Administration – Grundeinstellungen – Fencing Devices*)

15.5.9.1 *Liste der Fencing Devices*

Spalten in dieser Tabelle

- *Name*: Hier wird der Name des Fencing Device angezeigt.
- *Kommentar*: Weitere Informationen über das Fencing Device.
- *Typ*: Zeigt die herstellerbezogene Typenbezeichnung.
- *Admin GUI*: Zeigt die URL für die Administrationsoberfläche des Fencing Device.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion kann man das Fencing Device bearbeiten.
- *Teste Erreichbarkeit*: Diese Aktion testet, ob das angegebene Fencing-Gerät unter der angegebenen IP-Adresse und der entsprechenden Zugriffsmethode (SNMP, spezieller Port, Logindaten) für den Cluster Manager erreichbar ist.
- *Löschen*: Mit dieser Aktion wird das Fencing Device aus der Liste gelöscht.

Aktionen für dieses Formular

- *Hinzufügen*: Mit dieser Aktion kann ein Fencing Device hinzugefügt werden.

15.5.9.2 Bearbeiten, Abschnitt *Steckdosenleiste*

Felder in diesem Abschnitt

- *Name*: Hier wird ein Name eingetragen oder angezeigt.
- *Kommentar*: Feld, um mehr Informationen zu hinterlegen.
- *Typ*: Es gibt verschiedene Hersteller und Varianten von Fencing Devices. Alle angezeigten Fencing Devices werden automatisch unterstützt.

  Falls der verwendete Hersteller nicht aufgeführt ist, kann als Typ Custom ausgewählt werden. Damit kann ein angepassten Steuerungsskript benutzt werden, das auf allen Cluster-Nodes nach /usr/lib/stonith/plugins/external/custom kopiert werden muss.
- *URL Admin GUI*: Für einen einfacheren Zugriff auf die Administration das Fencing Device, kann hier direkt die URL hinterlegt werden. Dieses Feld ist optional und wird für die Steuerung des Fencing Device nicht zwingend benötigt.
- *IP-Adresse*: Hier muss für die Steuerung der Host des Fencing Device hinterlegt werden. Ist der Host noch nicht in der Liste vorhanden, kann über das verlinkte Hosts-Formular in der Liste oben rechts, der entsprechende Host angelegt werden.
- *SNMP write community*: Wenn SNMP benutzt wird, ist in dieses Feld die SNMP Community für die Authentifizierung einzutragen. In den meisten Fällen kann als Community der allgemeine Standardwert „public“ eingegeben werden.
- *OID ohne Outlet-Zahl*: Für SNMP ist eine OID erforderlich, die hier eingetragen wird.
- *Port*: Hier muss der Port der Administration hinterlegt werden.
- *Login*: Benutzt das Fencing Device einen geschützten Administrationszugang, muss hier der entsprechende Login hinterlegt werden.

- *Passwort*: Hier wird das, zum Login gehörende, Passwort hinterlegt.

15.5.9.3 Bearbeiten, Abschnitt *Steckdosen*
Felder in diesem Abschnitt

- *Steckdose*: Hier wird die Kennzeichnung der Steckdose angezeigt. Dieser Wert wird automatisch erstellt. Die Anzahl der Steckdosen ist abhängig vom angegebenen Modell.
- *Verbundener Node*: Hier wird der Cluster-Node angegeben, die über diese Steckdose mit Strom versorgt wird. Diese Einstellung muss sorgfältig auf Richtigkeit überprüft werden, damit das Fencing eines nicht funktionierenden Node korrekt ausgeführt werden kann.

15.5.9.4 Aktionen für dieses Formular

- *Abbrechen*: Der Dialog wird beendet, die Änderungen werden verworfen.
- *Teste Erreichbarkeit*: Diese Aktion testet, ob das angegebene Fencing-Gerät unter der angegebenen IP-Adresse und der entsprechenden Zugriffsmethode (SNMP, spezieller Port, Logindaten) für den Cluster Manager erreichbar ist.
- *Speichern*: Der Dialog wird beendet, die Änderungen werden gespeichert.

15.5.10 *Assistent zur Einrichtung Virtueller Maschinen*

(Dieser Dialog befindet sich unter *Cluster Domain – Cluster Administration – Virtualisierungsdienste – Assistent für virtuelle Maschinen*)

Der Assistent zur Einrichtung virtueller Maschinen richtet in wenigen Schritten das Virtualisierungssystem ein und generiert eine virtuelle Maschine mit der erforderlichen Hardware-Einstellung.

15.5.10.1 Ablauf

Im Schritt Eins wird die Typeinstellung vorgenommen. Prinzipiell kann hier unterschieden werden, ob die Voreinstellungen für ein Collax System oder für andere Betriebssysteme getroffen werden sollen.

Im zweiten Schritt wird das Installationsmedium ausgewählt. Üblicherweise wird ein ISO-Image ausgewählt. Beim Typ „Collax Server“ kann ebenso eine Vorlage für einen bestimmtes Collax Produkt gewählt werden. Soll ein Klon installiert werden, muss ein schon vorhandenes Disk-Image gewählt werden.

Im Schritt Drei werden die Basiseinstellungen der VM eingegeben. Es kann ebenso entschieden werden, ob eine Bildschirmkonsole (VNC) gestartet werden soll.

Im vierten Schritt wird die virtuelle Netzwerkschnittstelle eingerichtet. Bei einer Collax Server-Vorlage kann zusätzlich die Konfiguration der IP-Adresse und der Netzwerkmaske mit angegeben werden. Ansonsten wird der Treiber und die Schnittstelle des Host-Systems gewählt, auf die sich die virtuelle Schnittstelle binden soll.

Im letzten Schritt wird die Art der Virtualisierung der zu verwendenden Festplatte konfiguriert. Ein vorhandenes Disk-Image oder ein vorhandenes logisches Volume kann verwendet werden. Alternativ

kann eine neue Festplatte mit einem der beiden Typen erzeugt werden.

15.5.10.2 Konfiguration

Beim Fertigstellen des Assistenten werden die angegebenen Hardware-Elemente der virtuellen Maschine angelegt und der Maschine zugeordnet. Zeigt der Logauszug die Meldung „Done“, kann die Maschine gestartet werden.

Wurde eine Collax Server-Vorlage gewählt, werden bei der Fertigstellung die erforderlichen Image-Daten online herunter geladen und der Server komplett installiert.

15.5.11 GUI-Referenz: *Virtuelle Festplatten*

(Dieser Dialog befindet sich unter *Cluster-Administration – Virtualisierungsdienste – Virtuelle Festplatten*

In diesem Dialog werden alle Laufwerke aufgelistet, die im Cluster für die Verwendung in virtuellen Maschinen zur Verfügung stehen. Die Laufwerke sind unterschiedlichen Typs und werden über die Einstellungen für iSCSI-Knoten und Embedded SAN(eSAN) konfiguriert.

Sollen auf den Laufwerken Collax Platform Server betrieben werden, so können diese Gastsysteme mit der Aktion *Installieren* direkt, ohne der Verwendung eines ISO-Images oder CDROMs, aufgespielt werden.

15.5.11.1 *Festplatten*

Spalten in der Tabelle

- *Typ*: Zeigt den Typ der vorhandenen Festplatte an. Im Cluster-Verbund gibt es den Typ *eSAN*, der eine eSAN-Ressource beschreibt, oder den Typ *iSCSI*, wenn es sich um eine Festplatte innerhalb eines eingebundenen iSCSI-Target handelt.
- *Name*: Zeigt den Namen der Festplatte an.
- *Kommentar*: Zeigt weitere Informationen zur Festplatte an.
- *Größe*: Zeigt die Größe der Festplatte an.
- *Status*: Zeigt den Synchronisationsstatus vom Typ eSAN an. Bei Vollständiger Synchronisation ist dieser Status 'OK'. Ein '?' bedeutet dass der Status nicht ausgelesen werden kann. Bleibt das Feld leer, so ist die Festplatte nicht vom Typ eSAN.
- *Verwendung*: Diese Spalte Zeigt an, welche virtuelle Maschine die angezeigte virtuelle Festplatte verwendet. Zusätzlich wird angezeigt, ob die Festplatte im Cluster als Cluster-Share benutzt wird, um Snapshots oder ISO-Dateien zu speichern, oder ob eine Festplatte durch eine Export-Methode im Netzwerk zur Verfügung gestellt wird.

Aktionen für dieses Formular

- *Detail*: Über diese Aktion kann die Konfiguration und der Status der ausgewählten virtuellen Festplatte vom Typ eSAN eingesehen werden.
- *eSAN-Festplatte erweitern*: In diesem Dialog kann die Größe einer virtuellen Festplatte vom Typ eSAN erweitert werden. Die Größe der Festplatte kann auch erweitert werden, wenn diese verwendet oder exportiert wird. Wird die Festplatte von einer virtuellen Maschine verwendet, muss diese VM nach der

Erweiterung heruntergefahren und gestartet werden, damit der größere Festplattenbereich erkannt wird.

- *Festplatte erweitern*: In diesem Dialog kann die Größe einer virtuellen Festplatte vom Typ Diskimage erweitert werden. Die Größe der Festplatte kann auch erweitert werden, wenn diese verwendet oder exportiert wird. Wird die Festplatte von einer virtuellen Maschine verwendet, muss diese VM nach der Erweiterung heruntergefahren und gestartet werden, damit der größere Festplattenbereich erkannt wird.
- *iSCSI-Target Export*: Diese Aktion öffnet einen Dialog, um die Festplatte im Netzwerk als iSCSI-Target zur Verfügung zu stellen. Für jede Festplatte wird automatisch ein eigenes iSCSI-Target inklusive einer LUN angelegt, gegen das optional authentifiziert werden kann.
- *iSCSI-Target löschen*: Öffnet den Dialog, um den Export über iSCSI aufzuheben.
- *Dateifreigabe*: Um die Festplatte im Netzwerk über SMB/CIFS, NFS, FTP oder AppleShare freigeben zu können, muss die Festplatte mindestens 2,5GB groß sein und der Status muss OK sein. Diese Aktion öffnet den Dialog, um eine Festplatte des Typs eSAN oder iSCSI im Netzwerk als Ordner freizugeben.
- *Cluster-Dateisystem entfernen*: Mit dieser Aktion kann auf ein gewähltes Festplattenlaufwerk das Cluster-Dateisystem (OCFS2) gelöscht werden. Dies ist sinnvoll, wenn das Festplattenlaufwerk für andere Zwecke als für das Cluster-Share eingesetzt werden soll. Nach der Aktion wird eine Aktivierung der Einstellungen automatisch ausgeführt.
- *Löschen*: Hier kann man die ausgewählte virtuelle Festplatte löschen, sofern diese von keiner virtuellen Maschine benutzt wird.

Aktionen für dieses Formular

- *Aktualisieren*: Wenn Diskimage-Dateien hochgeladen werden, zeigt die Liste der virtuellen Festplatten diese erst an, wenn die Aktion ausgeführt wurde.
- *Hinzufügen*: In diesem Dialog kann man virtuelle Festplatten vom Typ eSAN , Diskimage und iSCSI hinzufügen.

15.5.11.2 *Virtuelle Festplatte bearbeiten*

Abschnitt

Felder in diesem Abschnitt

- *Typ*: Hier kann der Typ der zu bearbeitenden virtuellen Festplatte ausgewählt werden. Ansonsten wird der Typ eSAN angezeigt.

Abschnitt *Virtuelle Festplatte*

Felder in diesem Abschnitt

- *Name*: Hier wird der Namen der virtuellen Festplatte festgelegt oder angezeigt.
- *Verfügbarer Platz*: Dieses Feld zeigt den noch freien Speicherplatz des HA-Storages der Cluster Nodes an.
- *Größe*: Hier wird die Größe der virtuellen Festplatte gesetzt. Sie muss mindestens 4 MB groß sein.
- *Konfigurierte Größe*: Hier wird die Größe der eSAN-Festplatte angezeigt.

Abschnitt *Details*

In diesem Abschnitt werden Detailinformationen über die eSAN-Festplatte angezeigt.

Abschnitt *Information*
Felder in dieser Tabelle

- *Insgesamt verfügbarer Platz*: Diese Information zeigt an, wie viel Platz auf dem Cluster-Share insgesamt zur Verfügung steht.
- *Belegt*: Diese Angabe zeigt den belegten Speicherplatz auf dem Cluster-Share an. Dazu zählen Snapshots, ISO-Dateien und vorhandene Diskimages. Diskimages werden mit ihrer maximalen Größe in den belegten Platz eingerechnet.
- *Momentan freier Platz*: Dieser Platz steht für weitere Diskimages zur Verfügung.

Abschnitt *Diskimage-Datei (neu)*
Felder in diesem Abschnitt

- *Name*: Hier wird der Name des Diskimages festgelegt.
- *Größe*: Hier wird die Größe des Diskimages festgelegt.

Abschnitt *ISCSI*

In diesem Abschnitt können iSCSI-Targets (Zielgerät) eines iSCSI-Portals importiert und deren LUNs anschließend als Festplatten verwendet werden. Der iSCSI-Initiator muss für die Verbindung zu iSCSI-Targets im Dialog *Cluster-Administration – Grundeinstellungen – Storage* aktiviert sein.

Felder in diesem Abschnitt

- *Ist HA-Target*: Falls die Targets über mehrere iSCSI-Portale verteilt sind, kann hier diese Option aktiviert werden. Für den Import im Collax Cluster ist die Anzahl der Portale auf genau zwei optimiert.
- *Portal*: Hier gibt man das Portal ein, über den iSCSI-Targets erreichbar sind. In einem Collax Cluster mit mehr als zwei Nodes kann hier ein Cluster Node gewählt werden, der entsprechende iSCSI-Targets exportiert hat.
- *Portal 2*: Hier gibt man das zweite Portal ein, über den iSCSI-Targets erreichbar sind. In einem Collax Cluster mit mehr als zwei Nodes kann hier ein Cluster Node gewählt werden, der entsprechende iSCSI-Targets exportiert hat.
- *Port*: Hier wird der Port angegeben, über welchen die Verbindung zum iSCSI-Portal aufgebaut wird.
- *Discovery-Authentifizierung*: Für die Prüfung (Discovery) kann eine Authentifizierung erforderlich sein.
- *Benutzer*: Hier wird der Benutzername für die Authentifizierung während der Prüfung (Discovery) eingetragen.
- *Passwort*: Hier wird das Passwort für die Authentifizierung eingetragen.

Aktionen für diesen Abschnitt

- *Prüfen*: Hier wird geprüft, welche iSCSI-Targets auf dem Portal verfügbar sind.

Abschnitt *Ergebnis*
Felder in diesem Abschnitt

- *Neue iSCSI Targets*: Hier werden die auf dem Portal liegenden iSCSI-Targets gelistet. Falls keine Targets verfügbar sind, erscheint ein Hinweis

Aktionen für dieses Formular

- *Zurück*: Führt zurück zur Übersicht.
- *Abbrechen*: Der Dialog wird beendet, die Änderungen werden verworfen.
- *Importieren*: Mit dieser Aktion werden die gewählten iSCSI-Targets und deren LUNs als Festplatten importiert. Es erfolgt direkt eine Aktivierung der Konfiguration.
- *Speichern*: Der Dialog wird beendet, die Änderungen werden gespeichert.

15.5.11.3 *iSCSI Target bearbeiten*

Abschnitt
Felder in diesem Abschnitt

- :

Tab *Grundeinstellungen*
Felder in diesem Abschnitt

- *Name*: Hier steht der iSCSI-Targetname. Der IQN wird automatisch gesetzt.
- *Beschreibung*: Hier kann man eine Beschreibung für das iSCSI-Target verfassen.

Tab *Grundeinstellungen*, Abschnitt *Authentifizierung*
Felder in diesem Abschnitt

- *Authentifizierung*: Hier die Authentifizierung für dieses Target einstellen.
- *Benutzer*: Benutzer für die Authentifizierung an diesem Target.
- *Passwort*: Passwort für die Authentifizierung an diesem Target.
- *IQNs*: Hier können die iSCSI-Initiator (Controller) angegeben werden, die sich mit diesem iSCSI-Target verbinden dürfen. Hier sind die IQNs der Collax Nodes voreingestellt.

Aktionen für diesen Abschnitt

- *ACLs zurücksetzen*: Setzt die IQNs auf die Voreinstellung zurück.

Aktionen für dieses Formular

- *Abbrechen*: Beendet den Dialog, die Änderungen werden verworfen.
- *Löschen*: Diese Aktion beendet den iSCSI Target-Export.
- *Speichern*: Beendet den Dialog, die Einstellungen werden gespeichert.

15.5.11.4 *iSCSI-Festplatte bearbeiten*

Tab *Grundeinstellungen*, Abschnitt *iSCSI-Knoten*
Felder in diesem Abschnitt

- *Name*: Hier steht der Name des iSCSI-Targets.
- *Info*: Hier kann man eine kurze Info für den iSCSI-Knoten eintragen.

Tab *Grundeinstellungen*, Abschnitt *Portal*
Felder in diesem Abschnitt

- *Ist HA-Target*: Falls die Targets über mehrere iSCSI-Portale verteilt sind, kann hier diese Option aktiviert werden. Für den Import im Collax Cluster ist die Anzahl der Portale auf genau zwei optimiert.
- *Portal*: Hier gibt man das Portal ein, über den iSCSI-Targets erreichbar sind. In einem Collax Cluster mit mehr als zwei Nodes kann hier ein Cluster Node gewählt werden, der entsprechende iSCSI-Targets exportiert hat.
- *Portal 2*: Hier gibt man das zweite Portal ein, über den iSCSI-Targets erreichbar sind. In einem Collax Cluster mit mehr als zwei Nodes kann hier ein Cluster Node gewählt werden, der entsprechende iSCSI-Targets exportiert hat.
- *Port*: Hier wird der Port angegeben, über welchen die Verbindung zum iSCSI-Portal aufgebaut wird.

Tab *Grundeinstellungen*, Abschnitt *Authentifizierung*
Felder in diesem Abschnitt

- *iSCSI Initiator gegenüber iSCSI Target*: Hier wird festgelegt, ob sich der iSCSI-Initiator gegenüber dem iSCSI-Target authentifizieren soll.

- *Benutzer*: Benutzernamen für die Authentifizierung am iSCSI-Target.
- *Passwort*: Passwort für die Authentifizierung am iSCSI-Target.
- *iSCSI Target gegenüber iSCSI Initiator*: Hier wird eingestellt, ob sich das iSCSI-Target gegenüber diesem iSCSI-Initiator authentifizieren soll.
- *Benutzer*: Benutzernamen für die Authentifizierung an diesem iSCSI-Initiator.
- *Passwort*: Passwort für die Authentifizierung an diesem iSCSI-Initiator.

Aktionen für dieses Formular

- *Abbrechen*: Beendet den Dialog, die Einstellungen werden verworfen.
- *Speichern*: Beendet den Dialog, die Einstellungen werden gespeichert.

15.5.11.5 *eSAN-Festplatte erweitern*

Abschnitt *Erweitern*

Felder in diesem Abschnitt

- *Name*: Hier steht der Name der zu bearbeitenden virtuellen Festplatte.
- *Aktuelle Größe*: Dieses Feld zeigt die aktuell konfigurierte Größe der virtuellen Festplatte an.
- *Verfügbarer Speicherplatz*: Um den hier angezeigten Speicherplatz kann die Festplatte maximal erweitert werden.
- *Erweitern um*: Hier wird festgelegt, um wie viel die virtuelle Festplatte vergrößert werden soll.

Aktionen für dieses Formular

- *Erweitern*: Mit dieser Aktion wird die Erweiterung der virtuellen Festplatte ausgeführt. Anschließend muss die Einstellung aktiviert werden.
- *Abbrechen*: Beendet den Dialog, die Einstellungen werden verworfen.

Abschnitt
Felder in diesem Abschnitt

- *Name*: Hier sieht man den Namen der eSAN-Festplatte.

Abschnitt *Hinweis*
Felder in diesem Abschnitt

- : Zeigt einen Hinweis, falls die Festplatte nicht erweitert werden kann.

15.5.11.6 *Erweitern*
Abschnitt *Erweitern*
Felder in diesem Abschnitt

- *Name*: Hier steht der Name der zu bearbeitenden virtuellen Festplatte.
- *Info*: Hier steht der Gerätename der virtuellen Festplatte im System.
- *Aktuelle Größe*: Dieses Feld zeigt die aktuell konfigurierte Größe der virtuellen Festplatte an.
- *Verfügbarer Speicherplatz*: Um den hier angezeigten Speicherplatz kann die Festplatte maximal erweitert werden.

- *Erweitern um*: Hier wird festgelegt, um wie viel die virtuelle Festplatte vergrößert werden soll.

Aktionen für dieses Formular

- *Erweitern*: Mit dieser Aktion wird die Erweiterung der virtuellen Festplatte ausgeführt. Anschließend muss die Einstellung aktiviert werden.
- *Abbrechen*: Beendet den Dialog, die Einstellungen werden verworfen.

15.5.11.7 GUI-Referenz: *Diskimage-Datei löschen*

Abschnitt *Hinweis*

Felder in diesem Abschnitt

- : Zeigt den entsprechenden Hinweis.

Abschnitt *Details*

Felder in diesem Abschnitt

- *Name*: Zeigt den Namen des Diskimages.
- *Pfad*: Zeigt den Pfad zum Diskimage.
- *Format*: Zeigt das Format des Diskimages.
- *Dateigröße*: Zeigt die tatsächliche Größe des Diskimages.
- *Größe*: Zeigt die konfigurierte Größe des Diskimages.

Aktionen für dieses Formular

- *Abbrechen*: Mit diesem Button kann die aktuelle Aktion abgebrochen werden.

- *Löschen*: Mit diesem Button wird das Diskimage endgültig gelöscht.

15.5.11.8 *Cluster-Dateisystem entfernen*

Abschnitt *Einstellungen*
Felder in diesem Abschnitt

- *Name*: Zeigt den Namen der virtuellen Disk.
- *Kommentar*: Zeigt weitere Informationen.

Abschnitt *Hinweis*
Felder in diesem Abschnitt

- : Zeigt einen entsprechenden Hinweis.

Abschnitt *Fortschritt*
Felder in diesem Abschnitt

- *Ausgabe*: Zeigt die detaillierte Ausgabe der Aktion.

Aktionen für dieses Formular

- *Entfernen*: Diese Aktion entfernt das OCFS-Dateisystem.
- *Zurück*: Führt zurück zur Übersicht.

15.5.11.9 GUI-Referenz: *Dateisystem exportieren*

Tab *Export*, Abschnitt *Export*
Felder in diesem Abschnitt

- *Export-Name*: Hier muss der Export-Name eingetragen werden.
- *Disk-Name*: Hier steht der Disk-Name.
- *Exportiere über*: Hier kann ausgewählt werden über was exportiert werden soll.

Tab *Berechtigungen*
Felder in diesem Abschnitt

- *Leseberechtigung für*: Hier kann man auswählen wer zum Lesen berechtigt ist.
- *Schreibberechtigung für*: Hier kann man auswählen wer zum Schreiben berechtigt ist.

Aktionen für dieses Formular

- *Speichern*: Auf der oben gewählten Festplatte wird währen der Aktivierung ein Cluster-Dateisystem angelegt. *Alle Daten auf der Festplatte gehen dadurch verloren.* Beendet den Dialog, die Änderungen werden gespeichert.
- *Zurück*: Beendet den Dialog. Die Einstellungen werden verworfen.

15.5.12 ISO-Dateien hochladen

Wenn für die Installation von virtuellen Maschinen ein ISO-Installationsmedium benötigt wird, können diese ISO-Dateien vorweg hochgeladen werden. Alternativ können die ISO-Dateien auch während dem Erzeugen einer virtuellen Maschine hochgeladen werden.

- Um vorher ISO-Dateien hochzuladen, geben Sie in der Suche „ISO“ ein, drücken Sie Enter und klicken Sie anschließend auf das angezeigte Suchergebnis.
- Klicken Sie auf *Hinzufügen* und geben Sie über den Knopf „Browse“ eine ISO-Datei, die auf Ihrer Arbeitstation abgelegt ist, an.
- Durch die Betätigung der Aktion *Hochladen* wird die Datei in den Cluster übertragen. Der Fortschritt wird über die Job-Notification angezeigt. Während des Hochladens sind keine weiteren Aktionen möglich. Der erfolgreiche Abschluss wird mit der Anzeige *hochgeladenes ISO* angezeigt.
- Schließen Sie den Dialog mit ESC.

15.6 Virtuelle Maschinen

Dieser Dialog dient dazu, die virtuellen Maschinen im Cluster zu verwalten. Es werden Maschinen angezeigt und verwaltet, die im Collax Cluster ausfallsicher betrieben werden.

15.6.1 Verwandte Themen

- VM migrieren (S. 449)
- GUI Referenz (S. 444)

15.6.2 GUI-Referenz: *Virtuelle Maschinen*

(Dieser Dialog befindet sich unter *Cluster-Administration – Virtualisierungsdienste – Virtuelle Maschinen*)

15.6.2.1 *Virtuelle Maschine wählen*

Abschnitt *VT-Hardware*

Felder in diesem Abschnitt

- : Voraussetzung für die Benutzung der Virtualisierung ist Hardware mit Unterstützung von Intel VT oder AMD-V. Falls die Hardware nicht virtualisierungsfähig ist, wird hier ein entsprechender Hinweis angezeigt.

Abschnitt *Virtualisierungsdienst*

Felder in diesem Abschnitt

- : Der Virtualisierungsdienst wurde gestoppt oder steht aus unbekanntem Grund nicht zur Verfügung. Falls der Virtualisierungsdienst nicht verfügbar ist, wird hier ein entsprechender Hinweis angezeigt.

XXX missing title found
Spalten in der Tabelle

- *Name*: Zeigt den Namen der virtuellen Maschine.
- *Kommentar*: Weitere Informationen zur VM können hier eingegeben werden.
- *Ort*: Zeigt den Node an, auf dem die virtuelle Maschine betrieben wird.
- *Hochverfügbar*: Zeigt an, ob die virtuelle Maschine im Cluster-Verbund ausfallsicher betrieben wird oder lokal auf einer bestimmten Cluster Node gestartet ist.

  Ja – zeigt an, dass die virtuelle Maschine auf einer bestimmten Cluster Node ausfallsicher gestartet werden kann, oder betrieben wird, und dass diese virtuelle Maschine beim Ausfall dieses Nodes automatisch auf einem anderen Cluster Node gestartet wird.

  Ja/Bevorzugt – zeigt an, dass die virtuelle Maschine auf einer bestimmten Cluster Node bevorzugt betrieben werden soll oder betrieben wird. Auch wenn die virtuelle Maschine ausgeschaltet und wieder eingeschaltet wird, startet diese wenn möglich auf der in der Spalte *Präferierter Node* angegebenen Cluster Node.

  Ja/Sticky – zeigt an, dass die virtuelle Maschine auf einen bestimmten Cluster Node umgezogen wurde. In diesem Fall bleibt die virtuelle Maschine auf den angegebenen Cluster Node gebunden und wird bei Ausfall *nicht* automatisch auf einem anderen Cluster Node gestartet. Auch wenn die virtuelle Maschine ausgeschaltet und wieder eingeschaltet wird, startet diese nur auf dem Cluster Node auf den umgezogen wurde.

  Nein/lokal – besagt, dass die virtuelle Maschine nur auf einer bestimmten Cluster Node lokal betrieben wird. Solche Maschinen sind keine Ressourcen der bestehenden Cluster Domain, also

nicht ausfallsicher, und können auch nicht umgezogen werden, weder automatisch noch manuell. Alle weiteren Aktionen sind in diesem Formular anwendbar.

- *Bevorzugter Node*: Zeigt den Node an, auf dem die VM bevorzugt gestartet oder betrieben wird.
- *Status*: Der Status einer virtuellen Maschine kann *An* , *Ruhezustand* oder *Aus* sein.

  An bedeutet, dass die virtuelle Maschine gestartet ist, oder dass vom Ruhezustand in den gestarteten Zustand gewechselt wurde.

  Wurde die virtuelle Maschine angehalten , so befindet sie sich im *Ruhezustand*. In diesem Zustand werden laufende Daten im Speicher gehalten, damit der aktive Betrieb sehr schnell fortgesetzt werden kann. Diese laufenden Daten gehen verloren, wenn das Host-System neu gestartet wird. Passiert dies, ist danach der Status der virtuellen Maschine *Aus*

  Wird die virtuelle Maschine heruntergefahren oder ausgeschaltet, wird ebenso der Status *Aus* eingenommen.
- *CPUs*: Zeigt die Anzahl der zugeteilten CPUs.
- *RAM*: Zeigt die Menge des zugeteilten virtuellen Arbeitsspeichers.
- *Snapshots*: Zeigt die Anzahl der Snapshots der virtuellen Maschine.
- *Bildschirm*: Ist die virtuelle Maschine gestartet, wird in diesem Feld ein Link angezeigt, der nach dem anklicken die Bildschirmkonsole der entsprechenden virtuellen Maschine öffnet. Dazu wird ein neuer Browser-Reiter oder ein neues Fenster geöffnet.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Öffnet den Dialog zur Bearbeitung der Einstellungen der virtuellen Maschine.

- *Einschalten*: Ist die virtuelle Maschine ausgeschaltet, kann sie mit dieser Aktion angeschaltet werden. Die Maschine bootet daraufhin vom angegebenen Boot-Laufwerk.
- *Storage Migration*: Öffnet den Dialog, um den Festplatteninhalt der virtuellen Maschine auf andere Festplatten zu kopieren. Die Aktion ist nur möglich, wenn die VM ausgeschaltet ist.
- *Reset*: Mit dieser Aktion wird die virtuelle Maschine sofort kalt gestartet.
- *Reboot*: Mit dieser Aktion wird die virtuelle Maschine heruntergefahren und neu gestartet.
- *Herunterfahren*: Diese Aktion sorgt dafür, dass die virtuelle Maschine über das darauf laufende Betriebssystem per ACPI heruntergefahren wird. Hierbei gehen keine Daten verloren, da Prozesse auf der virtuellen Maschine korrekt beendet werden. Im Arbeitsspeicher befindliche Daten werden entsprechend auf die Festplatten geschrieben. Das Gastbetriebssystem muss hierzu ACPI-Aktionen verarbeiten können.
- *Ausschalten*: Lässt sich eine virtuelle Maschine nicht korrekt herunterfahren, kann sie mit dieser Aktion einfach ausgeschaltet werden. Dabei können im virtuellen Arbeitsspeicher befindliche Daten verloren gehen.
- *Pausieren*: Mit dieser Aktion wird die virtuelle Maschine in einen Zustand versetzt, in dem sie wenige Ressourcen in Anspruch nimmt. Daten im zugewiesenen Arbeitsspeicher werden nicht auf Festplatte gespeichert. Die Informationen über die Sitzung gehen durch das Herunterfahren des Virtualisierungs-Host verloren. Die virtuelle Maschine kann nach *Suspend (RAM)* durch die Aktion *Aufwecken*
  wieder gestartet werden.
- *Aufwecken*: Befindet sich die virtuelle Maschine im Ruhezustand kann mit dieser Aktion der aktive Betrieb wieder aufgenommen werden.

- *Snapshots*: Diese Aktion öffnet den Dialog, um Snapshots der VM zu verwalten.
- *ISOs*: Mit dieser Aktion können die verwendeten CD-/DVD-Laufwerke bestückt werden.
- *Migration*: Durch diese Aktion kann die virtuelle Maschine im laufenden Betrieb auf einen im Cluster-Verbund verfügbaren Node migriert werden. Die gewählte VM wird dann auf dem angegebenen Node bevorzugt betrieben oder gestartet, solange dieser bevorzugte Node eingestellt ist.
- *Löschen*: Mit dieser Aktion werden die Einstellungen der virtuellen Maschine gelöscht. Nach der Aktivierung im Cluster wird die Maschine von allen Cluster-Nodes entfernt.

Logausgabe
Felder in diesem Abschnitt

- *Ausgabe*: Hier wird die Logausgabe nach einer Aktion angezeigt.

Aktionen für dieses Formular

- *Neue VM anlegen*: Diese Aktion öffnet den Dialog zum Anlegen einer weiteren virtuellen Maschine.
- *Aktualisieren*: Hier kann die Ansicht des Formulars aktualisiert werden.
- *Zurück*: Führt zurück zur Tabelle der virtuellen Maschinen.

15.6.2.2 *Virtuelle Maschine*

Abschnitt *CD-/DVD-ROM Medien*
Felder in diesem Abschnitt

- *Information*: In dieser Liste werden alle DVD-Laufwerke angezeigt. Das Laufwerk kann leer sein, alternativ wird der Name der ISO-Datei gezeigt.
- *Eingelegtes ISO*: Die hier gewählte ISO-Datei kann ausgeworfen werden.
- *Verfügbare ISOs*: Eine hier gewählte ISO-Datei kann in einen leeren Laufwerksschacht eingelegt werden. Eine ISO-Datei kann nur einmal eingelegt werden.

Aktionen für diesen Abschnitt

- *ISO einlegen*: Eine verfübare ISO-Datei wird mit dieser Aktion in einen leeres Laufwerk eingelegt.
- *ISO Auswerfen*: Eine unter *Eingelegtes ISO* gewählte Datei wird aus dem entsprechenden Laufwerk entfernt.
- *Treiber-ISO einlegen*: Für die Installation von Paravirtualisierungstreibern für Windows-Betriebssysteme ist diese ISO-Datei erforderlich. Diese Aktion legt die virtuelle CD in das nächste leere Laufwerk, oder direkt in das erste Laufwerk. Eine andere ISO-Datei wird dabei ausgworfen.

15.6.2.3 *Virtuelle Maschine migrieren*

Um eine optimale Auslastung der Cluster Nodes zu erreichen, ist es unter Umständen sinnvoll eine virtuelle Maschine auf einen anderen Cluster Node zu migrieren. Falls eine virtuelle Maschine noch nicht gestartet ist, kann eine Einstellung zur Migration vorge-

nommen werden. Diese hat zur Folge, dass die VM bei Start auf dem angegebenen Node bootet, und dass diese VM nach einer Wartung automatisch auf diesen Node migriert wird.

- Schritt für Schritt (S. 450)
- Gui-Referenz (S. 450)

Schritt für Schritt

- Wählen Sie die virtuelle Maschine aus, die migriert werden soll
- Wählen Sie per rechtem Mausklick die Aktion Migration.
- *Bevorzugter Node* Wählen Sie nachfolgend einen Node aus, auf dem die virtuelle Maschine gestartet, oder auf den die virtuelle Maschine migriert werden soll.
- Im Feld *Beschreibung* wird angezeigt, wie die Aktion auf die virtuelle Maschine angewandt wird.
- Durch die Aktion *Ausführen* wird die Migration, oder die Beschriebene Aktion ausgeführt.

Felder in diesem Abschnitt

- *Virtuelle Maschine*: Name der virtuellen Maschine.
- *Gestartet auf*: Zeigt den Node, auf dem die virtuelle Maschine in Betrieb ist.
- *Bevorzugter Node*: Zeigt eine Liste der Nodes, auf die die laufende VM umgezogen bevorzugt betrieben werden kann. Ist die VM aus, wird hier der Node gewählt, auf dem die VM zukünftig gestartet wird.

  Ist der momentane Ort nicht identisch mit der Node, auf den umgezogen(migriert) werden soll, findet eine Live Migration statt. Der bevorzugte Betrieb auf einem Node hat den Vorteil, dass die VM bei Ausfall des Nodes auf einem anderen Node im Cluster

automatisch gestartet wird, UND dass die VM automatisch zum bevorzugten Node zurückkehrt (durch Live Migration), sobald dieser wieder im Cluster zur Verfügung steht. Wird ein bevorzugter Node gesetzt während die VM noch ausgeschaltet ist, wird diese VM beim Start auf dem angegebenen Node gestartet.
- *Fortschritt*: Dieses Feld zeigt den detaillierten Ablauf einer Live Migration.

Aktionen für dieses Formular

- *Ausführen*: Die VM wird je nach Einstellung auf den angegebenen Node live migriert oder die VM wird zukünftig auf dem angegebenen Node gestartet.

15.6.2.4 *Snapshots*

In diesem Dialog werden Snapshots der gewählten VM verwaltet.

Abschnitt *Disk Info*
Felder in diesem Abschnitt

- : Zeigt Informationen über den aktuellen Speicherplatz für Snapshots.

Abschnitt *Aktueller Zustand*
Felder in diesem Abschnitt

- *Virtuelle Maschine*: Zeigt den Namen der gewählten VM.
- *Ort*: Wenn die VM in Betrieb ist, wird der Node gelistet, auf dem die VM läuft.
- *Status*: Zeigt den Betriebsstatus der VM an.

- *Momentanes Disk Delta*: Zeigt den Größenunterschied zum letzten Snapshot.
- *Maximale Snapshotgröße*: Zeigt den maximal verfügbaren Speicherplatz für einen neuen Snapshot an.

Abschnitt *Hinweis*
Felder in diesem Abschnitt

- : Zeigt einen Hinweis, falls der maximal verfügbare Speicherplatz für einen neuen Snapshot nicht ausreicht.

Abschnitt *Snapshot Aktionen*
Felder in diesem Abschnitt

- *Aktion*: Hier können Aktionen zum Erstellen, Zusammenführen, Löschen und Wiederherstellen von Snapshots ausgewählt werden. Das *Erstellen* eines Snapshots unterscheidet zwischen Online- und Offline-Snapshot. Ein Online-Snapshot speichert, neben dem Erstellen einer abgezweigten Snapshot-Disk, den aktuellen Speicherzustand der Maschine im laufenden Betrieb. Durch das *Zusammenführen* werden alle Snapshots bis zum dem gewählten Zeitpunkt vereinigt, die virtuelle Maschine behält ihren aktuellen Zustand. Anders verhält es sich bei den Aktionen *Wiederherstellen* oder *Löschen*. Hier werden Zustände jüngerer als des gewählten Snapshots nicht erhalten, sondern gelöscht.
- *Live*: Beim Erstellen oder beim Zusammenführen wird die VM nicht mehr angehalten, sondern der Vorgang wird während des Betriebs unmerklich für Anwender durchgeführt.
- *Kommentar*: Für jeden Snapshot kann eine kurze Information hinterlegt werden.
- *Snapshot*: Hier wird die Liste der Snapshots angezeigt.

Aktionen für diesen Abschnitt

- *Ausführen*: Führt die gewählte Aktion aus.

Abschnitt *Bestätigen*
Felder in diesem Abschnitt

- : Soll ein Snapshot erzeugt, gelöscht oder zusammengeführt werden, wird hier eine entsprechende Bestätigung erforderlich.

Abschnitt *Verfügbare Snapshots*
Felder in diesem Abschnitt

- : Hier werden die verfügbaren Snapshots mit weiteren Details aufgelistet.

Aktionen für dieses Formular

- *Herunterfahren*: Hier kann die VM heruntergefahren werden, falls ein Offline-Snapshot erzeugt werden soll, die VM aber noch in Betrieb ist.
- *Ausschalten*: Hier kann die VM einfach ausgeschaltet werden.
- *Einschalten*: Hier kann die VM gestartet werden, falls ein Online-Snapshot erzeugt werden soll, die VM aber nicht in Betrieb ist.

15.6.2.5 *Virtuelle Maschine bearbeiten*
Abschnitt *Hinweis*
Felder in diesem Abschnitt

- : Dieser Abschnitt zeigt entsprechende Hinweise, wenn Veränderungen an der virtuellen Maschine vorgenommen werden.

Abschnitt *Virtuelle Maschine*
Felder in diesem Abschnitt

- *Name*: Hier wird der Name eingegeben oder angezeigt.
- *Kommentar*: Hier werden weitere Informationen hinterlegt.
- *Prozess-Priorisierung*: Hier wird die aktuelle Prioritätsstufe der virtuellen Maschine angezeigt. In der Auswahlliste kann bei Bedarf eine andere Priorität eingestellt werden.

Abschnitt *CPU/RAM*
Felder in diesem Abschnitt

- *Anzahl virtueller CPUs*: Die Anzahl der CPUs berechnet sich aus der Anzahl der Sockel und der Kerne. Maximal können einer VM 64 CPUs zugewiesen werden. Um eine 100% Auslastung des Host-Systems zu vermeiden, sollten den virtuellen Gästen insgesamt nicht mehr CPUs zugewiesen werden, als auf dem Host-System vorhanden sind.
- *Arbeitsspeicher*: Hier wird der Hauptspeicher für den virtuellen Gast zugewiesen. Die Anzahl kann in verschiedenen Einheiten eingegeben werden.
- *Verfügbarer RAM*: Für die virtuelle Maschine kann der hier angezeigte RAM maximal vergeben werden.
- *Hinweis*: Zeigt an, falls mehr virtuelle CPUs verwendet werden, als physikalisch vorhanden sind.

Abschnitt *Laufwerke*
Felder in diesem Abschnitt

- *Typ*: Üblicherweise wird hier der IDE-Controller verwendet. Der Disk-Typ „virtio“ bietet die volle Unterstützung des Kernel-Hypervisors für I/O-Virtualisierung. Innerhalb des Betriebssystems der VM müssen zur Unterstützung der Paravirtualisierung die „virtio“-Treiber installiert werden. Für Windows™-Betriebssysteme kann dazu die Option *Virtio-Treiber-Diskette* benutzt werden.
- *Laufwerk 1 bis 4*: Hier wird angegeben, welche Laufwerke von der virtuellen Maschine benutzt werden sollen. Jede virtuelle Maschine kann bis zu vier Laufwerke erhalten.

  Bei Auswahl von CDROM kann der virtuellen Maschine vor dem Starten im Dialog Detail ein CD-/DVD-ISO eingelegt werden.
- *Virtio Treiber Disk*: Hier kann der VM eine Diskette zugewiesen werden, auf der Virtio-Treiber für Festplatten von Windows Betriebssystemen vorhanden sind. Diese Option eignet sich für Neuinstallationen von Windows VMs, die paravirtualisierte Festplattentreiber nicht per CD-ROM-Laufwerk laden können.

Abschnitt *Netzwerkschnittstellen*
Felder in diesem Abschnitt

- *Typ*: Hier kann gewählt werden, welcher Netzwerk-Treiber auf den angegebenen Netzwerkschnittstellen emuliert werden soll. Falls das zu installierende Betriebssystem den paravirtualisierten Controller-Treiber ansteuern kann, ist es zu empfehlen als Controller *virtio* zu verwenden. Für die Installation innerhalb von Windows™-Betriebssystemen kann dazu die Option *Virtio-Treiber-Diskette* benutzt werden.
- *MAC-Adressen editieren*: Durch diese Option werden die MAC-

Adressen für die virtuellen Netzwerkschnittstellen sichtbar, die dann bearbeitet werden können.

- *NIC verbinden mit virtuellem Netzwerk-Switch*: Hier werden die Netzwerkschnittstellen mit einem angelegten Netzwerk-Switch verbunden. Die Netzwerkschnittstelle wird beim Verbinden mit dem virtuellen Switch automatisch erzeugt. Es können maximal acht NICs verbunden werden. Im System erhalten die NICs die Bezeichnung „cvm“, an welche die jeweilige Schnittstellennummer angehängt wird. Ist die Auswahl leer, wird keine Schnittstelle für die virtuelle Maschine erzeugt und auch nicht mit einem Netzwerk-Switch verbunden.

  Wenn mehrere virtuellen Switches verwendet werden, ist auf jeder einzelnen Node extra sorge zu tragen, dass die Netzwerkverbindung der virtuellen Maschinen funktioniert. Dies kann im Menü *Hardware – Netzwerkschnittstellen* vorgenommen werden.
- *MAC-Adresse für NIC*: Standardmäßig ist das Feld ausgeblendet. Hier können bei Bedarf spezielle MAC-Adressen für die virtuelle NIC eingetragen werden. Das Feld ist beim ersten Aufruf leer. Wird keine spezielle MAC-Adresse eingetragen, wird automatisch eine MAC-Adresse erzeugt.

Abschnitt *Bildschirm*
Felder in diesem Abschnitt

- *Aktiviere VNC- und RDP-Konsole*: Für den Fernzugriff auf die virtuelle Maschine ist hier die VNC-Konsole zu aktivieren.
- *Konsolen-Passwort*: Soll der Fernzugriff geschützt werden, muss hier ein Passwort eingegeben werden. Soll das Passwort geändert werden, muss anschließend die virtuelle Maschine herunter und wieder hochgefahren werden.
- *VNC-Tastaturbelegung*: Um den korrekten Einsatz einer Tastatur

per VNC zu ermöglichen, kann hier das entsprechende Ländertastatur-Layout eingestellt werden.
- *VGA*: Hier kann die emulierte Grafikkarte für die VM eingestellt werden.
- *VNC- und RDP-Zugriff für ...*: Für die Netzwerke und die Hosts der gewählten Gruppen ist der Zugriff per VNC oder RDP möglich.

15.6.2.6 Erweiterte Einstellungen
Abschnitt *Hardware*
Felder in diesem Abschnitt

- *Anzahl der CPU Sockel*: Gibt die Anzahl der CPU-Sockel für eine VM an. Diese Einstellung ist wichtig, falls das Betriebssystem der VM nur eine begrenzte Anzahl von CPU-Sockel berücksichtigt.
- *Anzahl der CPU Kerne*: Gibt die Anzahl der CPU-Kerne pro CPU-Sockel an. Dieser Wert wird automatisch aus der Anzahl der virtuellen CPUs und der Anzahl der eingestellten Sockel berechnet.
- *Boot-Reihenfolge*: Sind einem Gast-System mehrere Laufwerke oder Netzwerkschnittstellen zugewiesen, kann hier eingestellt werden, in welcher Reihenfolge die virtuelle Maschine starten soll.
- *HDD-Caching*: Mit dieser Option kann der Caching-Modus der virtuellen Festplatten spezifiziert werden. Die korrekte Einstellung des Modus richtet sich dann nach dem Dateisystem der VM und dieser hat Einfluss darauf, ob bei einem Absturz oder direktem Ausschalten der VM Daten verloren gehen. Für moderne Dateisysteme und Collax Server ab Version 5.5.0 kann der Modus *Performance* eingestellt werden. Ansonsten soll die Einstellung *Datensicherheit* gewählt werden.
- *RTC Zeit*: Diese Einstellung hat Einfluss auf die Richtigkeit der

Uhrzeit des Betriebsystems der virtuellen Maschine. Für Linux-basierende Systeme soll UTC, für Windows-Systeme lokale Zeit eingestellt werden.

- *BIOS*: Hier soll die neuste BIOS-Version für das Starten der VM eingestellt sein. Falls Windows-VMs mit älteren Paravirtualisierungstreibern (Virtio) betrieben werden, sollte ebenso eine ältere BIOS-Version gewählt werden.

Abschnitt *Cluster*
Felder in diesem Abschnitt

- *Live migrieren*: Wenn diese Option gesetzt ist, wird die virtuelle Maschine live migriert. Während einer Live Migration ist die VM weiterhin verfügbar. Ist diese Option nicht gesetzt, wird die VM für die Dauer der Migration nicht verfügbar sein.
- *Verhalten beim Stopp der Ressource*: Hier wird festgelegt, wie sich die virtuelle Maschine verhalten soll, wenn diese als Ressource gestoppt wird. Je nach Betriebssystem kann hier zwischen *Herunterfahren/shutdown* oder hartem *Ausschalten/shutoff* gewählt werden.
- *Maximale Zeit für Shutdown*: Mit diesem Wert wird festgelegt, wie lange eine virtuelle Maschine maximal benötigt, um ordnungsgemäß herunterzufahren. Nach dieser Zeit wird die virtuelle Maschine durch den Cluster Manager automatisch ausgeschaltet, auch wenn die Maschine nicht ordentlich herunterfahren konnte. Je nach Betriebssystem sind hier über 15 Minuten erforderlich.

Aktionen für dieses Formular

- *Abbrechen*: Bearbeiten der VM abbrechen. Die Änderungen werden verworfen.

- *Speichern*: Bearbeiten der VM beenden. Die Änderungen werden gespeichert.

15.6.2.7 *VM löschen*

Dieser Dialog behandelt das Entfernen einer VM.

Abschnitt *Hinweis*
Felder in diesem Abschnitt

- : Zeigt einen Hinweis, falls die virtuelle Maschine noch in Betrieb ist. Um eine VM zu entfernen muss diese ausgeschaltet sein.
- *Name*: Dieses Feld zeigt den Namen der VM.

Aktionen für diesen Abschnitt

- *Ausschalten*: Ermöglicht das Ausschalten der VM.

Abschnitt *Hinweis*
Felder in diesem Abschnitt

- : Falls von der virtuellen Maschine Snapshots erstellt wurden, müssen bestimmte Dinge beachtet werden, bevor die VM gelöscht werden kann.

Abschnitt *Snapshots*
Felder in diesem Abschnitt

- : Zeigt bestehende Snapshots der VM an.

Abschnitt *Optionen*
Felder in diesem Abschnitt

- *Name*: Zeigt den Namen der VM an.
- *In Festplatte(n) ... erhalten*: Auswahl, welcher Zustand in die übrigbleibende Festplatte übertragen werden soll, falls die Konfiguration der VM gelöscht soll.

Abschnitt *Ausgabe*
Felder in diesem Abschnitt

- *Ausgabe*: Zeigt Details über die durchgeführte Aktion.

Aktionen für dieses Formular

- *VM und Snapshots entfernen*: Die Konfiguration der VM wird gelöscht, die Snapshots werden mit dem gewählten Zustand in die verbleibende Festplatte geschrieben und danach ebenso gelöscht.
- *Abbrechen*: Der Vorgang wird abgebochen und führt zurück zur Übersicht.
- *Zurück*: Führt zurück zur Übersicht.

15.6.2.8 *Storage Migration*

Durch die Storage Migration können einerseits virtuelle Maschinen und deren Inhalt in die Verwaltung eines einzelnen Cluster Node verschoben werden. Zum anderen ist es möglich nur die Festplatten einer virtuellen Maschine auf weitere vorhandene Festplatten im Cluster zu migrieren. So können beispielsweise iSCSI-Festplatten auf hochverfügbare eSAN-Festplatten umgezogen werden.

Abschnitt
Felder in diesem Abschnitt

- *Virtuelle Maschine*: Zeigt den Namen der virtuellen Maschine.
- *Aktion*: Durch die Auswahl wird gesteuert, ob die gesamte virtuelle Maschine mit Festplatten auf einen V-Cube migriert werden soll, oder ob ausschließlich die Festplatten innerhalb des Clusters migriert werden sollen (z.B. von iSCSI zu eSAN).

Abschnitt *Festplatte*
Felder in diesem Abschnitt

- *Inhalt von ...*: Zeigt den Namen der Festplatten, die migriert werden soll.
- *Umziehen auf ...*: Aus dieser Liste wird die Festplatte gewählt, auf die die Daten der oben genannten Festplatte kopiert werden sollen.

Abschnitt *Festplatte*
Felder in diesem Abschnitt

- *Inhalt von ...*: Zeigt den Namen der Festplatte, die migriert werden soll.
- *Auf vorhandene Festplatte migrieren*: Hier kann gewählt werden, ob eine vorhandene Festplatte als Speicherziel benutzt werden soll.
- *Auf neue Festplatte migrieren*: Hier wird bei der Migration eine neue Festplatte angelegt, deren Typ hier gewählt werden soll.
- *Festplatte auf V-Cube*: Wird gewählt, dass die Daten auf eine vorhandene Festplatte auf dem V-Cube migriert werden sollen, erscheint hier eine Auswahl mit Zielfestplatten.

Abschnitt *Netzwerkanschluss der VM*
Felder in diesem Abschnitt

- *Virtueller Switch*: Zeigt den Namen des virtuellen Netzwerk-Switch im Cluster.
- *Verbinden mit virtuellem Switch im V-Cube*: Hier wird der virtuelle Netzwerk-Switch auf dem V-Cube ausgewählt, mit dem die virtuelle Maschine verbunden werden soll.

Abschnitt *Status*
Felder in diesem Abschnitt

- *Ausgabe*: Zeigt den Fortschritt der Storage Migration.

Aktionen für dieses Formular

- *Abbrechen*: Beendet den Dialog, die Änderungen werden verworfen.
- *Migration starten*: Die Migration der Daten wird gestartet. Einzelne Snapshots der Festplatten werden auf der Zielfestplatte zusammengeführt. Der aktuelle Zustand bleibt also erhalten, die älteren Snapshot-Zustände werden gelöscht. Details werden in einem separaten Abschnitt ausgegeben

15.6.2.9 *System installieren*
Abschnitt *Installiere*
Felder in diesem Abschnitt

- *Vorlage*: Hier werden Collax Server als Vorlagen aufgelistet. Die Liste kann erweitert werden, wenn weitere Vorlagen in das Verzeichnis template im Cluster-Share abgelegt werden.

- *Ziel-Festplatte*: Die angegebene Festplatte wird mit dem System installiert. Alle Daten gehen verloren.

Abschnitt *Netzwerkeinstellungen*
Felder in diesem Abschnitt

- *Verwenden*: Soll ein Collax System auf die Festplatte installiert werden, können während der Installation die Netzwerkeinstellungen gesetzt werden.
- *FQDN*: Hier wird der vollständig qualifizierte DNS-Name des zu installierenden Rechners eingegeben.
- *IP-Adresse*: Hier wird die IP-Adresse des zu installierenden Rechners eingegeben.
- *Netzwerkmaske*: Hier wird die passende Netzwerkmaske des zu installierenden Rechners eingegeben.
- *Gateway*: Hier wird das Netzwerk-Gateway für den zu installierenden Rechners eingegeben.

Aktionen für dieses Formular

- *Installieren*: Mit dieser Aktion wird die angegebene Vorlage auf die Festplatte installiert. Zur korrekten Durchführung der Aktion ist ein funktionierender Internetzugang erforderlich.

15.7 Netzwerktechnik und -aufbau

Neben dem Interconnect-Netzwerk ist es auch erforderlich, Netzwerke für den Zugriff auf die im Cluster verwalteten virtuellen Maschinen zu definieren. Um eine größere Anzahl von virtuellen Maschinen über den Cluster zu verbinden und gleichzeitig wenig physikalische Netzwerkschnittstellen einzusetzen, werden für die virtuellen Maschinen VLAN-Netzwerke verwendet.

15.7.1 *Virtuelle Netzwerk-Switches*

(Dieser Dialog befindet sich unter *Cluster-Administration – Virtualisierungsdienste – Virtuelle Netzwerk-Switches*

Für den Zugriff auf die virtuellen Maschinen können hier virtuelle Netzwerke angelegt werden. Daran lassen sich mehrere virtuelle Maschinen anschließen. Jede virtuelle Maschine im Cluster hat maximal acht Netzwerkschnittstellen, die an einen virtuelle Netzwerk-Switch angeschlossen werden können.

Die Netzwerkschnittstellen einzelner virtueller Maschinen im Cluster werden unter *Cluster-Administration – Virtualisierungsdienste – Virtuelle Maschinen* im Reiter *Hardware* konfiguriert.

Wenn mehrere Netzwerk-Switches verwendet werden, ist auf jeder einzelnen Node extra sorge zu tragen, dass die Netzwerkverbindung der virtuellen Maschinen funktioniert. Dies kann im Menü *Hardware – Netzwerkschnittstellen* vorgenommen werden.

15.7.1.1 *Virtuellen Netzwerk-Switch wählen*

Spalten in dieser Tabelle

- *Name*: Bezeichnung der Netzwerk-Switch.
- *Kommentar*: Weitere Information über den Netzwerk-Switch.
- *VLAN Tag*: Zeigt den verwendeten VLAN-Tag für den angelegten Netzwerk-Switch.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Das gewählte Element kann nach dieser Aktion bearbeitet werden.
- *Löschen*: Das gewählte Element wird gelöscht.

Aktionen für dieses Formular

- *Hinzufügen*: Mit dieser Aktion kann ein virtueller Netzwerk-Switch hinzugefügt werden. Wenn mehrere Netzwerk-Switches verwendet werden, ist auf jeder einzelnen Node extra sorge zu tragen, dass die Netzwerkverbindung der virtuellen Maschinen funktioniert. Dies kann im Menü *Hardware – Netzwerkschnittstellen* vorgenommen werden.

15.7.1.2 *Virtuellen Netzwerk-Switch bearbeiten*

Felder in diesem Formular

- *Name*: In diesem Feld wird die Bezeichnung des Netzwerk-Switchs eingegeben oder angezeigt.
- *Kommentar*: Hier werden weitere Informationen zum Netzwerk-Switch angegeben. Dieses Feld eignet sich, um den Zweck des

Netzwerks oder der virtuellen Maschinen in diesem Netzwerk näher zu beschreiben.

- *Virtuellen Switch innerhalb des Clusters verbinden*: Diese Option kann zwei Nutzungsszenarien abdecken. *Der voreingestellte Netzwerk-Switch default darf nur mit aktiviertem STP verbunden werden*

  Virtuelle DMZ Wenn eine virtuelle Infrastruktur mit mehreren virtuellen Switches aufgebaut werden soll, müssen diese Switches von jedem Cluster Node aus ansteuerbar sein. Hintergrund ist die Tatsache, dass VMs verteilt im Cluster betrieben werden und gleichzeitig über dieselbe Netzwerkinfrastruktur kommunizieren können müssen. Deshalb sind die virtuellen Switches innerhalb des Clusters zu verbinden. Die Verbindung geschieht über ein physikalisches Netzwerk-Interface, welches auf jedem Cluster-Node im Formular *Einstellungen – Cluster – Lokaler Node – Allgemein*) über das Feld *Virtuelle Netze im Cluster über dieses Interface verbinden* einstellbar ist.

  Im Normalfall kann die Verknüpfung über die Schnittstellen des Cluster-Interconnect erfolgen. Falls weitere unbenutzte Netzwerkschnittstellen verfügbar sind, kann im oben genannten Menüpunkt alternativ auch eine andere Schnittstelle gewählt werden. Ist die Verkabelung der gewählten Schnittstellen über einen physikalischen Switch geführt, muss dieser das gesetzte VLAN-TAG behandeln können.

  Erhöhte Erreichbarkeit mit STP Falls für die Netzwerk-Infrastruktur eine erhöhte Erreichbarkeit der virtuellen Maschinen und des Cluster-Interconnect bewerkstelligt werden soll, kann mit dieser Option der virtuelle Default-Switch (dieser ist standardmäßig über Netzwerkschnittstellen zum LAN verbunden) mit dem Cluster-Interconnect zu einem Ethernet-Ring zusammengeschaltet werden. *Hierfür muss zwingend das STP-Protokoll im*

physikalischen Switch und das hier gesetzte VLAN-Tag konfiguriert sein. Wenn das STP-Protokoll nicht konfiguriert ist, kann es zum Ausfall der Netzwerktopologie kommen. Wenn das VLAN-Tag nicht konfiguriert ist, werden die Cluster-Nodes nicht mehr erreichbar sein.

Eine genaue Beschreibung dieses Szenarios ist auf http://www.collax.com verfügbar.

- *VLAN-Tag*: Mit dem VLAN-Tag können die einzelnen Netzwerke für die virtuellen Maschinen unterschieden werden. Hier kann eine numerische Marke zwischen der Zahl 2 und der Zahl 4096 eingegeben werden.

Aktionen für dieses Formular

- *Abbrechen*: Bearbeiten des Netzwerk-Switch beenden. Die Änderungen werden verworfen.
- *Löschen*: Diese Aktion löscht den Netzwerk-Switch.
- *Speichern*: Bearbeiten des Dialogs beenden. Die Änderungen werden gespeichert.

15.7.2 GUI-Referenz: *Cluster-Konfiguration*

(Dieser Dialog befindet sich unter *Cluster-Administration – Cluster Konfiguration – Aktivieren*)

15.7.2.1 Abschnitt *Ausgabe*
Felder in diesem Abschnitt

- *Ausgabe*: Wenn Einstellungen im Cluster aktiviert werden, wird hier der detaillierte Fortschritt angezeigt.

15.7.2.2 Abschnitt *Änderungen*
Felder in diesem Abschnitt

- *Tabelle*: Hier werden die Änderungen in den jeweiligen Bereichen angezeigt. Die erste Spalte zeigt an, ob ein Element hinzukommt (+), entfällt (-), oder ob sich ein Element geändert hat (C).

  Die zweite Spalte listet die jeweilige Objektgruppe, zu der das Konfigurationsemelent gehört. In der letzten Spalte wird der Wert der vorgenommenen Konfiguration angezeigt.

15.7.2.3 Abschnitt *Aktivierung*
Felder in diesem Abschnitt

- *Cluster Nodes*: Dieser Abschnitt zeigt die Cluster Nodes auf denen eine Aktivierung der Einstellungen vorgenommen wird.
- *Job-Notify*: Diese Aktion öffnet ein Fenster in der Fortschritt von laufenden Systemaufgaben tabellarisch angezeigt werden. So wird unter anderem der Fortschritt einer Aktivierung von Systemeinstellungen oder der Fortschritt automatisch gestarteter Sicherungsjobs angezeigt.

Aktionen für diesen Abschnitt

- *Aktivieren*: Mit dieser Aktion werden Einstellungen auf alle im Cluster befindlichen, aktiven Hosts übertragen. Wenn der erforderliche Dienst für eine Aktivierung nicht gestartet ist, kann diese Aktion nicht durchgeführt werden. Die Logausgabe zeigt entsprechende Details.
- *Undo*: Diese Aktion macht die Änderungen stufenweise rückgängig. Es werden pro Stufe immer alle Änderungen in einem Dialog zurückgenommen. Schon aktivierte Änderungen können hierdurch nicht rückgängig gemacht werden.
- *Redo*: Diese Aktion stellt zurückgenommene Änderungen wieder her.

15.7.2.4 Aktionen für dieses Formular

- *Zurück*: Führt nach der Logausgabe zurück in den Dialog.

15.8 Status und Monitoring

Collax V-Cube informiert über alle Aktivitäten, die im Hintergrund ablaufen. Gleichzeitig werden relevante Messwerte über die virtuellen Maschinen oder den Nodes aufgezeichnet.

15.8.1 GUI-Referenz: *Status Aktive Überwachung*

(Dieser Dialog befindet sich unter *Cluster-Administration – Status/Wartung – Aktive Überwachung*)

In diesem Dialog wird der Status der aktiven Überwachung angezeigt. Intern verwendet das System dazu *Nagios*, dessen Web-GUI hier eingeblendet wird. In dem Menü auf der linken Seite können verschiedene Informationen und Statistiken abgerufen werden.

Wichtig ist das *Tactical Overview*, welches auf einen Blick den Zustand der überwachten Computer (*Hosts*) und Dienste (*Services*) anzeigt. Interessant ist auch die *Status Map*, in der alle Hosts auf einen Blick erfasst werden können. Zudem visualisiert diese Übersicht die Abhängigkeiten der Systeme untereinander.

Die Konfiguration der einzelnen Hosts und der geprüften Dienste auf jedem Host wird in den Einstellungen des jeweiligen *Hosts* vorgenommen.

15.8.2 *Cluster Nodes*

(Dieser Dialog befindet sich unter *Cluster-Administration – Status/Wartung – Cluster Nodes*)

In diesem Dialog werden alle dem Cluster beigetretenen Nodes verwaltet.

15.8.2.1 *Cluster Node wählen*
XXX missing title found
Spalten in der Tabelle

- *Aktiv*: Dieses Feld mit einem grünen Haken zeigt, dass der Node im Cluster verfügbar und aktiv ist. Ein rotes Kreuz symbolisiert einen Fehler. Ein Ausrufezeichen symbolisiert einen Zwischenzustand des Nodes, der nicht fehlerhaft ist, aber der Node ist nicht aktiv im Cluster. Ein rotes Kreuz zeugt an, dass der Node sich Wartungsmodus befindet.
- *Name*: Zeigt den Namen der Maschine im Cluster-Verbund.
- *IP-Adresse*: Zeigt die IP-Adresse der Nodes.
- *Status*: Hier werden der Status des Node im Cluster angezeigt.

  Node is Cluster member – Eine Cluster-Node befindet sich während dem Normalbetrieb im Status *Node is Cluster member*. Dies bedeutet, die Maschine ist im Cluster-Verbund verfügbar und funktioniert somit innerhalb der normalen Parameter. Sie verwaltet Cluster-Ressourcen oder kann bei einem Ausfall einer anderen Node deren Cluster-Ressourcen übernehmen.

  Non-Member (offline) – Es gibt mehrere Gründe, warum eine Node den Status *Non-Member (offline)* einnehmen kann. Prinzipiell ist in diesem Zustand der Dienst *HA Cluster* ausgeschaltet, was auch zutrifft, wenn der Node im Fehlerfall durch das Fencing Device stromlos gesetzt wurde. Dieser Zustand bleibt bestehen, wenn der Node nach dem Fencing wieder gebootet wird, was aus Wartungsgründen geschieht. Denn es ist anzunehmen, dass ein grundlegender Fehler vorliegt, den es gilt zu beseitigen, bevor der Cluster Node wieder dem Cluster-Verbund aktiv beitreten kann. Zusammenfassend tritt der Zustand im Fehlerfall automatisch dann ein, wenn der Node aus ist und wenn der Node nach einem Fencing-Ereignis gestartet wird. Ebenso tritt der Zustand

ein, wenn der Dienst von Hand deaktiviert wurde, von was hier dringend abgeraten wird.

Wurde eine Cluster-Node durch das Fencing Device ausgeschaltet, werden alle Ressourcen der Node auf noch verfügbaren Nodes gestartet. Hierbei können die Ressourcen nicht mehr migriert werden sondern müssen neu gestartet werden. Dies betrifft *Embedded-SAN (eSAN)* nicht.

Um den Zustand *Non-Member (offline)* zu verlassen, ist zunächst die Fehlerursache zu analysieren. Erste Hinweise finden sich im Logfile syslog.ak. Sobald diese Ursache behoben ist, kann die betroffene Cluster-Node durch die Aktion *Nodes aktivieren* wieder in den Verbund aufgenommen werden.

Non-Member (offline, standby) – Um eine Cluster-Node vorübergehend kontrolliert zu Wartungszwecken aus dem Cluster-Verbund zu nehmen, wird zunächst die Aktion *Standby* ausgeführt und anschließend der Dienst *HA Cluster* gestoppt. Dadurch fällt der Node in den Status *Non-Member (offline, standby)*. In diesem Status kann jedwelche Einstellung auf der Software- oder Hardwareseite der Node durchgeführt oder verändert werden. Dazu zählen Hardwaretausch, Software-Updates und Veränderungen an der Netzwerk- und Hardwarekonfiguration des V-Cube. Die virtuellen Maschinen wurden hierbei ohne Betriebsunterbrechung direkt auf andere Nodes migriert.

Non-Member (online, standby) – Dieser Status zeigt an, dass der Cluster Node korrekt arbeitet und sich diese in Bereitschaft befindet. Die virtuellen Maschinen wurden ohne Betriebsunterbrechung direkt auf andere Nodes migriert. Der Cluster Node kann mit der Aktion *Online* wieder in den Verbund aufgenommen werden.

- *Lokale Administration*: Über diesen Link können die Einstellungen jedes einzelnen Nodes erreicht werden. Der Hostname des Nodes muss per DNS auflösbar sein.

Aktionen für jeden Tabelleneintrag

- *Nodes aktivieren*: Ist der Status *Non-Member (online, standby)* kann der Cluster-Node mit dieser Aktion im Cluster verfügbar gemacht werden. Virtuelle Maschinen werden automatisch auf diesen Node migriert oder verteilt, wenn die entsprechende Präferenz für eine virtuelle Maschine gesetzt wurde.
- *Wartungsmodus starten*: Für Wartungszwecke kann der Cluster-Node vorübergehend in den Wartungsmodus gesetzt werden. Virtuelle Maschinen, die auf diesem Node laufen werden automatisch auf andere Nodes im Cluster migriert.
- *Aus dem Cluster entfernen*: Eine Node kann aus dem Cluster-Verbund entfernt werden, wenn deren Status entweder *Non-Member (offline, standby)* oder *Non-Member (offline)* ist. Hierbei wird davon ausgegangen, dass die betreffende Maschine auf Grund von Hardware-Ausfall für den Cluster-Verbund nicht mehr zur Verteilung der Ressourcen nutzbar ist. Es können nur Nodes gewählt werden, die nicht der Maschine entsprechen, von der zu dem Zeitpunkt administriert wird. Mit dieser Aktion werden alle Informationen bezüglich der gewählten Node unwiderruflich aus dem Cluster-Management gelöscht.

  Es ist nach dem Entfernen der Node möglich einen Server mit gleicher oder besserer Hardware und derselben Hardwarekonfiguration wieder als Cluster Node in den Verbund aufzunehmen. Der Hostnamen und die IP-Adressen dürfen identisch sein.

Abschnitt *Hinweis*
Felder in diesem Abschnitt

- : Falls der Node keine Informationen über die Cluster Information Base abrufen kann, wird dieser Hinweis eingeblendet. Ursache hierfür kann ein deaktivierter Dienst *HA Cluster* sein.

Aktionen für dieses Formular

- *Aktualisieren*: Aktualisiert die Ansicht und lädt den Status neu.

15.8.3 *Cluster Ressourcen*

(Dieser Dialog befindet sich unter *Cluster-Administration – Status/Wartung – Cluster Ressourcen*)

Hier können relevante Ressourcen des Clusters überwacht werden. Ressourcen bilden die zentrale Elemente eines Clusters: Alle wesentlichen Konzepte der HA-Lösung werden durch Ressourcen beschrieben - so ist letztendlich eine Virtuelle Maschine eine Ressource. Aber auch Festplattenabbilder für die virtuellen Maschinen oder das Fencing Device sind Ressourcen.

Innerhalb der Cluster-Ressourcen bestehen Abhängigkeiten, ohne die das HA-Konzept nicht funktionieren kann. So ist im Cluster-Verbund Grundvoraussetzung, dass ein Fencing Device definiert ist und von der Ressourcen-Verwaltungssoftware gestartet werden kann.

15.8.3.1 XXX missing title found

Spalten in der Tabelle

- *Name*: Hier wird der Name der Ressource angezeigt. Der Name beinhaltet Abkürzungen.
- *Ort*: Zeigt den Ort, d.h. den Node an, auf dem sich die Ressource befindet. Üblicherweise werden Ressourcen auf allen Hosts gestartet. Ausnahmen sind das Fencing Device und die virtuellen Maschinen.
- *Info*: In diesem Feld werden eventuell auftretende Fehler beim Starten oder Stoppen einer Ressource angezeigt.

- *Ist-Zustand*: Zeigt an, ob die Ressource momentan gestartet oder gestoppt ist.
- *Soll-Zustand*: Zeigt an, ob die Ressource gestartet oder gestoppt sein soll. Weicht der Ist- vom Soll-Zustand über einen längeren Zeitraum ab, liegt wahrscheinlich ein Fehlerfall vor.

Aktionen für jeden Tabelleneintrag

- *Detail*: Mit dieser Aktion wird eine grafische Darstellung der Ressource und deren Abhängigkeit zu anderen Ressourcen angezeigt.
- *Bereinigen*: Unter bestimmten Umständen ist es erforderlich, einzelne Cluster-Ressourcen zu bereinigen. Diese Aktion prüft, ob die Ressource noch verwendet wird. Ist dies der Fall, wird die Ressource gestoppt, der Status zurückgesetzt und gestartet. Eine Ressource wird nicht mehr verwendet und muss bereinigt werden, wenn das entsprechende Element gelöscht wurde.
- *Starten*: Mit dieser Aktion kann eine gestoppte Ressource gestartet werden. Üblicherweise braucht diese Aktion nicht ausgeführt werden, da in einer funktionierenden Cluster-Domain Ressourcen automatisch korrekt gestartet oder gestoppt werden.
- *Stoppen*: Mit dieser Aktion kann eine gestartete Ressource gestoppt werden. Üblicherweise braucht diese Aktion nicht ausgeführt werden, da in einer funktionierenden Cluster-Domain Ressourcen automatisch korrekt gestartet oder gestoppt werden.
- *Manage*: Diese Aktion ist nur dann möglich, wenn die Ressource nicht durch den Cluster verwaltet wird. Mit dieser Aktion wird die Verwaltung durch den Cluster wieder aktiviert.

15.8.3.2 Abschnitt *Hinweis*
Felder in diesem Abschnitt

- : Falls Informationen innerhalb des Clusters nicht verfügbar sind wird hier ein entsprechender Hinweis ausgegeben.

15.8.3.3 Aktionen für dieses Formular

- *Alle bereinigen*: Mit dieser Aktion werden alle Cluster-Ressourcen bereinigt. Das bedeutet, dass alle Ressourcen gestoppt, deren Status aktualisiert und anschließend wieder gestartet werden. Verwaiste Ressourcen werden hierdurch entfernt.

  Hinweis: Diese Aktion darf nur zur Fehlerermittlung ausgeführt werden, da laufenden virtuelle Maschinen gestoppt werden und so im Netzwerk temporär nicht mehr zur Verfügung stehen.
- *Graphische Übersicht*: Führt zu einer graphischen Übersicht der Ressourcen im Cluster und stellt Abhängigkeiten dar.
- *Aktualisieren*: Mit dieser Aktion werden die Informationen über die Ressourcen aktualisiert. Das Formular baut sich anschließend neu auf.

15.8.3.4 *Ressourcen Constraints*
XXX missing title found

- : In der graphischen Übersicht werden Abhängigkeiten und Status der Cluster Ressourcen visualisiert dargestellt. Hierbei ist anhand der Einfärbung und der Umrandung ersichtlich, wie der detaillierte Zustand einer Ressource ist.

  Die *Füllfarbe* kennzeichnet die Auswertung von Ist- und Soll-

Zustand. Grün (gestartet) und orange (gestoppt) bedeuten, dass Ist- und Soll-Zustand identisch sind. Der Zustand ist in beiden Fällen in Ordnung, da gewollt. Mit der Färbung in rot wird angezeigt, dass die Ressource gestartet sein soll aber auf Grund eines Fehlers nicht gestartet ist.

Die *Umrandung* zeigt an, ob die Ressource im Cluster gestartet (grün), gestoppt (rot) oder auf Grund einer Abhängigkeit momentan gestartet ist, aber sich im Wartezustand befindet (gelb).

Aktionen für dieses Formular

- *Zurück*: Führt zurück zur Übersicht.

15.8.4 GUI-Referenz: *Dienste im Cluster*

(Dieser Dialog befindet sich unter *Cluster-Administration – Status/Wartung – Cluster Dienste*)

Dieser Dialog zeigt die Dienste aller im Cluster-Verbund aktiven Nodes an. Falls erforderlich kann ein Dienst im Cluster über diesen Dialog gestoppt oder gestartet werden.

15.8.4.1 *Cluster Dienst wählen*

Spalten in dieser Tabelle

- *Dienst*: Zeigt die Bezeichnung des Dienstes an.
- *Subsystem*: Diese Spalte zeigt die Gruppe an, zu der der Dienst gehört.
- *Ort*: Zeigt an, auf welchem Host der Dienst läuft.

- *Status*: Hier wird der Status des Dienstes angezeigt. „Running“ bedeutet, dass der Dienst aktiviert ist und läuft, „stopped“ hingegen, dass der Dienst in der Konfiguration aktiviert ist, der Dienst jedoch aus unbestimmtem Grund gestopped wurde. Der Status „Crashed“ bedeutet, dass der Dienst zwar aktiviert wurde, dieser jedoch auf Grund eines Fehlers nicht gestartet wurde.

Aktionen für jeden Tabelleneintrag

- *Start*: Um einen Dienst zu starten, muss über das Kontextmenü (rechter Mausklick) „Start“ angeklickt werden.
- *Stop*: Um einen Dienst zu starten, muss über das Kontextmenü (rechter Mausklick) „Stop“ angeklickt werden.

Aktionen für dieses Formular

- *Aktualisieren*: Aktualisiert die Liste der Cluster Dienste.

15.8.5 GUI-Referenz: *Cluster Monitor*

(Dieser Dialog befindet sich unter *Cluster-Administration – Status/Wartung – Cluster Monitor*)

15.8.5.1 Felder in diesem Formular

- *Cluster Ressourcen Monitor*: Der Cluster Ressourcen Monitor erlaubt es, den Status des Clusters zu kontrollieren. Seine Ausgabe umfasst die Anzahl der Knoten und der Ressourcen, die im Cluster konfiguriert sind, inklusive dem gegenwärtigen Status.

Im Abschnitt *Node List* werden alle im Cluster konfigurierten Hosts mit den zugeteilten Cluster Ressourcen aufgelistet. Im Normalfall hat ein Host den Status *online*, der Status wird grün hinterlegt. Im Fehlerfall werden Statusmeldungen mit in Farbe Rot angezeigt.

Sind Ressourcen oder Nodes nicht aktiv, werden diese im Abschnitt *Inactive Resources* aufgelistet.

- *Hinweis*: Wenn der HA Cluster-Dienst nicht gestartet ist wird hier ein entsprechender Hinweis ausgegeben.

15.8.5.2 Aktionen für dieses Formular

- *Aktualisieren*: Diese Aktion aktualisiert die Cluster-Monitor-Ausgabe.

16 Verschiedene Dienste

16.1 *Datum und Zeit*

Eine möglichst exakte Systemzeit ist wichtig, um beispielsweise Logdateien zwischen verschiedenen Servern vergleichen zu können. Daher kann die Systemzeit des V-Cubes über NTP mit Zeitservern abgeglichen werden. Alternativ kann ein DCF77-Funkempfänger angeschlossen werden.

Seine eigene Systemzeit kann der V-Cube wiederum für andere Systeme per NTP im Netzwerk bereitstellen.

Intern wird die Uhrzeit als GMT, also Greenwich-Standardzeit, gespeichert. Diese wird dann unter Kenntnis des Standorts (Kontinent und Ort) in die lokale Zeit konvertiert; dabei wird auch die Umstellung mit Sommer- und Winterzeit berücksichtigt.

NTP („Network Time Protocol“) wird genutzt, um eine Zeitinformation im Internet zu übertragen. Üblicherweise werden mehrere Server per NTP befragt, da so eine genauere Uhrzeit ermittelt werden kann. Dies ist möglich, da die übertragene Uhrzeit durch die Laufzeit der IP-Pakete verfälscht wird. NTP besitzt Mechanismen, um diesen Fehler zu ermitteln und zu korrigieren. Je mehr Zeitserver zur Verfügung stehen, desto genauer wird die Uhrzeit. Über Internetabgleich ist eine minimale Abweichung von 10 Millisekunden erreichbar.

Eine noch genauere Uhrzeit lässt sich mit einem Empfänger erreichen, der ein von einer zuständigen Einrichtung übertragenes Funksignal auswertet. In Deutschland geschieht dies durch die Physikalisch-Technische Bundesanstalt (PTB), die den DCF77-Sender bei Frankfurt betreibt. Dieses Signal wird von Funkuhren und -Weckern ausgewertet. Es existiert verschiedene Hardware, mit der

ein Computer dieses Signal auswerten kann. Der V-Cube unterstützt ein solches Gerät zum Anschluss an die serielle Schnittstelle.

16.1.1 GUI-Referenz: Konfiguration

(Dieser Dialog befindet sich unter *Zeit – Konfiguration*)

In diesem Dialog kann die Systemzeit geändert und die Zeitzone angegeben werden. Die Systemzeit kann auch über eine Synchronisationsquelle gesetzt werden.

16.1.1.1 Abschnitt *Zeitzone*

Felder in diesem Abschnitt

- *Kontinent*: Hier wird der Kontinent ausgewählt. Damit wird die Auswahl der Einträge im Feld *Region/Ort* angepasst.
- *Region/Ort*: Hier wird die Region oder ein Ort in der Nähe ausgewählt.

16.1.1.2 Abschnitt *Synchronisationsquelle*

Über eine Synchronisationsquelle kann die Systemuhr automatisch gesetzt werden.

Wird hier die *Systemuhr* ausgewählt, wird ausschließlich die interne Uhr des Systems genutzt. Diese gehen meist allerdings nicht sehr genau. Bei einem Abgleich von Logdateiinformationen sind exakte Uhrzeiten jedoch unerlässlich. Daher sollte eine andere Quelle gewählt werden.

Wenn das System über eine Standleitung ans Internet angeschlos-

sen ist oder im lokalen Netz ein NTP-Server betrieben wird, kann mit „NTP“ die Uhrzeit permanent synchronisiert werden.

Eine andere Möglichkeit ist, einen „DCF-77-Funkempfänger“ an das System anzuschließen und darüber permanent die Uhrzeit zu synchronisieren.

Felder in diesem Abschnitt

- *Typ*: Hier wird die Synchronisationsquelle ausgewählt.
- *Zeitserver*: Wird *NTP* als Quelle ausgewählt, muss hier ein Zeitserver angegeben werden, der über NTP ansprechbar ist.
- *Alternativer Zeitserver*: Hier kann ein zweiter Zeitserver angegeben werden, um eine bessere Qualität der ermittelten Uhrzeit zu erreichen.
- *Empfänger*: In dieser Liste sind alle unterstützten DCF-77-Empfänger aufgelistet.
- *Schnittstelle*: Hier wird die serielle Schnittstelle ausgewählt, an die der Empfänger angeschlossen ist. Es sind nur die Schnittstellen verfügbar, die weder mit serieller Konsole oder Modem noch einer USV belegt sind.
- *Datum*: Wird die interne Hardwareuhr des Rechners als Zeitquelle ausgewählt, kann hier das aktuelle Datum korrigiert werden.
- *Zeit*: Wird die interne Hardwareuhr des Rechners als Zeitquelle ausgewählt, kann hier die aktuelle Zeit korrigiert werden.

16.1.1.3 Aktionen für diesen Dialog

- *Datum/Zeit setzen*: Mit dieser Aktion wird die eingegebene Zeit mit Datum übernommen.

  Hinweis: War vorher eine andere Synchronisationsquelle als

die Systemuhr eingestellt, muss die Konfiguration zunächst aktiviert werden. Danach sollte die Uhrzeit kontrolliert und gesetzt werden.

16.1.2 GUI-Referenz: *NTP-Server*

(Dieser Dialog befindet sich unter *Serverdienste – NTP – Konfiguration*)

In diesem Dialog wird der NTP-Dienst konfiguriert. Über diesen können andere Systeme ihre Systemzeit abgleichen.

16.1.2.1 Tab *Grundeinstellungen*

Felder in diesem Abschnitt

- *Aktivieren*: Mit dieser Option wird auf diesem System der NTP-Zeitserver aktiviert.

16.1.2.2 Tab *Berechtigungen*

Felder in diesem Abschnitt

- *Zugang zu NTP-Port erlauben für*: Rechner und Netze, die zu einer der aktivierten Gruppen gehören, dürfen den NTP-Dienst abfragen. Für Benutzer in diesen Gruppen hat diese Einstellung keine direkten Auswirkungen.

16.1.2.3 Tab *Optionen*

Felder in diesem Abschnitt

- *Broadcast verwenden*: Wird diese Option aktiviert, sendet der Server seine aktuelle Systemzeit als Broadcast-Nachricht in das lokale Netz.

16.2 Netzwerküberwachung

In jedem Netzwerk ist die automatische Überwachung von wichtigen Komponenten empfohlen, um schnell auf Ausfälle reagieren zu können. Der V-Cube bietet die Möglichkeit, in ein bestehendes Überwachungssystem eingebunden zu werden. Dazu können mit SNMP („Simple Network Management Protocol“) wichtige Parameter ausgelesen werden. SNMP ist ein verbreitetes und einfaches Protokoll und wird von vielen Managementsystemen unterstützt. Um auf die Daten des V-Cubes zuzugreifen, müssen SNMP aktiviert und die „SNMP-Community“ gesetzt werden.

Der V-Cube kann auch selbst das umliegende Netzwerk überwachen. Dazu stehen zwei unterschiedliche Mechanismen zur Verfügung. Bei der „passiven Überwachung“ steht mehr der Sicherheitsaspekt im Vordergrund, um neue, fremde Systeme im Netzwerk zu erkennen. Der V-Cube speichert dabei die IP- und MAC-Adressen aller Systeme, von denen er Datenpakete im Netzwerk „sieht“. Dies beschränkt sich auf die Netzwerksegmente, an die der V-Cube direkt mit einer Ethernetkarte angeschlossen ist (lokale Netze). Die passive Netzwerküberwachung ist notwendig, damit die Funktion *Hosts importieren* im V-Cube zur Verfügung steht.

Über die Option *Versende E-Mail bei Änderungen* wird beim Auftau-

chen von neuen Geräten im Netzwerk eine E-Mail verschickt. Damit werden fremde Geräte im Netzwerk schnell erkannt.

Bei der „aktiven Überwachung“ müssen hingegen die zu überwachenden Systeme vorher bekannt sein. Diese werden dann permanent überprüft und Ausfälle per E-Mail gemeldet.

Die zu überwachenden Systeme werden im V-Cube als *Hosts* angelegt. Dabei können die verschiedenen Dienste ausgewählt werden, die überwacht werden sollen. So ist es möglich, einen Mailserver zu überwachen, indem permanent die Dienste SMTP, POP3 und IMAP abgefragt werden. Der zu überwachende Server kann im lokalen Netz oder im Internet oder hinter einem VPN-Tunnel stehen. Er muss nur per IP-Adresse erreichbar sein, und der V-Cube muss auf die zu überwachenden Dienste zugreifen dürfen.

Die aktive Überwachung nutzt der V-Cube auch intern, um sich selbst zu überwachen und die betroffenen Dienste bei Ausfällen neu zu starten. In solchen Fällen wird keine Alarmierung vorgenommen.

16.2.1 Schritt für Schritt: Host überwachen

- Prüfen Sie, ob unter *Überwachung – Aktiv* die aktive Überwachung eingeschaltet ist. Falls nicht, aktivieren Sie diese.
- Bei einem Ausfall erhalten Sie *3 Meldungen* im *Abstand von 10 Minuten*. Sie können diese Werte auf Ihre Bedürfnisse anpassen.
- Wechseln Sie zu *Netzwerk – DNS – Hosts* und bearbeiten Sie den Host-Eintrag, den Sie überwachen möchten.
- Wenn noch kein Eintrag zu dem Host existiert, legen Sie zunächst einen neuen Eintrag (S. 241) an.
- Wechseln Sie im Host-Eintrag auf den Reiter *Netzwerk-Tests*.
- Hier können Sie verschiedene Tests aktivieren, die auf diesen Host angewendet werden. Um beispielsweise einen Mailserver

zu überwachen, aktivieren Sie die Tests für *IMAP*, *POP3* und *SMTP*.

- Über den *Alarmierungszeitraum* können Sie festlegen, wann Alarme ausgelöst werden. Sie können eigene Zeiträume in den *Benutzungsrichtlinien* definieren. So kann die Überwachung von internen Servern auf die Arbeitszeit begrenzt werden.
- Wenn Sie eine komplexe Netzwerkstruktur administrieren, können Sie unter *Erreichbar über* den vorhergehenden Router (aus Sicht des V-Cubes) angeben. Fällt dieser aus, wird für Systeme dahinter kein Alarm ausgelöst. Deren Zustand ist dann „unbestimmt".
- Wechseln Sie zu den *Benutzungsrichtlinien* und bearbeiten Sie die Gruppe, über die Sie die Überwachungsberechtigung verwalten möchten. Legen Sie ggf. eine neue Gruppe zu diesem Zweck an. In den *Berechtigungen* der Gruppe unter dem Punkt *Monitor* können Sie den Zugriff auf die *aktive Überwachung* gewähren.
- Fügen Sie Benutzer als Mitglieder zu dieser Gruppe hinzu. Diese Benutzer haben nach Aktivierung der Konfiguration Zugriff auf die Nagios-Überwachungskonsole über das User-Webportal und können dort den Status des Netzwerkes einsehen. Diese Benutzer werden zudem bei einem Alarm über E-Mail benachrichtigt, vorausgesetzt, auf dem V-Cube ist ein E-Mail-System eingerichtet.

16.2.2 GUI-Referenz: *SNMP*

(Dieser Dialog befindet sich unter *Überwachung – SNMP*)

Über SNMP können verschiedene Daten dieses Systems mittels einer geeigneten Software über Netzwerk überwacht und aufgezeichnet werden.

16.2.2.1 Tab *Grundeinstellungen*
Felder in diesem Abschnitt

- *Aktivieren*: Wird diese Option aktiviert, ist der SNMP-Server über das Netzwerk erreichbar. Andernfalls ist das System so konfiguriert, dass nur Verbindungen vom lokalen System zulässig sind.
- *Community zum Lesen*: Hier wird der Name der „Community" für SNMPv1/SNMPv2c angegeben. Die Community ist eine Art Passwort für den Zugriff auf die SNMP-Daten. Der Name der Community wird im Allgemeinen als Klartext übermittelt und bietet daher nur minimalen Schutz.
- *Standort*: Hier kann der Standort des Systems angegeben werden.

16.2.2.2 Tab *Berechtigungen*
Felder in diesem Abschnitt

- *Zugriff auf SNMP-Port erlauben für*: Alle Rechner und Netze, die zu einer der aktivierten Gruppen gehören, bekommen Zugriff auf den SNMP-Dienst. Für Benutzer hat diese Einstellung keine Auswirkungen.

16.2.3 GUI-Referenz: *Netzwerk passiv überwachen*

(Dieser Dialog befindet sich unter *Überwachung – Passiv*)

Die passive Netzwerküberwachung überwacht die Netzwerkschnittstellen nach Datenpaketen und kann so IP-Adressen und MAC-Adressen von Systemen entdecken, die im gleichen Netzwerksegment kommunizieren.

Das Aktivieren dieser Option bietet die Möglichkeit, beim Anlegen von *Hosts* direkt alle Systeme zu importieren. Dabei wird deren jeweilige IP-Adresse und MAC-Adresse automatisch übernommen.

16.2.3.1 Felder in diesem Dialog

- *Aktivieren*: Hier kann die Überwachung aktiviert werden. Dabei werden Pakete auf allen oder gewählten Netzwerkschnittstellen überprüft und die MAC- sowie IP-Adressen der aktiven Computersysteme erkannt.
- *Versende E-Mail*: Mit dieser Option wird der Administrator per E-Mail benachrichtigt, wenn Änderungen im Netzwerk erkannt werden (neue Systeme erscheinen, vorhandene Systeme ändern ihre IP-Nummer, usw.).
- *Alle Ethernet-Links*: Mit dieser Option wird Überwachung auf allen angelegten Verbindungen vom Typs Ethernet aktiviert.
- *Ausgewählte Ethernet-Links*: Hier kann die Überwachung auf bestimmte Ethernet-Links beschränkt werden. Es ist möglich, mehrere Links auszuwählen.

16.2.3.2 Aktionen für diesen Dialog

- *Lösche bislang ermittelte Daten*: Hiermit werden alle bisher ermittelten Daten gelöscht.

  Dies ist nützlich, wenn viele alte oder unwichtige Systeme erkannt und in die Liste aufgenommen wurden.

  Hinweis: Der V-Cube wird nach dem Löschen sofort weiter Daten ermitteln.

16.2.4 *Fernüberwachung*

(Dieser Dialog befindet sich unter *Überwachung – Fernüberwachung (NRPE)*

In diesem Formular kann die Fernüberwachung des lokalen Servers ermöglicht werden. Technische Basis für die Fernüberwachung ist der NRPE-Dienst, Nagios Remote Plugin Execution. Um die Fernüberwachung in einem geschützten Netzwerk zu ermöglichen, muss darin Zugriff auf Port 5666 gewährt werden. Der Zugriff auf den Collax Server wird im Reiter Berechtigungen erlaubt.

16.2.4.1 Tab *Grundeinstellungen* Felder in diesem Abschnitt

- *Aktiviert*: Hier wird die Möglichkeit zur Fernüberwachung dieses lokalen Servers eingeschaltet.

16.2.4.2 Tab *Berechtigungen*, Abschnitt *Zugriff erlauben für ...* Felder in diesem Abschnitt

- *Fernüberwachung über NRPE*: Die Rechner der gewählten Gruppen dürfen dieses System fernüberwachen. Der Zugriff erfolgt über Port 5666. Hier werden nur Gruppen angezeigt, die Hosts enthalten.

16.2.4.3 Aktionen für dieses Formular

- *Abbrechen*: Bearbeiten des Fernüberwachungs-Zugriff beenden. Die Änderungen werden verworfen.
- *Speichern*: Bearbeiten des Fernüberwachungs-Zugriff beenden. Die Änderungen werden gespeichert.

16.2.5 GUI-Referenz: *Aktive Überwachung*

(Dieser Dialog befindet sich unter *Überwachung – Aktiv*)

In diesen Dialogen wird die Konfiguration der aktiven Überwachung vorgenommen. Intern verwendet das System dazu *Nagios.* Primär wird Nagios zur Selbstüberwachung des Systems eingesetzt. Es können jedoch auch weitere Systeme im Netz überwacht werden.

In diesem Teil der Konfiguration wird angegeben, ob der aktive Monitor zur Überwachung gestartet werden soll sowie welche Gruppen beim Ausfall eines Dienstes alarmiert werden sollen und Zugang zum Web-Interface erhalten.

Die Konfiguration der einzelnen Hosts und der geprüften Dienste auf jedem Host wird in den Einstellungen des jeweiligen *Hosts* vorgenommen.

16.2.5.1 Tab *Grundeinstellungen*
Felder in diesem Abschnitt

- *Aktivieren*: Hier wird die Netzwerküberwachung der Systemdienste und von entsprechend konfigurierten Rechnern mittels Nagios aktiviert.
- *Anzahl der Meldungen*: Hier kann die Anzahl der Meldungen begrenzt werden, die für einen Vorfall versandt werden.

Wird hier „1“ angegeben, wird eine E-Mail versandt, wenn ein Dienst oder ein Host ausfällt. Eine weitere E-Mail wird versandt, wenn das Problem behoben wurde.

Wird ein Wert größer als „1“ angegeben, wird eine E-Mail bei Ausfall versandt und jeweils nach Ablauf des „Alarmintervalls“ eine weitere. Hinweis: Es wird keine E-Mail mehr versandt, wenn das Problem nach der maximalen Anzahl von Meldungen behoben wird.

Bleibt der Wert leer oder wird eine „0“ angegeben, hängt das Verhalten vom Wert im Feld *Alarmintervall* ab. Wird dort ebenfalls eine „0“ eingetragen, werden keine Meldungen verschickt. Dann wird der Status der überwachten Dienste und Rechner nur in der Nagios-Web-Oberfläche angezeigt. Wird ein Wert größer 0 im Feld *Alarmintervall* angegeben, werden die Fehlermeldungen im angegebenen Intervall wiederholt.

- *Alarmintervall (Minuten)*: Hier wird das Intervall angegeben, in dem ein Alarm wiederholt werden soll. Dieser Wert steht in engem Zusammenhang mit der *Anzahl der Meldungen*.

16.2.5.2 Tab *Berechtigungen*

Felder in diesem Abschnitt

- *Nagios Benachrichtigungs-Berechtigung*: Für alle aktivierten Benutzer wird ein „contact“-Eintrag in der Nagios-Konfiguration erzeugt; jede aktivierte Gruppe erscheint als „contactgroup“. Diese Benutzer und Gruppen erhalten von Nagios automatisch E-Mail Benachrichtigungen.
- *Zugriff auf aktive Überwachung*: Alle Benutzer, die zu einer der aktivierten Gruppen gehören, bekommen über den URL „https://IP-Adresse:8001/nagios/“ oder die Web-Access-Seite Zugriff auf

die aktive Überwachung. Rechner und Netze sind von dieser Einstellung nicht betroffen.

16.2.6 *Watchdog-Timer*

Der Watchdog ist ein Timer, der einen Reset auslöst, wenn er abläuft. Im normalen Betriebszustand läuft der Watchdog-Timer nie ab, weil in bestimmten Zeitintervallen das System geprüft wird. Wenn die Datenpartition korrekt beschrieben werden kann, wird der Timer zurückgesetzt. Für diese Art der Systemüberwachung mit Fehlerkorrektur ist entsprechende Hardware erforderlich. Diese Watchdog-Überwachung unterstützt die Hardware des Intel 6300ESB Watchdog Timer.

Wurde ein Reset auf Grund eines schweren Systemfehlers ausgelöst, bleibt der Watchdog-Timer inaktiv, um eine Reset-Schleife zu verhindern. Der Watchdog-Timer kann im Betrieb über den Dialog *System – Überwachung/Auswertung – Status – Dienste* wieder gestartet werden.

16.2.6.1 Abschnitt *Hinweis*

Felder in diesem Abschnitt

- : Um die Watchdog-Überwachung zu aktivieren muss das Gerät Intel 6300ESB Watchdog Timer vorhanden sein.

16.2.6.2 Abschnitt *Einstellungen*

Felder in diesem Abschnitt

- *Aktivieren*: Hier wird die Watchdog-Überwachnung aktiviert.

Aktionen für diesen Abschnitt

- *Abbrechen*: Beendet den Dialog, die Änderungen werden verworfen.
- *Speichern*: Beendet den Dialog, die Änderungen werden gespeichert.

16.3 Server Management mit Spotlight

Collax Spotlight soll helfen den Überblick über mehrere Collax Server zu bewahren, die Administration von mehreren Server zu erleichtern und frühzeitig bei anbahnenden Problemen zu warnen.

Spotlight sammelt Informationen der Spotlight Agenten ein und visualisiert diese innerhalb des Web-Access. Über das Management im Web-Access können verschiedene Detailstufen eingesehen werden.

16.3.1 Schritt für Schritt: Spotlight und Spotlight Agent einrichten

16.3.1.1 Spotlight Server

- Wechseln Sie auf dem Spotlight Server ins Formular *Spotlight – Konfiguration* und aktivieren Sie Spotlight.
- Tragen sie im Feld *Servername* die IP-Adresse oder den DNS-Servernamen ein, den die Spotlight Agenten über das Netzwerk erreichen können.
- Vergeben Sie entsprechenden Benutzern über die Angabe einer Gruppen Berechtigung auf das Spotlight Management. Zusätzlich markieren Sie Gruppen mit Netzwerken, aus denen die Spotlight Agenten Zugriff erhalten sollen.
- Speichern Sie die Einstellungen.
- Laden Sie sich über den Knopf *Download Agent-Konfiguration* eine vorgefertigte Konfiguration für die Spotlight Agenten herunter.
- Aktivieren Sie die Einstellungen
- Wenn Sie den V-Cube hinter einer Firewall installiert haben, die keine direkten HTTPS-Zugriffe zulässt, muss ein port forwarding eingerichtet werden.

16.3.1.2 Spotlight Agent

- Wechseln Sie auf dem Spotlight Server ins Formular *Spotlight Agent – Konfiguration*.
- Geben Sie im Abschnitt *Upload* die vorweg gespeicherte Konfigurationsdatei ein und laden Sie die Datei hoch.
- Die Einstellungen für die Verbindung sind nun automatisch eingerichtet worden.
- Wechseln Sie auf den Reiter *Informationsbereiche* und wählen Sie

aus, welche Bereiche von Spotlight ausgewertet werden sollen.
- Wechseln Sie auf den Reiter *Kommandos* und definieren Sie, welche Befehle von Spotlight ausgeführt werden dürfen.
- Speichern und aktivieren Sie die Einstellungen. Der Spotlight Agent meldet sich automatisch bei Spotlight an.
- Wechseln Sie nun in den Web-Access.

16.3.2 Erste Schritte im Spotlight Management

Das Management-Interface von Spotlight wird über den Web Access aufgerufen oder kann direkt mit der URL https://spotlightserver/ak/spotlight/ aufgerufen werden. Dort haben Sie die Möglichkeit sich im linken Bereich eine Baumstruktur für die verwalteten Server aufzubauen. Hierzu können Sie per Rechtsklick oder über die Buttons am unteren Rand neue Ordner anlegen.

Im bereits vorhandenen Ordner „unsortiert“ finden Sie alle Server von denen der Spotlight Agent erfolgreich eine Verbindung zu Houston aufbauen konnte. Per Drag&Drop können Sie die Server in die Struktur ziehen.

Setzen Sie nun ein Häkchen in der Box neben einem Server oder einem Ordner. Die markierten Server werden nun im rechten Bereich angezeigt. Mit einem einfachen Klick werden durch Ausklappen weitere Informationen angezeigt.

Mit einem Doppelklick wird für den Server eine neue Registerkarte geöffnet, auf der Sie alle Detailinformationen zu diesem Server finden. Über die Buttons haben Sie die Möglichkeit zu diesem Server einen Kommentar zu hinterlegen oder eine Aufgabe zu definieren, die zu einem bestimmten Zeitpunkt ausgeführt werden soll. Mit dem Button „Start ssh“ können Sie eine ssh-Session über ein Browser-Applett starten. Über den Button „Administrationsoberfläche“ gelangen

Sie direkt zur Konfiguration des ausgewählten Servers. Wenn Sie die Credentials hinterlegt haben („Anmeldeinformationen hinterlegen“), werden Sie in beiden Fällen automatisch angemeldet.

Wenn Sie auf „Add Task“ klicken, erhalten Sie eine Auswahl der Aufgaben, die auf diesem Server durchgeführt werden dürfen. Es dürfen nur Befehle ausgeführt werden, die in der Konfiguration des Spotlight-Agenten explizit erlaubt wurden. Nachdem eine neue Aufgabe festgelegt wurde, erscheint sie in der Tabelle. Wurde die Aufgabe ausgeführt, können Sie hier die Ausgabe des Befehls abrufen. Einen Überblick über alle Aufgaben aller Server finden Sie in der Registerkarte „Aufgaben“.

Über der Baumstruktur finden Sie Filter mit der Sie die Auswahl der angezeigten Server einschränken können. Mit dem Plus-Button können Sie beliebige eigene Filter definieren und benutzen. Ist ein Filter aktiv, was zur Folge hat, dass einige Server in der Übersicht fehlen können, ist der Filter-Button rot. Es können auch mehrere Filter kombiniert werden. Mit dem Besen-Knopf können Sie alle Filter deaktivieren, so dass wieder alle Server angezeigt werden

16.3.3 GUI-Referenz: *Spotlight*

(Dieser Dialog befindet sich unter *Überwachung – Spotlight*

16.3.3.1 Abschnitt *Grundeinstellungen*

Felder in diesem Abschnitt

- *Aktiviert*: Diese Option aktiviert die zentrale Sammlung von Daten von Spotlight Agenten.
- *Servername*: Hier muss eine IP-Adresse oder ein DNS-Server-

namenn des Spotlight-Servers angegeben werden, den die Spotlight-Agenten netzwerktechnisch erreichen können.
- *Berechtigungen*: Spotlight-Agenten aus den gewählten Netzwerkgruppen dürfen auf den Spotlight-Server zugreifen. Zusätzlich erhalten Benutzer und Netzwerke der gewählten Gruppen Zugriff auf die Spotlight Web-Applikation im Collax Web Access.
- : Es erscheint ein Hinweis, falls kein Zertifikat hinterlegt wurde.

Aktionen für diesen Abschnitt

- *Download Agent-Konfiguration*: Um die Einstellungen für die Spotlight-Agenten zu vereinfachen, kann hier die passenden Konfigurationsdatei heruntergeladen werden. Diese kann auf allen Spotlight-Agenten, die über diesen Server verwaltet werden, hochgeladen und benutzt werden.

16.3.3.2 Aktionen für dieses Formular

- *Abbrechen*: Beendet den Dialog, Änderungen werden verworfen.
- *Speichern*: Beendet den Dialog, Änderungen werden gespeichert.

16.3.4 GUI-Referenz: *Spotlight Agent*

(Dieser Dialog befindet sich unter *Überwachung – Spotlight Agent*

16.3.4.1 Tab *Grundeinstellungen*, Abschnitt *Upload*
Aktionen für diesen Abschnitt

- *Upload*: Um die Verbindungskonfiguration zwischen dem Spotlight-Agenten und dem Spotlight-Server zu vereinfachen, kann hier die Konfiguration von Spotlight hochgeladen werden. Die Konfigurationsdatei „ spotlight.token“ enthält entsprechende Zertifikate und die IP-Adresse oder DNS-Namen des Spotlight-Servers.

16.3.4.2 Abschnitt *Grundeinstellungen*
Felder in diesem Abschnitt

- *Aktiviert*: Hier kann der Spotlight-Agent aktiviert werden.
- *Zertifikat*: Dieses Zertifikat wird verwendet, um Daten zwischen dem Spotlight-Server und dem Spotlight-Agenten zu verschlüsseln.
- *IP-Adresse Spotlight-Server*: Hier ist die IP-Adresse anzugeben, unter der der Spotlight-Server von den Spotlight-Agenten aus erreichbar ist.

16.3.4.3 Tab *Informationsbereiche*
Felder in diesem Abschnitt

- *Folgende Informationen übertragen*: Informationen der gewählten Dienste des laufenden Systems können vom Spotlight-Server über den Agenten abgefragt werden.

16.3.4.4 Tab *Kommandos*, Abschnitt *Globale Kommando-Optionen* Felder in diesem Abschnitt

- *Administrations-GUI und SSH erlauben*: Mit dieser Option wird dem Spotlight-Server erlaubt Verbindungen zur Adminstrationsoberflache und zum SSH-Dienst des Spotlight-Agenten aufzubauen. Ist diese Option aktiviert, muss der Spotlight-Server auf den Ports 8892 und 8895 erreichbar sein.
- *Freie Kommandos erlauben*: Diese Option erlaubt es dem Spotlight-Server beliebige Systemkommandos auf dem Spotlight-Agenten auszuführen und deren Ergebnisse auszuwerten. Aus sicherheitstechnischen Gründen sollte dies nur in einzelnen Fällen erlaubt werden. Alternativ können frei definierbare Kommandos fest hinterlegt werden. Siehe Aktion *Neues Kommando*.

16.3.4.5 Tab *Kommandos*, Abschnitt *Kommando* Felder in diesem Abschnitt

- *Name*: Zeigt oder deklariert den Namen des definierten Kommandos.
- *Kommando*: Zeigt oder deklariert das Systemkommando.
- *Parameteranzahl*: Zeigt oder definiert die Parameteranzahl des deklarierten Systemkommandos.
- *Kommentar*: Weitere Informationen über das Kommando.
- *Aktiviert*: Definiert, ob das Kommando vom Spotlight-Server ausgeführt werden darf.
- *Name*: Zeigt den Namen des vordefinierten Kommandos.
- *Kommentar*: Zeigt weitere Informationen über das vordefinierte Kommando.
- *Aktiviert*: Definiert, ob das vordefinierte Kommando vom Spotlight-Server ausgeführt werden darf.

Aktionen für diesen Abschnitt

- *Neues Kommando*: Diese Aktion öffnet einen Dialog um ein neues Systemkommando zu definieren. In der Verwaltungs-GUI des Spotlight-Servers wird dieses Kommando in die Liste der ausführbaren Kommandos eingetragen.
- *Löschen*: Diese Aktion löscht ein hinzugefügtes Kommando.

16.3.4.6 Aktionen für dieses Formular

- *Abbrechen*: Beendet den Dialog, die Änderungen werden verworfen.
- *Speichern*: Beendet den Dialog, die Änderungen werden gespeichert.

16.4 USV

16.4.1 GUI-Referenz: *USV-Geräte*

(Dieser Dialog befindet sich unter *USV – USV-Geräte*)

In diesem Dialog können USV-Geräte (Unterbrechungsfreie Stromversorgungen) eingerichtet werden. Das System, das direkt mit der USV kommuniziert, wird als *Master* bezeichnet. Der Status der USV kann über das Netzwerk an andere Systeme (*Clients*) weitergereicht werden, umso bei einem längeren Stromausfall alle Systeme geregelt herunterzufahren.

Bei einem Stromausfall laufen die angeschlossenen Systeme zunächst auf Batteriebetrieb weiter. Wenn der Ladezustand der

Batterien einen kritischen Wert erreicht, schickt der Master den Clients ein Kommando zum Herunterfahren. Anschließend fährt er selbst herunter und sendet als letztes Kommando der USV den Befehl zum Abschalten. Manche USVs können bei Rückkehr des Stroms eine Zeitlang warten und die Batterien bis über die kritische Grenze laden, bevor sie die Systeme wieder einschalten. Dann kann ein zweiter folgender Stromausfall ebenfalls abgefangen werden.

Weitere Informationen zur Technik und möglichen Anschlussstrategien sind auf der Projektseite dieser Software zu finden: <http://www.networkupstools.org/>.

Eine Kompatibilitätsliste ist unter dieser Adresse abrufbar: <http://www.networkupstools.org/stable-hcl.html>.

16.4.1.1 *Geräte*

(Dieser Dialog befindet sich unter *USV – USV-Geräte*)

Felder in diesem Dialog

- *Name*: Hier wird der Name der USV angezeigt.
- *Kommentar*: Hier steht der Kommentartext zu der USV.
- *Netzwerk*: Hier wird angezeigt, ob es sich um eine „Netzwerk-USV“ handelt. Eine solche USV ist nicht direkt angeschlossen, sondern der Status wird von einem anderen System über das Netzwerk erfragt (vorausgesetzt, der Switch ist auch an einer USV angeschlossen).
- *Master*: Für jede USV muss im Netzwerk ein Master existieren, der die Kommunikation mit der USV übernimmt.
- *Versorgt dieses System*: Hier wird angezeigt, ob auf einen Stromausfall reagiert wird.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion werden die Einstellungen der USV bearbeitet.
- *Löschen*: Mit dieser Aktion wird die USV gelöscht.

Aktionen für diesen Dialog

- *Suche*: Mit dieser Aktion kann nach, an USB angeschlossenen, USV-Geräten gesucht werden.
- *Anlegen*: Mit dieser Aktion wird eine neue USV angelegt.

16.4.1.2 *Bearbeiten*

(Dieser Dialog befindet sich unter *USV – USV-Geräte*)

Felder in diesem Dialog

- *Name*: Hier wird der Name der USV angegeben.
- *Kommentar*: Hier kann ein Kommentartext zur USV eingegeben werden.
- *Diese USV steuern*: Wenn die USV lokal angeschlossen ist, kann das System als *Master* mit der USV kommunizieren. Dann muss das Modell und die Schnittstelle der USV ausgewählt werden.
- *Versorgt dieses System*: Wird diese Option aktiviert, wird die USV beobachtet und es wird auf einen Ausfall der USV reagiert. Das deaktivieren dieser Option ist hilfreich, wenn die Stromversorgung des Systems nicht an die USV angeschlossen ist. Das deaktivieren dieser Option ist nur bei über Netzwerk abfragbaren USVs möglich.

- *Über Netzwerk abfragen*: Wird diese Option aktiviert, kann die USV über das Netzwerk abgefragt werden. Dazu muss auf der USV oder dem entsprechenden Steuerungssystem ein *Nut-USV-Daemon* ab Version 1.1.0 laufen.
- *Rechner*: Der Hostname oder die IP-Adresse des Rechners, an dem die USV angeschlossen ist.
- *Name der USV dort*: Wenn mehrere USVs angesteuert werden, kann hier ein Name als Identifikator hinterlegt werden. Damit können die USV-Geräte besser unterschieden werden.
- *User*: Der Benutzername, der zur Authentifizierung gesendet wird.
- *Passwort*: Das Passwort zur Authentifizierung.
- *Typ*: Hier muss der Typ der USV aus der Liste der unterstützten Geräte ausgewählt werden.
- *Anschluss*: Hier wird der Port ausgewählt, an dem die USV angeschlossen ist, z. B. die erste serielle Schnittstelle COM1 (ttyS0). Die serielle Schnittstelle muss hierzu unter *Hardware* für die Verwendung *Sonstiges* konfiguriert sein.

16.4.2 GUI-Referenz: *USV-Benutzer*

(Dieser Dialog befindet sich unter *USV – USV-Benutzer*)

In diesem Dialog werden Benutzeraccounts verwaltet, die den USV-Status abfragen dürfen. Dabei handelt es sich nicht um vollwertige Benutzerkonten. Normale Benutzer können die USV nicht abfragen.

16.4.2.1 *USV-Benutzer wählen*

(Dieser Dialog befindet sich unter *USV – USV-Benutzer*)

Felder in diesem Dialog

- *Benutzer*: Der Name des USV-Benutzers.
- *Beschreibung*: Hier wird der Kommentartext zum Benutzer angezeigt.
- *Erlaube Master*: Hier wird angezeigt, ob der Benutzer die Berechtigung hat, als *Master* zu arbeiten.

Aktionen für jeden Tabelleneintrag

- *Bearbeiten*: Mit dieser Aktion wird der ausgewählte USV-Benutzeraccount bearbeitet.
- *Löschen*: Mit dieser Aktion wird der angelegte Benutzeraccount gelöscht.

Aktionen für diesen Dialog

- *Anlegen*: Mit dieser Aktion wird ein neues USV-Benutzerkonto angelegt.

16.4.2.2 *USV-Benutzer bearbeiten*

(Dieser Dialog befindet sich unter *USV – USV-Benutzer*)

Felder in diesem Dialog

- *Name*: Hier wird der Name des USV-Benutzers eingegeben. Es handelt sich hierbei nicht um vollwertige Benutzeraccounts, sondern um eine Kombination aus Login und Passwort zur Authentifizierung am USV-Monitor-Dienst.

- *Name*: Hier wird der Name des USV-Benutzers angezeigt. Wird ein bestehendes Nutzerprofil bearbeitet, kann der Name nicht geändert werden.
- *Kommentar*: Hier kann ein Kommentartext zum Benutzer eingegeben werden.
- *Passwort*: Hier wird das Passwort für den Benutzer gesetzt.
- *Passwort (Wiederholung)*: Da das Passwort aus Sicherheitsgründen bei der Eingabe nicht lesbar ist, muss es hier wiederholt werden.
- *Darf die USV steuern*: Diese Option erlaubt dem Benutzer, Master einer USV zu sein. Ein Rechner pro USV muss immer Master sein. Es kann nur einen Master für eine USV geben. Der Master übernimmt Steueraufgaben bei der Koordination der Shutdowns und ist zudem derjenige, der USV-Steuerkommandos absenden darf (instcmd). Sinnvollerweise wird der Master auf dem System eingerichtet, welches direkt mit der USV verbunden ist.

16.4.3 *USV-Dienst*

In diesem Formular kann die Zugriffsberechtigung auf den USV-Verwaltungsdienst für Netzwerke gesetzt werden. Ein Zugriff auf den USV-Dienst ist dann sinnvoll, wenn am Server eine USV lokal angeschlossen ist und wenn die Information eines Stromausfalls an andere Rechner im Netzwerk weitergegeben werden soll.

16.4.3.1 Felder in diesem Formular

- *Zugriff erlauben für*: Mit dieser Berechtigung wird der entsprechende Firewall-Port geöffnet. Rechner und Netzwerke in den

aktivierten Gruppen dürfen dann auf den USV-Dienst zugreifen. Der Zugriff ist über das Network UPS Tool (NUT) oder einfach über weitere Collax Server möglich.

Zugriff auf den USV-Dienst ist dann möglich, wenn mindestens ein USV-Gerät an einem seriellen oder an einem USB-Anschluss konfiguriert ist.

16.4.3.2 Aktionen für dieses Formular

- *Abbrechen*: Bearbeiten des USV-Dienstes beenden. Die Änderungen werden verworfen.
- *Speichern*: Bearbeiten des USV-Dienstes beenden. Die Änderungen werden gespeichert.

17 Lizenzierung, Update und Softwaremodule

17.1 Lizenz

Die Lizenz eines V-Cube legt fest, wie viele Benutzeraccounts, Netzwerklinks und Maildomains maximal verwendet werden dürfen. Lizenzen ohne Beschränkungen sind dabei ebenfalls erhältlich.

Die Lizenz wird in Form einen Lizenzcodes geliefert und muss in der Weboberfläche eingegeben werden. Nach Eingabe des Lizenzcodes wird die Lizenz online geprüft und im Anschluss auf dem V-Cube freigeschaltet.

Eine Lizenz ist immer mit der Subscription kombiniert. Diese berechtigt innerhalb der Laufzeit zum Zugriff auf den Updateserver, um Softwareaktualisierungen durchzuführen und zusätzliche Softwaremodule zu installieren.

Ein nicht registriertes System erlaubt nur eine minimale Anzahl von Benutzern und Netzwerklinks. Damit ist es möglich, eine Internetverbindung aufzubauen und die Registrierung durchzuführen.

In der Weboberfläche wird die aktuell zulässige sowie die bereits genutze Anzahl angezeigt. Bei Änderungen an der Lizenz muss ggf. der Lizenzstatus online aktualisiert werden, um die korrekte Ausgabe zu erhalten. Über das Collax Web Account kann eine Übersicht über die einzelnen Lizenzen abgefragt werden, etwa die Laufzeit. Bei der Lizenzaktivierung können mehrere Systeme unter einem Account in Collax Web Account aufgenommen werden.

17.1.1 GUI-Referenz: *Lizenzen und Module*

(Dieser Dialog befindet sich unter *System – Systembetrieb – Software – Lizenzen und Module*)

17.1.1.1 Tab *Status*, Abschnitt *Systemlizenz*

Felder in diesem Abschnitt

- *Unregistriert*: Dieser Informationstext weist darauf hin, dass das System noch nicht registriert ist. Damit ist es nicht möglich, Updates durchzuführen oder weitere Softwaremodule zu installieren.
- *Lizenznummer*: Hier wird die auf diesem System verwendete Lizenznummer angezeigt.
- *Collax Web Account*: Dieser Link verweist direkt in das Collax Web Account. Dort sind weitere Informationen zu der Lizenz abrufbar, etwa über die Laufzeit.
- *Support-Übersicht und Dokumente*: Dieser Link verweist auf die Supportinformationen auf der Collax-Website. Hier sind u. a. die Release-Notes zu den einzelnen Versionsständen abrufbar.
- *Lizenzstatus ungültig*: Dieser Text wird angezeigt, wenn eine ungültige Lizenz für das System vorliegt.

Dieses System ist nicht registriert. Bitte registrieren Sie zuerst Ihre Software, um alle Funktionen nutzen zu können.

Solange das System unregistriert ist, gelten die unten dargestellten Limitierungen.

Diese Lizenz ist nur für nichtkommerziellen Einsatz zugelassen.

Sie haben die Möglichkeit, die Lizenz dieser Maschine zu löschen, um eine neue Lizenz zu registrieren. Drücken Sie dazu den Knopf „Lizenz freigeben“.

Lizenzen können nur einmal registriert werden. Damit sie ein weiteres Mal verwendet werden können, müssen sie vom Collax-Support freigeschaltet werden. Dies dient zu Ihrem Schutz, damit Dritte Ihre Lizenz nicht ebenfalls verwenden können.

Geben Sie Lizenzen nur frei, wenn es erforderlich ist.

Diese Lizenz ist nur für Händler zugelassen und darf nicht weiterverkauft werden.

17.1.1.2 Tab *Status*, Abschnitt *Nur für nichtkommerzielle Nutzung*

Felder in diesem Abschnitt

- *Hinweis*: Bei der Verwendung einer Lizenz für nichtkommerzielle, private Nutzung wird dieser Hinweistext angezeigt.

17.1.1.3 Tab *Status*, Abschnitt *Nicht für Wiederverkauf*

Felder in diesem Abschnitt

- *Not for resale*: Bei einer Lizenz, die nicht für den Wiederverkauf bestimmt ist, wird dieser Hinweistext angezeigt.

17.1.1.4 Tab *Status*, Abschnitt *Berechtigungen*

In dieser Übersicht wird die derzeit benutzte und die erlaubte Anzahl von Benutzerkonten, Netzwerklinks, E-Maildomains von Modulen und Funktionen dargestellt.

Kann die benutzte Anzahl nicht genau ermittelt werden, weil beispielsweise der V-Cube als Mail-Relayserver eingesetzt wird und daher die Benutzer auf einem nachgeschalteten Mailserver verwaltet werden, wird der Wert „Externe Benutzer“ angezeigt.

Spalten in der Tabelle

- *Limit*: In dieser Spalte werden die einzelnen Objekte bzw. Module aufgelistet, für die Beschränkungen existieren.
- *Benutzt*: In dieser Spalte wird für jedes Objekt die vom System ermittelte Anzahl aktuell genutzter Berechtigungen angezeigt.
- *Erlaubt*: In dieser Spalte wird die durch die Lizenz maximal zulässige Anzahl von Berechtigungen für das jeweilige Objekt angezeigt.

17.1.1.5 Tab *Status*, Abschnitt *Zusatzmodule*

In dieser Tabelle werden die verfügbaren Zusatzmodule angezeigt. Für jedes Modul wird aufgelistet, welcher Lizenz es unterliegt und ob es auf dem V-Cube bereits installiert ist.

Spalten in der Tabelle

- *Paket*: In dieser Spalte wird die Bezeichnung des Softwaremoduls ausgegeben.
- *Beschreibung*: Hier wird eine kurze Beschreibung zu jedem Modul angezeigt, die den genauen Einsatzzweck erläutert.
- *Status*: In dieser Spalte wird angezeigt, ob das Modul bereits installiert ist oder nicht.
- *Lizenz*: Hier wird der Lizenztyp des jeweiligen Softwaremoduls angezeigt. Es gibt kostenlose Module, für die keine weitere Lizenz erworben werden muss, kostenpflichtige Module, für die ein Aktivierungsschlüssel erworben werden muss, und kostenpflichtige Module, für die eine Hersteller-Lizenz erhältlich ist.

  Eine solche Hersteller-Lizenz ist eine Lizenzdatei, die im

Gegensatz zu den hier verwalteten Lizenzschlüsseln in der Weboberfläche bei der Konfiguration des Softwaremoduls selbst eingespielt wird.

Aktionen für jeden Tabelleneintrag

- *Installieren*: Mit dieser Aktion wird das Softwaremodul installiert. Dabei werden entsprechende Pakete vom Updateserver heruntergeladen und in das System integriert.

  Eine Installation kann im Regelfall dann erfolgen, wenn das betreffende Produkt oder Zusatzmodul mit einem Lizenzschlüssel aktiviert wurde.
- *Entfernen*: Mit dieser Aktion wird ein Softwaremodul wieder aus dem System entfernt.

17.1.1.6 Tab *Lizenz-Verwaltung*, Abschnitt *Zusätzliche Lizenzen*

Felder in diesem Abschnitt

- *Zusätzliche Lizenzen*: Um weitere Benutzer oder zusätzliche Softwaremodule zu lizenzieren, können hier weitere Lizenzen dem System hinzugefügt werden.
- *Lizenzschlüssel*: In diesem Feld muss der Aktivierungsschlüssel angegeben werden.

Aktionen für diesen Abschnitt

- *Aktivieren*: Mit dieser Aktion wird der Aktivierungsschlüssel in das System übernommen und online überprüft.

17.1.1.7 Tab *Lizenz-Verwaltung*, Abschnitt *Lizenz freigeben*

Felder in diesem Abschnitt

- *Lizenz freigeben*: Bei einem Wechsel der Lizenz oder bei einem Verkauf des Systems oder aus sonstigem Grund kann die Lizenz auf dieser Seite von dem System entfernt werden.

  Nach diesem Vorgang ist der V-Cube bezüglich der Lizenzierung wieder im Auslieferungszustand, d. h., er ist eine lizenzlose, unregistrierte, im Funktionsumfang eingeschränkte Testversion.

Aktionen für diesen Abschnitt

- *Lizenz freigeben*: Mit dieser Aktion wird die Lizenz freigegeben.

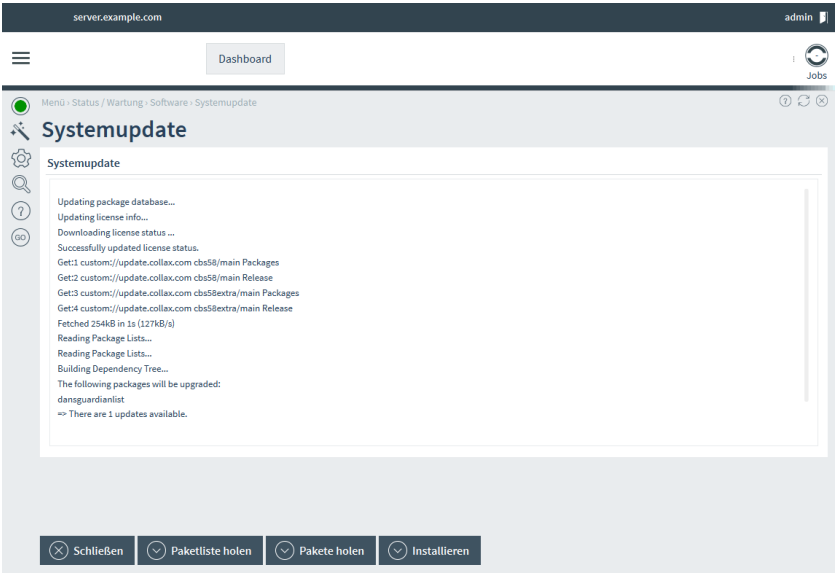
17.1.1.8 Aktionen für dieses Formular

- *Zurück*: Diese Aktion führt zurück zur Hauptansicht.
- *Lizenzstatus aktualisieren*: Mit dieser Aktion wird der angezeigte Lizenzstatus mit dem Registrierungsserver abgeglichen. Dies kann in seltenen Fällen notwendig sein, wenn Änderungen an der Lizenz durchgeführt wurden.

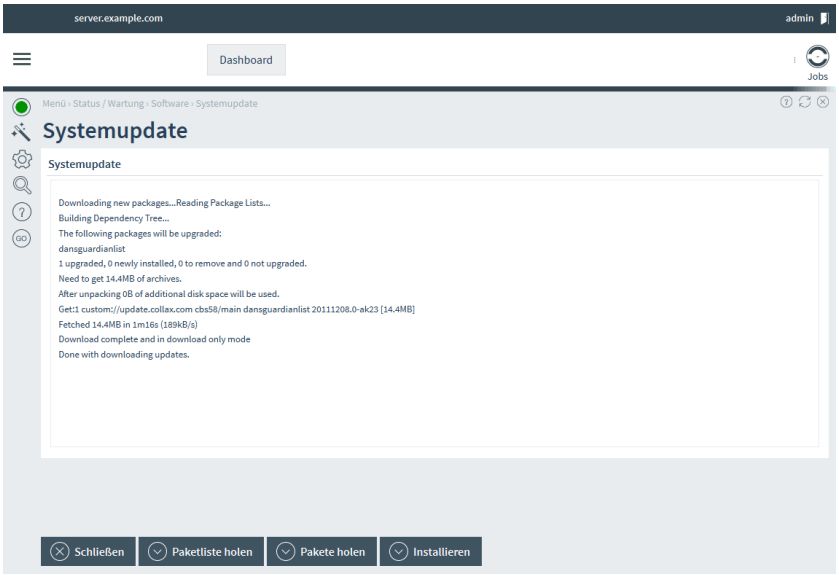
17.2 Systemsoftware

17.2.1 Schritt für Schritt: System aktualisieren

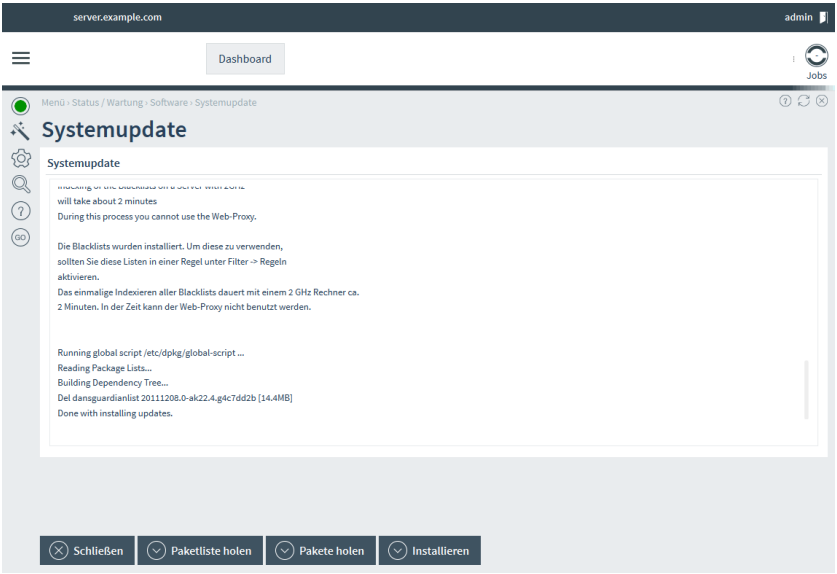
- Wechseln Sie auf den Reiter *System* links vom Hauptmenü.
- Rufen Sie dort unter *Systembetrieb – Software* die Seite *Systemupdate* auf.
- Am unteren Rand sind drei Schalter. Klicken Sie auf *Paketliste holen*. Nun wird die aktuelle Paketliste vom Update-Server heruntergeladen.
- Wenn Sie den V-Cube hinter einer Firewall installiert haben, die keine direkten HTTPS-Zugriffe nach außen lässt, müssen Sie unter *Einstellungen – Systembetrieb – Softwareupdate – Konfiguration* einen *Proxy-Server* einstellen.



- Während des Ladens der Paketliste erscheint eine Animation. Wenn Sie auf die Animation klicken, sehen Sie ein Terminalfenster mit detaillierteren Ausgaben.
- Wenn auf dem Update-Server neue Pakete vorhanden sind, sehen Sie eine Zeile diesen oder ähnlichen Inhalts: *25 packages upgraded, 1 newly installed, 0 to remove and 0 not upgraded*. Hier werden 25 Pakete aktualisiert und ein neues Paket wird dem System hinzugefügt.



- Um den Download der Pakete zu starten, klicken Sie auf *Pakete holen*.



- Durch *Installieren* starten Sie die Installation der heruntergeladenen Pakete.
- Auch hier können Sie das Terminalfenster für eine detaillierte Ausgabe öffnen. In diesem Fall wird durch das Update der Kernel ausgetauscht, dazu muss der V-Cube neu gestartet werden. Ein entsprechender Hinweis findet sich am Ende der Ausgabe.

17.2.2 GUI-Referenz: *Systemupdate*

(Dieser Dialog befindet sich unter *Systembetrieb – Software – Systemupdate*)

In diesem Dialog werden Softwareupdates heruntergeladen und installiert. Die Updates werden von einem Update-Server heruntergeladen, dazu muss das System registriert sein und über einen gültigen

Subscriptionvertrag verfügen. Releasenotes und weitere Hinweise zu den Updates sind auf der Webseite des Herstellers verfügbar.

Beim Download von Dateien wird das HTTPS-Zertifikat des Update-Servers überprüft. Dadurch wird gewährleistet, dass die Updates nicht durch Dritte verfälscht wurden.

17.2.2.1 Felder in diesem Dialog

- *Release-Notes*: Neuerungen und Änderungen eines Systemupdates sind für Collax-Server in Release-Notes festgehalten. An dieser Stelle können die aktuellen Release-Notes eingesehen werden.
- *Ausgabe*: In diesem Feld werden die Ausgaben der Updateaktionen angezeigt. Es sollte auf jeden Fall bis zur Ausgabe der Zeile *done* abgewartet werden, bevor weitere Konfigurationen o. ä. vorgenommen werden.

17.2.2.2 Aktionen für diesen Dialog

- *Paketliste holen*: Hier wird eine aktuelle Paketliste vom Updateserver heruntergeladen. Sind neue Pakete auf dem Server verfügbar, wird dies mit ausgegeben.
- *Pakete holen*: Hier wird der Download der aktualisierten Pakete gestartet. Im Anschluss wird keine Installation durchgeführt.
- *Installieren*: Hier wird die Installation der Pakete gestartet. Wurden vorher keine Pakete heruntergeladen, wird zunächst der Download durchgeführt.

17.2.3 GUI-Referenz: *Manueller Upload*

(Dieser Dialog befindet sich unter *Systembetrieb – Software – Manueller Upload*)

In seltenen Fällen besteht die Möglichkeit, spezielle Updatedateien manuell einzuspielen. Pakete aus nicht vertrauenswürdigen Quellen können die Integrität des Systems gefährden. Hier sollten also nur Pakete in Absprache mit dem Support des Herstellers eingespielt werden.

17.2.3.1 Felder in diesem Dialog

- *Datei*: Hier wird die Datei ausgewählt, die eingespielt werden soll. Es muss sich dabei um ein gültiges V-Cube-Softwarepaket handeln.
- *Ergebnis*: Nach der Installation werden hier die Ausgaben der Installation angezeigt.

17.2.3.2 Aktionen für diesen Dialog

- *Update einspielen*: Mit dieser Aktion wird der Upload gestartet.

17.2.4 *Endbenutzer-Lizenzvertrag*

(Dieser Dialog befindet sich unter *Systembetrieb – Software – Endbenutzer-Lizenzvertrag*)

In diesem Formular wird der Endbenutzer-Lizenzvertrag der erworbenen Software angezeigt.

17.2.5 *Registrierung des Servers*

(Dieser Dialog befindet sich unter *System – Systembetrieb – Software – Registrierung*)

Mit Hilfe dieses Assistenten wird der V-Cube registriert. Dieser Assistent gleicht die beim Hersteller hinterlegten Daten des Fachhandelspartner ab und bietet die Möglichkeit diese Daten falls erforderlich, zu korrigieren.

17.2.5.1 Ablauf

Im ersten Schritt wird die Erreichbarkeit des Collax Lizenzierungs-Server getestet. Anschließend kann die erhaltene Lizenznummer eingegeben werden.

Nachfolgend werden die hinterlegten Daten des Fachhandelspartner zur Überprüfung angezeigt. Änderungen können vorgenommen werden. Im Anschluss werden die Endbenutzerdaten zur Kontrolle angezeigt.

Handelt es sich bei der eingetragenen Lizenz um eine NFR-Lizenz (nicht für den Wiederverkauf bestimmt), kann die Registrierung fertiggestellt werden. Wird eine Lizenz für die private Nutzung registriert, entfällt die Anzeige des Fachhandelspartner. Es werden nur die Endbenutzerdaten angezeigt.

Der Server wird nach der Zusammenfassung registriert. Durch die Registrierung kann die Software-Update-Funktionen des Servers und der registrierten Software-Module für die Dauer der Laufzeit genutzt werden. Detailinformationen über die Lizenz können über das Collax Web Account unter http://www.collax.com abgerufen werden

17.3 GUI-Referenz: *Update-Konfiguration*

(Dieser Dialog befindet sich unter *Softwareupdate – Konfiguration*)

In diesem Dialog kann ein Proxy für den Download von Systemupdates konfiguriert werden. Dies kann notwendig sein, wenn der V-Cube hinter einer Firewall betrieben wird und keine direkte Internetverbindung aufbauen kann. Der Proxyserver muss allerdings HTTPS unterstützen.

17.3.1 Felder in diesem Dialog

- *Proxy für Updates benutzen*: Durch das Aktivieren dieser Option werden Updates über einen Proxyserver heruntergeladen.
- *Typ des Proxys*: Da die Verbindung zum Updateserver verschlüsselt ist, sollte hier bei Verwendung eines zwischengeschaltetem Proxy, das Systemupdate mittels CONNECT-Methode angefordert werden. Falls diese Methode nicht zum Erfolg führt, weil der Proxy diese nicht unterstützt, kann hier optional auch die GET-Methode verwendet werden.
- *Proxy*: Hier wird der Hostname oder die IP-Adresse des Proxyservers angegeben, der verwendet werden soll.
- *Proxy-Port*: Der Port des Proxyservers muss hier angegeben werden. Ein Standard-Squid-Proxy benutzt meist den Port 3128.
- *Proxy-Authentifizierung benutzen*: Falls der Proxy einen Benutzernamen und ein Passwort zur Authentifizierung verlangt, muss diese Option aktiviert werden.
- *Proxy-Benutzername*: Hier wird der Benutzername zur Nutzung des Proxyservers angegeben.
- *Proxy-Passwort*: Hier wird das zugehörige Passwort angegeben.

18 Systembetrieb

18.1 GUI-Referenz: *Netzwerk-Tools*

(Dieser Dialog befindet sich unter *Systembetrieb – Werkzeugkasten – Netzwerk-Tools*)

Der Werkzeugkasten bietet die Möglichkeit, vom V-Cube aus verschiedene Netzwerktests durchzuführen. Hier können DNS-Anfragen durchgeführt, Ping-Anfragen verschickt und Routen untersucht werden.

18.1.1 Abschnitt *Netzwerktest*

18.1.1.1 Felder in diesem Abschnitt

- *Name oder IP-Adresse*: Hier wird die IP-Adresse oder der Host- bzw. Domainname angegeben, der abgefragt und überprüft werden soll.
- *Aktion*: Hier wird die Aktion ausgewählt, die für die Adresse bzw. den Namen durchgeführt werden soll. Es können mehrere Aktionen ausgewählt werden, diese werden nacheinander durchgeführt.

  Die Aktion *dns* befragt einen DNS-Server nach dem angegebenen Namen oder der Adresse. Welche Informationen abgefragt werden und welcher DNS-Server befragt wird, kann angegeben werden, wenn die *dns*-Option aktiviert wurde.

  Mit der Aktion *whois* kann abgefragt werden, wem eine Internetdomain oder eine IP-Adresse gehört. Leider funktioniert der Dienst nicht (mehr) mit allen Top-Level-Domains, insbesondere

nicht mit Namen unterhalb von „.de“. Hier wurde die Veröffentlichung der Informationen aus Datenschutzgründen eingestellt.

Die Aktion *route* ermittelt, über welchen Link ein Zielrechner derzeit erreicht werden könnte. Diese Aktion nutzt die Routingtabellen des Systems, es werden keine Daten verschickt. Wenn hier ein Name eingegeben wurde, muss dieser Name zunächst per DNS-Anfrage in eine IP-Adresse aufgelöst werden. Ist der DNS-Server nicht erreichbar oder nicht konfiguriert, kann die Route nicht ermittelt werden.

Die Aktion *ping* sendet ICMP Echo-Request-Pakete an den Zielrechner und prüft, ob und mit welcher Laufzeit ICMP Echo-Reply-Pakete empfangen werden. Wenn als Ziel ein Hostname angegeben wird, muss der Name zuerst auf eine IP-Adresse aufgelöst werden. Ist der DNS-Server nicht erreichbar oder nicht konfiguriert, kann das Ping nicht verschickt werden.

- *Frage DNS nach*: Wird *dns* als Aktion ausgewählt, kann hier angegeben werden, welche Informationen im DNS abgefragt werden.
- *Nameserver*: Hier kann ein Nameserver angegeben werden, der befragt werden soll. Bleibt das Feld leer, wird der aktuell im System konfigurierte DNS verwendet.

18.1.2 Abschnitt *Fernzugriff*

18.1.2.1 Felder in diesem Abschnitt

- *Konsolen*: Hier können zwei Konsolen für Fernzugriff ausgewählt werden. Die Konsolen werden in einem Browser-Pop-Up-Fenster geöffnet. Damit die Aktion korrekt gestartet werden kann, müssen Pop-Up-Fenster vom Browser erlaubt sein.

  Mit *SSH* wird ein Terminal über eine verschlüsselte Verbindung

geöffnet. Ein Benutzername für das Login muss angegeben werden.

Eine unverschlüsselte Verbindung kann mit der Wahl von *Telnet* gestartet werden. Hier kann der Ziel-Port angegeben werden, standardmäßig wird Port 23 benutzt.

- *SSH-Benutzername*: Hier wird der Benutzername für den Fernzugriff per SSH eingegeben.
- *Telnet-Port*: Hier wird der Ziel-Port für die Telnet-Verbindung angegeben. Der Telnet-Dienst benutzt als Standard Port 23. Für Tests anderer Dienste kann dieser Port verändert werden.

18.1.3 Abschnitt *Antworten*

Hier werden die ermittelten Informationen angezeigt.

18.1.4 Aktionen für diesen Dialog

- *Aktion starten*: Abfragen über die Toolbox starten.

18.1.5 GUI-Referenz: *Aufräumen*

(Dieser Dialog befindet sich unter *Systembetrieb – Werkzeugkasten – Aufräumen*)

Der Verbleib von benutzerbezogenen Daten im Collax System geschieht, um generell Datenverlust zu vermeiden. In diesem Dialog können Daten, die noch auf dem Collax Server gespeichert sind aber keine zugehörigen Benutzer oder Konfigurationsdaten enthalten, endgültig im System aufgeräumt werden. Die zu diesen Daten

gehörenden Elemente wie Verzeichnisse, Benutzer oder Datensicherungsaufgaben wurden zuvor über die Administrationsoberfläche entfernt.

Bei Sicherungen kann es auch bei ungewollten Unterbrechungen der Sicherungsarbeiten dazu kommen, dass verwaiste Datensätze (Medien) im System hinterbleiben. Diese Medien können ebenso über diesen Dialog aufgeräumt werden.

18.1.5.1 Tab *Verzeichnisse*
Felder in diesem Abschnitt

- *Verwaiste Verzeichnisse*: Hier wird eine Liste von File-Shares angezeigt, die aus der Collax Administration entfernt wurden.

18.1.5.2 Aktionen für diesen Dialog

- *Verzeichnisse löschen*: Die ausgewählten Verzeichnisse werden durch diese Aktion endgültig aus dem System gelöscht. Alle Inhaltsdaten der gewählten Ordner gehen dadurch verloren.

18.1.5.3 Tab *Persönliche Ordner*
Felder in diesem Abschnitt

- *Verwaiste Ordner*: Hier wird eine Liste von persönlichen Ordnern angezeigt, deren Besitzer nicht mehr auf dem Collax Server existieren.

18.1.5.4 Aktionen für diesen Dialog

- *Ordner löschen*: Durch diese Aktion werden die gewählten persönlichen Ordner endgültig aus dem System gelöscht. Alle Inhaltsdaten der gewählten Ordner gehen dadurch verloren.

18.1.5.5 Tab *Postfächer*
Felder in diesem Abschnitt

- *Verwaiste Postfächer*: Hier wird eine Liste von Postfächern angezeigt, deren Besitzer nicht mehr auf dem System existieren. Der Name des Postfach lautet identisch zu dem Login des nicht mehr existenten Benutzers.

18.1.5.6 Aktionen für diesen Dialog

- *Postfächer löschen*: Mit dieser Aktion werden die gewählten Postfächer aus dem Collax System gelöscht. Alle E-Mails der gewählten Postfächer gehen dadurch verloren.

18.1.5.7 Tab *Sicherungsdaten*
Felder in diesem Abschnitt

- *Verwaiste Sicherungsdaten*: Hier wird eine Liste von lokalen Sicherungsdaten angezeigt, bei denen referenzierende Informationen aus der Konfiguration entfernt wurden oder durch einen unterbrochenen Sicherungsdurchlauf verloren gingen.

18.1.5.8 Aktionen für diesen Dialog

- *Sicherungsdaten löschen*: Die ausgewählten lokalen Sicherungsdaten werden mit dieser Aktion bereinigt und aus dem Collax System entfernt.

18.2 *Festplattenverwaltung*

Über die Festplattenverwaltung ist es mit Hilfe des „Logical Volume Management“ (LVM) möglich, weitere Festplattenkapazitäten nachzurüsten und damit die Datenpartition des V-Cubes zu vergrößern.

Der V-Cube behandelt dabei Festplatten und physikalische Partitionen als „physikalische Volumes“. Aus diesen physikalischen Volumes werden „logische Volumes“ gebildet, diese werden vom System als Partitionen zum Speichern von Daten verwendet.

Mehrere „logische Volumes“ gehören zu einer „Volume Group“, die durch Hinzufügen von „physikalischen Volumes“ erweitert werden kann.

18.2.1 GUI-Referenz: Festplattenverwaltung

(Dieser Dialog befindet sich unter *Systembetrieb – Hardware – Festplattenverwaltung*)

In diesem Dialog werden alle vorhandenen Volume-Gruppen verwaltet. Informationen zu angeschlossenen Festplatten können eingesehen werden.

18.2.1.1 Tab *Volume-Gruppen*, Abschnitt *Volume-Gruppe*

Felder im Abschnitt

- *Name*: Name der angezeigten Volume-Gruppe.
- *Größe*: Gesamte Größe des Speicherplatzes, die die Volume-Gruppe mit allen beinhalteten Logischen Volumes einnimmt.
- *Benutzt*: Zeigt den Anteil des Speicherplatzes der Volume-Gruppe, der mit Daten gefüllt ist.
- *Verfügbar*: Zeigt den Anteil des Speicherplatzes der Volume-Gruppe, der noch zur Verfügung steht.

18.2.1.2 Tab *Volume-Gruppen*, Abschnitt *Physikalische Volumes*

Spalten in der Tabelle

- *Name*: Zeigt den Namen des physikalischen Volumes.
- *Gerät*: Zeigt den Gerätenamen des physikalischen Volumes.
- *Info*: Hier werden Details über den Geräteanschluss oder die Herstellerbezeichnung angezeigt.
- *Größe*: Hier wird die gesamte Größe des Geräts angezeigt.

Aktionen für jeden Tabelleneintrag

- *Entfernen*: Wird ein physikalisches Volume nicht von logischen Volumes benutzt und ist darauf kein Dateisystem vorhanden, kann das physikalische Volume mit dieser Aktion aus der Gruppe entfernt werden. Ein Detail-Formular wird geöffnet.

18.2.1.3 Tab *Volume-Gruppen*, Abschnitt *Logische Volumes* Spalten in der Tabelle

- *Name*: Hier wird der Name der logischen Volumes angezeigt. Auf Collax Servern ist das logische Volume „datavolume“ immer vorhanden.
- *Benutzt physikalisches Volume*: Zeigt an, auf welches physikalische Volume zugegriffen wird.
- *Verwendung*: Zeigt an, ob das logische Volume vom System oder von einer virtuellen Maschine benutzt wird.
- *Größe*: Zeigt die gesamte Größe des logischen Volumes an. Maximal kann die Größe des benutzten physikalischen Volumes eingenommen werden.

Aktionen für jeden Tabelleneintrag

- *Erweitern*: Steht innerhalb der Volume-Gruppe noch Speicherplatz zur Verfügung, kann der Speicherplatz einzelner logischer Volumes erweitert werden. Maximal kann das Volume um den Speicherplatz erweitert werden, der in der zugehörigen Volume-Gruppe als *Verfügbar* bezeichnet ist.
- *Entfernen*: Wenn das Volume weder vom System noch von einer virtuellen Maschine verwendet wird, kann es mit dieser Aktion entfernt werden. Ein Detail-Formular wird geöffnet.

18.2.1.4 Aktionen für diesen Abschnitt

- *Logisches Volume anlegen*: Steht weiterer Speicherplatz in der Volume-Gruppe zur Verfügung, kann mit dieser Aktion ein neues logisches Volume erzeugt werden.

18.2.1.5 Tab *Volume-Gruppe*, Abschnitt *Verfügbare Hardware*

Die Tabelle zeigt am Server angeschlossene Geräte, die zur Verwendung in Volume-Gruppen zur Verfügung stehen.

Spalten in der Tabelle

- *Name*: Hier wird der Name des Geräts angezeigt.
- *Gerät*: Zeigt die Systembezeichnung des Geräts an.
- *Info*: Zeigt weitere Informationen über das Gerät.
- *Größe*: Hier wird die gesamte Größe des Geräts angezeigt.

Aktionen für jeden Tabelleneintrag

- *Physikalisches Volume generieren*: Um das angezeigte Gerät im LVM-System verwenden zu können, kann hier ein physikalisches Volume generiert werden.

18.2.1.6 Tab *Festplatten*, Abschnitt *Blockgeräte*

Diese Tabelle zeigt alle dem Server vorhandenen blockorientierten Geräte.

Spalten in der Tabelle

- *Name*: Name des Geräts.
- *Gerät*: Zeigt die Systembezeichnung des Geräts an.
- *Typ*: Hier wird angezeigt, ob es sich bei dem Gerät um eine Partition, eine erweiterte Partition, ein Volume oder ein Gerät mit Dateisystem handelt. Ist das Feld leer, wurde kein darauf

vorhandenes Dateisystem erkannt, das Gerät wird dann in der Tabelle *Verfügbare Hardware* aufgelistet.
- *Info*: Detailinformation über das Gerät.
- *Größe*: Zeigt die Gesamtgröße des Geräts an.
- *Verwendung*: Hier wird angezeigt, ob das Gerät von einer Volume-Gruppe, vom Backup-System, von einer virtuellen Maschine oder vom Betriebssystem verwendet wird.

Aktionen für jeden Tabelleneintrag

- *Benutzen für ...*: Mit dieser Aktion kann das Gerät zu einer bestehender Volume-Gruppe hinzugefügt werden.
- *Initialisieren ...*: Wurde ein Gerät im System erkannt, das nicht verwendet wird und dessen Partitionen nicht verwendet werden, kann das Gerät mit dieser Aktion initialisiert werden. Nach der Initialisierung kann das Gerät von bestehenden Volume-Gruppen, vom Backup-System oder von virtuellen Maschinen verwendet werden.

  Hinweis: Diese Aktion löscht ohne Rückfrage jedwelche Daten, die auf dem Gerät vorhanden sind.
- *Aus Volume-Gruppe entfernen*: Wird das angezeigte Gerät als physikalisches Volume in einer Volume-Gruppe verwendet und besteht in der Volume-Gruppe ausreichend freier Speicherplatz, dann kann das Gerät aus der Volume-Gruppe entfernt werden. Bei dieser Aktion gehen keine Daten verloren. Der belegte Speicherplatz des ausgewählten Geräts wird bei dieser Aktion auf die anderen Geräte in der Volume-Gruppe verteilt.

18.2.1.7 Tab *Festplatten*, Abschnitt *Logische Volumes*

Diese Tabelle zeigt alle dem Server vorhandenen logischen Geräte an.

Spalten in der Tabelle

- *Gerät*: Systembezeichnung des Geräts.
- *Typ*: Zeigt an, ob es sich um ein Volumen mit erzeugtem Dateisystem handelt.
- *Info*: Detailinformation zum logischen Volume.
- *Größe*: Zeigt die Gesamtgröße des Volumes.

18.2.2 *Physikalisches Volume generieren*

In diesem Detailformular können Informationen kontrolliert, abschließend ein physikalisches Volume erzeugt oder der Dialog abgebrochen werden.

18.2.2.1 Abschnitt *Physikalisches Volume*
Felder in diesem Abschnitt

- *Gerätename*: Zeigt den Gerätenamen des ausgewählten Geräts zur Kontrolle.
- *Information*: Zeigt Detailinformationen zur Kontrolle.
- *Größe*: Zeigt die Gesamtgröße zur Kontrolle.
- *In Volume-Gruppe*: Zeigt zur Kontrolle die Volume-Gruppe, in der das physikalische Volume erzeugt werden soll.

18.2.2.2 Abschnitt *Hinweis*
Felder in diesem Abschnitt

- : Zeigt einen Hinweis zur Beachtung, bevor die Aktion ausgeführt wird.

18.2.2.3 Aktionen für dieses Formular

- *Abbrechen*: Beendet den Dialog, das physikalische Volume wird nicht erzeugt.
- *Generieren*: Beendet den Dialog, das physikalisch Volume wird erzeugt. Die Systemausgabe wird angezeigt.
- *Zurück*: Die Aktion führt zurück ins Hauptformular, die Systemausgabe wird beendet.

18.2.2.4 *Systemausgabe*
Felder in diesem Abschnitt

- : Zeigt die Ausgabe vom Systemprozess.

18.2.3 *Physikalisches Volume löschen*

In diesem Detailformular können Informationen kontrolliert, abschließend das physikalische Volume gelöscht oder der Dialog abgebrochen werden.

18.2.3.1 Abschnitt *Physikalisches Volume*
Felder in diesem Abschnitt

- *Gerät*: Zeigt den Gerätenamen zur Kontrolle.
- *Info*: Zeigt Detailinformationen zur Kontrolle.
- *Größe*: Zeigt die Gesamtgröße des Volumes.
- *Aus Volume-Gruppe*: Zeigt zur Kontrolle die Volume-Gruppe, aus der das physikalische Volume entfernt werden soll.

18.2.3.2 Abschnitt *Hinweis*
Felder in diesem Abschnitt

- : Zeigt einen Hinweis zur Beachtung, bevor die Aktion ausgeführt wird.

18.2.3.3 Aktionen für dieses Formular

- *Abbrechen*: Beendet den Dialog, das physikalische Volume wird nicht gelöscht.
- *Löschen*: Beendet den Dialog, das physikalische Volume wird gelöscht. Die Systemausgabe wird angezeigt.
- *Zurück*: Die Aktion führt zurück ins Hauptformular, die Systemausgabe wird beendet.

18.2.3.4 Abschnitt *Systemausgabe*
Felder in diesem Abschnitt

- : Zeigt die Ausgabe vom Systemprozess.

18.2.4 *Logisches Volume anlegen*
18.2.4.1 Abschnitt *Logisches Volume*
Felder in diesem Abschnitt

- *Name*: Hier wird der Name angegeben, unter dem das Volume intern verwaltet wird.
- *In Volume-Gruppe*: Zeigt zur Kontrolle die Volume-Gruppe, in der das logische Volume erzeugt werden soll.
- *Maximale Volume-Größe*: Zeigt die Größe an, mit der das Volume maximal erzeugt werden kann.
- *Größe*: Hier wird angegeben, wie viel Speicherplatz das Volume einnehmen soll.
- *Dateisystem anlegen (ext3)*: Mit dieser Wahl wird angegeben, ob auf dem neuen Volume das Journaling-Dateisystem EXT3 angelegt werden soll.

18.2.4.2 Aktionen für dieses Formular

- *Abbrechen*: Beendet den Dialog, das logische Volume wird nicht angelegt.
- *Anlegen*: Beendet den Dialog, das logische Volume wird erzeugt. Die Systemausgabe wird angezeigt.
- *Zurück*: Die Aktion führt zurück ins Hauptformular, die Systemausgabe wird beendet.

18.2.4.3 Abschnitt *Systemausgabe*

Felder in diesem Abschnitt

- : Zeigt die Systemausgabe vom Systemprozess.

18.2.5 *Logical Volume erweitern*

18.2.5.1 Abschnitt *Logisches Volume*

Felder in diesem Abschnitt

- *Name*: Zeigt den Gerätenamen zur Kontrolle.
- *In Volume-Gruppe*: Zeigt zur Kontrolle die zugehörige Volume-Gruppe.
- *Aktuelle Größe*: Zeigt die Größe an, die das Volume aktuell belegt.
- *Zusätzlich verfügbar*: Zeigt die Größe an, um die das Volume maximal erweitert werden kann.
- *Erweitern um*: Hier wird die Größe des Speicherplatzes eingetragen, um die das Volume erweitert werden soll.

18.2.5.2 Aktionen für dieses Formular

- *Abbrechen*: Beendet den Dialog, das logische Volume wird nicht erweitert.
- *Erweitern*: Beendet den Dialog, das logische Volume wird erweitert. Die Systemausgabe wird angezeigt.
- *Zurück*: Die Aktion führt zurück ins Hauptformular, die Systemausgabe wird beendet.

18.2.5.3 *Systemausgabe*
Felder in diesem Abschnitt

- : Zeigt die Ausgabe vom Systemprozess.

18.2.6 *Logisches Volume entfernen*
18.2.6.1 Abschnitt *Logisches Volume*
Felder in diesem Abschnitt

- *Name*: Zeigt den internen Namen des Volumes zur Kontrolle.
- *Volume-Gruppe*: Zeigt zur Kontrolle die Volume-Gruppe, aus der das logische Volume entfernt werden soll.
- *Größe*: Zeigt den belegten Speicherplatz. Wird das Volume gelöscht, steht dieser Platz der Volume-Gruppe zur Verfügung.

18.2.6.2 Abschnitt *Hinweis*
Felder in diesem Abschnitt

- : Hinweis zur Beachtung, bevor das Volume entfernt wird.

18.2.6.3 Aktionen für dieses Formular

- *Abbrechen*: Beendet den Dialog, das logische Volume wird nicht gelöscht.
- *Löschen*: Beendet den Dialog, das logische Volume wird gelöscht. Die Systemausgabe wird angezeigt.
- *Zurück*: Die Aktion führt zurück ins Hauptformular, die Systemausgabe wird beendet.

18.2.6.4 Abschnitt *Systemausgabe*

Felder in diesem Abschnitt

- : Zeigt die Ausgabe vom Systemprozess.

18.3 GUI-Referenz: *Shutdown und Reboot*

(Dieser Dialog befindet sich unter *Systembetrieb – Shutdown/Reboot – Allgemein*)

In diesem Dialog kann das System heruntergefahren oder neu gestartet werden. Hier wird zusätzlich die „Uptime“ angezeigt, d. h. die Zeitspanne seit dem letzten Neustart.

Hinweis: Nach 497 Tagen gibt es einen „Wrap-around“; durch einen Überlauf fängt die Uptime wieder bei Null an.

18.3.1 Felder in diesem Dialog

- *Uptime*: Die Laufzeit des Systems seit dem letzten Neustart.

18.3.2 Aktionen für diesen Dialog

- *System herunterfahren*: Mit dieser Aktion wird das System heruntergefahren.
- *System neu starten*: Mit dieser Aktion wird das System heruntergefahren und anschließend neu gestartet.

19 Systeminformationen

Der V-Cube bietet umfangreiche Möglichkeiten zur Analyse und Steuerung des gesamten Systems. Diese sind alle unter *System – Überwachung/Auswertung* zugänglich.

19.1 Systeminformationen

Unter *Status – Systeminformationen* ist die Auslastung von Prozessor, Hauptspeicher und Festplattenspeicher einsehbar. Wenn ein V-Cube sehr träge reagiert, sollte die Auslastung überprüft werden. Interessant ist die Angabe von *Load Average*. Hier wird die gemittelte Last des Systems in der letzten Minute, in den letzten 5 Minuten und in den letzten 15 Minuten angegeben. Diese Load gibt die Auslastung aller Kompontenten wieder. Ein Wert kleiner 1 besagt, dass das System zeitweise nicht ausgelastet war. Ein Wert größer 1 zeigt an, dass einzelne Prozesse auf die Zuteilung von Resourcen warten mussten. Der Betrieb ist bis zu einer Load von ca. 4 problemlos möglich. Liegt die Load darüber, müssen geeignete Maßnahmen ergriffen werden. Die Load selbst kann bis in den dreistelligen Bereich steigen, wobei dann die Antwortzeiten eines Systems sehr groß werden.

Eine Möglichkeit zur genaueren Untersuchung der Load findet sich unter *Auswertungen – Systemstatistik* . Hier können bis zu sechs Parameter des Systems grafisch dargestellt und verglichen werden. Dabei kann das Zeitfenster der Anzeige in verschiedenen Stufen von vier Stunden bis zu einem Jahr eingestellt werden. Durch die Darstellung der Graphen übereinander lassen sich Zusammenhänge zwischen einzelnen Parametern herstellen.

19.2 Dienste

Alle im V-Cube vorhandenen Dienste sowie deren jeweiliger Zustand lassen sich unter *Status – Dienste* einsehen. Der Status jeden Dienstes wird zudem durch eine Ampel (rot bzw. grün für nicht laufend bzw. laufend) dargestellt.

Durch Anklicken dieser Ampel kann ein Dienst in den jeweils anderen Zustand geschaltet werden. Dienste, die noch nicht ausreichend konfiguriert sind, werden eventuell nicht starten. Diese Änderungen sind nur temporär und gehen mit dem Neustart des Systems verloren.

Wichtige Dienste, wie der Apache-Webserver (der die GUI bedient) oder der LDAP-Server (der die Benutzerkonten bereitstellt), sollten nicht grundlos deaktiviert werden, da dadurch der Zugriff auf den V-Cube erschwert wird.

Generell ist diese Seite als Übersicht gedacht, welche Dienste aktuell laufen. In seltenen Fällen können hier einzelne Dienste neu gestartet werden. Um Dienste dauerhaft zu (de-)aktivieren, muss in deren jeweiliger Konfiguration die Option *Aktivieren* entsprechend gesetzt werden.

19.3 Netzwerkstatus

Unter *Status – Link-Status* sind alle angelegten Links aufgelistet. Neben dem Typ und der gesetzten IP-Adresse werden die Zählerstände der ein- und ausgehenden Byte- und Paketzähler angezeigt. Durch Anklicken des *Namens* öffnet sich ein weiteres Fenster, in dem eine Byte-Statistik des jeweiligen Links grafisch angezeigt wird. Dabei werden Graphen für die letzte Stunde, den letzten Tag sowie die gesamte Woche angezeigt.

Zu jedem Link wird der *Status* angezeigt. Mögliche Werte sind „Ok“, „Disabled“ und „Broken“. Der Status „Broken“ zeigt eine Störung an, etwa wenn ein Netzwerkkabel keine Verbindung hat oder wenn die Einwahl zu einer Gegenseite fehlgeschlagen ist. Mit der Ampel können analog zu den Diensten einzelne Links deaktiviert und neu gestartet werden. Auch diese Änderungen sind nur temporär, d. h. bis zum nächsten Neustart gültig.

Wird der V-Cube als DHCP-Server eingesetzt, sind unter *Status – DHCP-Leases* alle per DHCP vergebenen IP-Adressen sowie deren Laufzeit einsehbar.

19.4 Mailqueue

Alle vom V-Cube erzeugten und empfangenen E-Mails werden vor der weiteren Zustellung in die Mailqueue aufgenommen. Wenn die Zustellung durch einen temporären Fehler fehlschlägt (wenn der Zielserver beispielsweise nicht erreichbar ist), verbleiben die E-Mails bis zu fünf Tage in der Mailqueue, bevor sie mit einer Fehlermeldung an den Absender zurückgeschickt werden.

Die Filtermechanismen für E-Mail im V-Cube werden auf alle neuen E-Mails in der Mailqueue angewandt. Ist eine E-Mail „sauber“, wird sie weiter zugestellt. Erkennt ein Filter eine E-Mail als unerwünscht, wird sie abhängig von der Einstellung des Filters aus der Mailqueue gelöscht, in Form einer neuen E-Mail an den Absender zurückgeschickt oder in der Mailqueue angehalten.

Der aktuelle Inhalt der Mailqueue kann unter *Status – Mail-Queue* eingesehen werden. Für jede E-Mail wird die Message-ID, der Zeitpunkt, zu dem sie in die Mailqueue kam, der aktuelle Status sowie die Adressen von Absender und Empfänger angezeigt.

Die Message-ID ist wichtig, um in den Logdateien alle Meldungen zu dieser E-Mail aufzufinden. Durch Anklicken der Message-ID wird ein Fenster geöffnet, in dem alle relevanten Einträge in der Logdatei zu dieser Mail angezeigt werden.

Der Status einer E-Mail zeigt an, warum sich diese E-Mail noch in der Mailqueue befindet. „Verzögert“ bedeutet, dass eine Zustellung aufgrund eines Fehlers nicht möglich war. Es erfolgen aber in wachsenden Zeitabständen erneute Zustellversuche. Wurde eine E-Mail beispielsweise durch einen Filter blockiert, ist der Zustand „Angehalten“. In diesem Fall muss die E-Mail über *Auswahl* markiert und dann mit *Löschen* entfernt oder mit *Freigeben* zugestellt werden.

Ist der V-Cube so konfiguriert, dass E-Mails nicht sofort ausgeliefert

werden, kann über den Schalter *Jetzt versenden* eine Auslieferung allur E-Mails erzwungen werden. Analog werden mit *Jetzt abholen* alle Abholaufträge für externe Postfächer gestartet.

19.5 Auswertungen

Die Auswertungen werden nachts aus den Logdateien erstellt. Um eine manuelle Auswertung auszulösen, kann *Jetzt aktualisieren* angeklickt werden.

Abgesehen von dienstespezifischen Details zeigen die Auswertung die Verteilung des Datenvolumens über einzelne Zeiträume. Zudem sind die „Top 10“ der Anwender sowie der besuchten Adressen sichtbar. Dazu kann auch jeweils eine vollständige Liste abgerufen werden.

19.6 System-Logdateien

Viele wichtige Dienste im V-Cube protokollieren ihre Ereignisse in einer zentralen Logdatei, der Syslog-Datei. Auf die Inhalte dieser Datei kann über die Weboberfläche unter *Logdateien* zugegriffen werden. Verschiedene Filter stehen zur Verfügung, um die gesuchte Information zu erhalten.

Zunächst kann der Zeitraum ausgewählt werden, üblicherweise werden Einträge von heute oder gestern gesucht. Es kann aber auch ein konkretes Datum angegeben werden (vorausgesetzt, von dem Zeitpunkt existieren Logdatei-Einträge; dies hängt von der Haltezeit der Logdateien ab).

Als nächstes kann das „Subsystem“ ausgewählt werden, von dem die Einträge gezeigt werden sollen. Folgende Subsysteme existieren:

Kategorien der Logdateien

Kategorie	Details
mail	E-Mail-System mit SMTP-Server postfix und POP/IMAP-Server cyrus.
kernel	Meldungen des Betriebssystemkerns.
firewall	Abhängig von ihrer Einstellung protokolliert die Firewall verschiedene Pakete/Verbindungen.
daemon	Alle Dienste, die keine eigene Kategorie zugeteilt bekommen haben, protokollieren in dieser Kategorie.
auth	Alle Meldungen über Anmeldungen am V-Cube werden hier erfasst, auch fehlgeschlagene.
syslog	Meldungen über den Systemstatus.
cron	Cron ist die interne Zeitsteuerung des V-Cubes. Hier werden alle Rückmeldungen dieses Dienstes ausgegeben.
ftp	Meldungen des FTP-Servers.

Über das Feld *Programm* können noch die Ausgaben eines einzelnen Dienstes gefiltert werden, etwa „fetchmail“ oder „pluto“.

Die Ausgabe kann entweder im *Textformat* oder in Form einer HTML-Tabelle erfolgen. In der HTML-Variante wird über die Farben grün, gelb und rot die Wichtigkeit der Meldung visualisiert.

19.7 GUI-Referenz: Status

19.7.1 *Systeminformationen*

(Dieser Dialog befindet sich unter *Überwachung/Auswertung – Status – Systeminformationen*)

19.7.1.1 Tab *Status/CPU*, Abschnitt *Status*

Felder in diesem Abschnitt

- *Uptime*: In diesem Feld wird von links nach rechts die aktuelle Systemzeit in der lokalen Zeitzone, die Laufzeit seit dem letzten Neustart des Systems, die Anzahl der über die Konsole angemeldeten Benutzer sowie die durchschnittliche Systemlast der letzten Minute, der letzten fünf Minuten und der letzten 15 Minuten angezeigt.

19.7.1.2 Tab *Status/CPU*, Abschnitt *Graphen*

In diesen Graphen werden CPU-Auslastungen dargestellt.

Felder in diesem Abschnitt

- *CPU-Graphen*: Auslastungen der CPU innerhalb der letzten vier Stunden werden hier in Bezug auf Systemprozesse, virtuellen Maschinen und Dienste dargestellt. Die Aktualisierung geschieht minütlich.

19.7.1.3 Tab *RAM*, Abschnitt *Graphen*
Felder in diesem Abschnitt

- *Speicherbelegung*: Hier wird die Systembenutzung des Hauptspeichers (RAM) der letzten vier Stunden angezeigt. Die Graphik wird minütlich aktualisiert.

19.7.1.4 Tab *Dateisystem*, Abschnitt *Graphen*
Felder in diesem Abschnitt

- *Dateisystem*: Hier wird die Benutzung der Wurzel- und der Datenpartition der letzten vier Stunden angezeigt. Ebenso wird anteilig die Benutzung der Datenpartition von Diensten grafisch dargestellt. Die Graphik wird minütlich aktualisiert.

19.7.1.5 Tab *Festplatten*, Abschnitt *Graphen*
Felder in diesem Abschnitt

- *Festplatten*: Hier werden die Ein- und Ausgabedetails angeschlossener Festplatten dargestellt. Die Graphik wird minütlich aktualisiert.

19.7.1.6 Tab *Netzwerk*, Abschnitt *Graphen*
Felder in diesem Abschnitt

- *Netzwerk*: Hier werden die Ein- und Ausgabedetails angeschlossener Netzwerkschnittstellen dargestellt. Dies betrifft physikalische Ethernet-Geräte aber auch Bridges. Die Graphik wird minütlich aktualisiert.

19.7.1.7 Tab *Virtuelle Maschinen*, Abschnitt *Graphen*
Felder in diesem Abschnitt

- *Virtuelle Maschinen*: Hier werden sämtliche Details angelegter virtueller Maschinen grafisch aufgezeichnet. Die Graphik wird minütlich aktualisiert.

19.7.2 *Dienste*

(Dieser Dialog befindet sich unter *Überwachung/Auswertung – Status – Dienste*)

Dieser Dialog zeigt alle wichtigen Dienste auf dem V-Cube und ihren aktuellen Status an. Die Dienste können hier gestoppt und gestartet werden.

19.7.2.1 Felder in diesem Dialog

- *Subsystem*: Hier wird das übergeordnete System angezeigt, zu dem der Dienst gehört.
- *Dienst*: Hier wird der Name des Dienstes angezeigt.
- *Status*: Hier wird der Status des Dienstes angezeigt. „Running“ bedeutet, dass der Dienst aktiviert ist und läuft, „stopped“ hingegen, dass der Dienst in der Konfiguration aktiviert ist, der Dienst jedoch aus unbestimmtem Grund gestopped wurde.
- *Test*: In dieser Spalte wird das Ergebnis aufgrund eines qualitativen Tests angezeigt. So kann hier z.B. als Ergebnis CRITICAL angezeigt werden, auch wenn der Status „Running“ ist. Das hier angezeigt Testergebnis entspricht dem der aktivien Überwachung.

19.7.2.2 Aktionen für jeden Tabelleneintrag

- *Start*: Um einen Dienst zu starten, muss über das Kontextmenü (rechter Mausklick) „Start“ angeklickt werden.
- *Stop*: Um einen Dienst zu beenden, muss über das Kontextmenü (rechter Mausklick) „Stop“ angeklickt werden.

19.7.3 *Link-Status*

(Dieser Dialog befindet sich unter *Überwachung/Auswertung – Status – Link-Status*)

Hier wird der Status der einzelnen Netzwerklinks angezeigt.

19.7.3.1 Felder in diesem Dialog

- *Name*: Hier steht der Name des Links.
- *Typ*: Hier steht der zugehörige Link-Typ.
- *IP-Adresse*: Hier wird die IP-Adresse des Systems angegeben, die auf dem jeweiligen Link gesetzt ist.
- *Bytes In/Out*: In diesem Feld wird das über diesen Link übertragene Datenvolumen angezeigt.

  Hinweis: In dieser Angabe wird mit 1000 Bytes = 1 KByte und 1000 KBytes = 1 MByte gerechnet (statt jeweils 1024).
- *Pakete In/Out*: In diesem Feld wird die Anzahl der bisher auf diesem Link empfangenen und gesendeten Pakete angegeben.
- *Status*: Hier wird der Status des Links angezeigt. Mögliche Zustände der Links sind „OK“, „Not established“ und „Disabled“.

19.7.3.2 Aktionen für jeden Tabelleneintrag

- *Deaktivieren*: Ist der Link aktiviert, wird ein grüner Schalter angezeigt. Über diesen kann der Link deaktiviert werden, so dass keine weiteren Daten übertragen werden.
- *Restart*: Mit dieser Aktion kann ein Link gestoppt werden. Der Neustart erfolgt im Anschluss automatisch.
- *Aktivieren*: Bei einem deaktivierten Link wird ein roter Schalter angezeigt. Über diesen kann der Link aktiviert werden.

19.7.3.3 Aktionen für diesen Dialog

- *Zurücksetzen*: Mit dieser Aktion werden die Zähler für Datenvolumen und Pakete zurückgesetzt.

19.7.4 *Ethernet-Status*

(Dieser Dialog befindet sich unter *Überwachung/Auswertung – Status – Ethernet-Status*)

In diesem Formular können Detailinformationen über den Ethernet-Status eingesehen werden. Zunächst kann im Graph eine schematische Abbildung der lokalen Schnittstellen und deren Verbindung zu den anliegenden Geräten eingesehen werden. Weitere Details können in der Liste für jedes einzelne Ethernet-Gerät abgerufen werden.

19.7.4.1 *Ethernet-Status*

Tab *Graph*

In diesem Schaubild sind die Netzwerkschnittstellen abgebildet. Zudem werden verbundene Geräte, wie Switch oder andere Server, gezeigt. Ist eine Schnittstelle rot umrandet, ist diese nicht verbunden oder wird nicht verwendet.

Tab *Liste*

Spalten in der Tabelle

- *Name*: Zeigt den Namen der Ethernet-Schnittstelle.
- *Art*: Zeigt die Art der Schnittstelle. Es gibt physikalische Schnittstellen und logische Schnittstellen. Zu den logischen Schnittstellen gehören VLAN, MAC-Vlan, Ethernet-Bond, Bridge oder die Loopback-Schnittstelle.
- *Status*: Zeigt den Status. Wird eine Schnittstelle verwendet hat diese den Status *up*. Bei *unknown* liegen momentan keine Informationen für die Schnittstelle vor.
- *MAC-Adresse*: Zeigt die Hardware-Adresse. Eine oder mehrere logischen Schnittstellen dürfen dieselbe MAC-Adresse besitzen, insofern keine spezielle konfiguriert wurde.

Aktionen für jeden Tabelleneintrag

- *Detail*: Per Doppelklick oder Rechter-Maus-Klick können die Details mit dieser Aktion abgerufen werden.

19.7.4.2 *Ethernet-Status (Detail)*

Tab *Grundlagen*

Hier werden die grundlegenden Informationen zur Schnittstelle angezeigt.

Tab *Grundlagen*, Abschnitt *VLAN*

Hier werden die grundlegenden Informationen zu VLAN angezeigt.

Tab *Grundlagen*, Abschnitt *Bündel*

Hier werden die grundlegenden Informationen zu einer Bonding-Schnittstelle angezeigt.

Tab *Grundlagen*, Abschnitt *Bridge Port*

Hier werden die grundlegenden Informationen zu einer Bridge angezeigt.

Tab *Grundlagen*, Abschnitt *IPv4 Adresse*

Hier werden die grundlegenden Informationen zu einer IPV4-Adresse angezeigt.

Tab *VLANs*, Abschnitt *VLAN*

Hier werden die grundlegenden Informationen zu VLAN angezeigt.

Tab *STP*

Hier werden die grundlegenden Informationen zu STP angezeigt.

Tab *Ports*, Abschnitt *Port* Abschnitt *MACs*

Hier werden die grundlegenden Informationen zu verwendeten Ports angezeigt.

Tab *Gegenstelle*, Abschnitt *Port*

Hier werden die grundlegenden Informationen zum Port der Gegenstelle angezeigt.

Tab *Gegenstelle*, Abschnitt *Gerät*

Hier werden die grundlegenden Informationen zum Gerät der Gegenstelle angezeigt.

Tab *Gegenstelle*, Abschnitt *Inventory*

Hier werden die grundlegenden Informationen zum Inventar der Gegenstelle angezeigt.

Aktionen für dieses Formular

- *Zurück*: Beendet den Dialog und führt zurück zur Übersicht.

19.7.5 *DHCP-Leases*

(Dieser Dialog befindet sich unter *Überwachung/Auswertung – Status – DHCP-Leases*)

In diesem Dialog wird angezeigt, welche IP-Adressen per DHCP an welche Rechner vergeben wurden.

19.7.5.1 Felder in diesem Dialog

- *IP-Adresse*: Hier wird die vergebene IP-Adresse angezeigt.
- *Hostname*: Hier wird der Hostname des angemeldeten Rechners aufgeführt.
- *MAC-Adresse*: Hier ist die Ethernet-MAC-Adresse des Rechners aufgeführt, an den die IP-Adresse zuletzt vergeben wurde.
- *Vergeben seit*: Zeigt an, wann die IP-Adresse zugewiesen wurde.
- *Vergeben bis*: Zeigt an, bis wann die IP-Adresse vergeben ist. Der DHCP-Server behält bereits abgelaufene Leases auch dann noch, wenn der Rechner die IP-Adresse nicht mehr weiter benutzt. Daher kann hier ein Zeitpunkt in der Vergangenheit angezeigt werden.
- *Status*: Zeigt den Status der DHCP-Lease an. Eine IP-Adresse ist normalerweise entweder als *free* oder *active* markiert. *Active* bedeutet, dass die Adresse benutzt wird und daher nicht bei einer DHCP-Anfrage vergeben wird. Als *free* wird eine IP-Adresse markiert, die bei einer DHCP-Anfrage neu vergeben werden kann.

  Der Status *conflict* bedeutet, dass der Server diese Adresse per DHCP vergeben wollte, aber ein anderer Rechner im Netz diese IP-Adresse benutzt oder zum Zeitpunkt des Versuchs benutzt hat.

  In der Regel werden zunächst solange neue IP-Adressen aus dem Adresspool vergeben, bis keine weiteren Adressen mehr zur

Verfügung stehen. Erst danach beginnt der DHCP-Server, bereits benutzte IP-Adressen neu zu vergeben.

19.7.6 GUI-Referenz: *eSAN-Ressourcen*

(Dieser Dialog befindet sich unter *System – Überwachung/Auswertung – Status – eSAN-Ressourcen*)

19.7.6.1 *eSAN-Ressourcen*

Hier wird eine Liste aller eSAN-Ressourcen und deren Status auf diesem Server angezeigt. In dieser Übersicht ist neben der lokalen Rolle der eSAN-Ressources auch der Verbindungszustand zum anderen Server sowie der Gerätename ersichtlich. Im funktionierenden Zustand ist die Rolle *Primary* und der Verbindungsstatus *Connected*.

Spalten in dieser Tabelle

- *Name*: Zeigt den Namen der einzelnen eSAN-Ressourcen.
- *Rolle*: Zeigt die lokale Rolle an. Im Normalzustand sollte der Wert *Primary* gezeigt werden, was bedeutet, dass das Gerät produktiv beschrieben werden kann. *Secondary* bedeutet, dass das Gerät nicht produktiv beschrieben werden kann, die Daten sind jedoch synchroniseirt.
- *Verbindung*: Zeigt an, ob die Synchronisationsverbindung besteht oder unterbrochen ist. Im Normalzustand ist der Verbindungszustand *Connected*.
- *Device-Name*: Zeigt den internen Gerätenamen an, welches im Cluster-Verbund weiter verwendet wird.

Aktionen für jeden Tabelleneintrag

- *Status*: Öffnet den Detail-Dialog.

19.7.6.2 *Ressource Status*

Abschnitt 1
Felder in diesem Abschnitt

- *Name*: Zeigt den Namen der eSAN-Ressource an.
- *Device name*: Zeigt den internen Gerätenamen, der durch den Cluster Manager verwendet wird.
- *Lokale Festplatte*: Zeigt den Gerätenamen des verwendeten Logischen Volume.

Abschnitt *Ausgabe*
Felder in diesem Abschnitt

- *Ausgabe*: Hier werden Details der initiierten Aktion ausgegeben.

Abschnitt *Status*
Felder in diesem Abschnitt

- *Verbindungszustand*: Zeigt an, ob die Synchronisationsverbindung besteht oder unterbrochen ist. Im Normalzustand ist der Verbindungszustand *Connected*.
- *Lokale Rolle*: Zeigt die lokale Rolle an. Im Normalzustand sollte der Wert *Primary* gezeigt werden, was bedeutet, dass das Gerät produktiv beschrieben werden kann. *Secondary* bedeutet,

dass das Gerät weder gelesen noch beschrieben werden kann. Die Daten sind jedoch synchronisiert, solange eine Verbindung besteht.

- *Remote-Rolle*: Wenn abrufbar wird die Rolle der Ressource auf der Gegenseite angezeigt. Im Normalzustand sollte der Wert *Primary* gezeigt werden, was bedeutet, dass das Gerät produktiv beschrieben werden kann. *Secondary* bedeutet, dass das Gerät weder gelesen noch beschrieben werden kann. Die Daten sind jedoch synchronisiert, solange eine Verbindung besteht. *Unknown* wird nur für die Gegenstelle angezeigt, wenn die Verbindung unterbrochen ist.
- *Lokaler Disk-Status*: Der lokale Disk-Status ist im Normalzustand *UpToDate*, die Daten sind somit konsistent und aktuell. <Mehr ...>
- *Remote-Disk-Status*: Der lokale Disk-Status ist im Normalzustand *UpToDate*, die Daten sind somit konsistent und aktuell. Wenn die Verbindung unterbrochen ist, wird der Status *DUnknown* angezeigt. <Mehr ...>
- *Nutzbare Grösse*: Zeigt die Gesamtgröße der Ressource an.
- *Benutzter Platz*: Zeigt den benutzten Speicherplatz der Ressource an.
- *Fortschritt (%)*: Zeigt während der Synchronisation den Fortschritt an.

Aktionen für diesen Abschnitt

- *Wechsle zu Primär*: Mit dieser Aktion kann die lokale Rolle auf Primär gesetzt werden. Die Rolle kann nur geändert werden, wenn die lokale Rolle Secondary ist.
- *Wechsle zu Primär (forciert)*: Diese Aktion ist während einem Bare-Metal-Restore auszuführen und erzwingt einen Rollenwechsel auf Primary.

- *Wechsle zu Sekundär*: Diese Aktion ändert die lokale Rolle von Primary auf Secondary.
- *Lokale Kopie ungültig machen (outdate)*: In der lokalen Rolle Secondary kann die eSAN-Ressource ungültig gemacht werden. Später wird versucht, die Daten von der Gegenseite zu synchronisieren.
- *Verbinden*: Hier kann eine unterbrochene Verbindung wieder hergestellt werden.
- *Verbindung lösen*: Falls die Gegenseite dies zulässt, kann mit dieser Aktion die Verbindung unterbrochen werden.
- *Festplatte anbinden*: Ist der Disk-Status auf Diskless, kann mit dieser Aktion das referenzierte lokale Logische Volume angebunden werden.
- *Festplattenbindung lösen*: Diese Aktion löst das lokale Logische Volume von der eSAN-Ressource ab. Der Disk-Status wechselt dann auf Diskless.
- *Ressource starten*: Hiermit kann die eSAN-Ressource gestartet werden.
- *Ressource stoppen*: Hiermit kann die eSAN-Ressource beendet werden.

Aktionen für dieses Formular

- *Status auffrischen*: Hiermit wird der Dialog aktualisiert und die neuen Statuswerte werden eingelesen.
- *Zurück*: Führt zurück in die Übersicht.

19.7.7 *USV-Status*

(Dieser Dialog befindet sich unter *Überwachung/Auswertung – Status – USV-Status*)

19.7.7.1 Abschnitt *Status*

Hier wird der Status einer angeschlossenen USV angezeigt.

Felder in diesem Abschnitt

Mit einem Klick auf den Namen der angelegten USV werden weitere Informationen zu dem Gerät angezeigt.

19.7.7.2 Abschnitt *Hinweis*

Felder in diesem Abschnitt

- *Auf diesem System ist noch keine USV eingerichtet. Daher ist hier kein Status abrufbar*: Hier werden detaillierte Informationen über die ausgewählte USV angezeigt. Mit der Aktion *Back to Overview* wird wieder die gesamte Liste angezeigt.

19.7.8 *Status Aktive Überwachung*

(Dieser Dialog befindet sich unter *Überwachung/Auswertung – Status – Aktive Überwachung*)

In diesem Dialog wird der Status der aktiven Überwachung angezeigt. Intern verwendet das System dazu *Nagios*, dessen Web-GUI

hier eingeblendet wird. In dem Menü auf der linken Seite können verschiedene Informationen und Statistiken abgerufen werden.

Wichtig ist das *Tactical Overview*, welches auf einen Blick den Zustand der überwachten Computer (*Hosts*) und Dienste (*Services*) anzeigt. Interessant ist auch die *Status Map*, in der alle Hosts auf einen Blick erfasst werden können. Zudem visualisiert diese Übersicht die Abhängigkeiten der Systeme untereinander.

Die Konfiguration der einzelnen Hosts und der geprüften Dienste auf jedem Host wird in den Einstellungen des jeweiligen *Hosts* vorgenommen.

19.7.9 *Mail-Queue*

(Dieser Dialog befindet sich unter *Überwachung/Auswertung – Status – Mail-Queue*)

Alle eingehenden E-Mails werden in der Mailqueue, einer Warteschlange, zwischengespeichert. Sie sind vorweg durch eingeschaltete Filter geprüft worden. Von hier aus erfolgt die weitere Zustellung in einzelne Postfächer oder an andere Server. Ist eine *Wartezeit beim Versand* eingestellt, oder kommt es zu Problemen beim Versand, etwa weil ein anderer Mailserver nicht erreichbar ist, werden die E-Mails weiter in der Mail-Queue aufbewahrt. Das System unternimmt in regelmäßigen Abständen weitere Versuche, die E-Mails zuzustellen.

19.7.9.1 Spalten in der Tabelle

- *ID*: Dieses Feld enthält die Message-ID, unter der die E-Mail im Mailsystem verwaltet wird.

  Durch das Anklicken der Message-ID öffnet sich ein neues

Fenster, welches alle Einträge zu dieser E-Mail aus der Logdatei anzeigt.

- *Empfangen*: Diese Spalte zeigt den Zeitpunkt an, an dem die E-Mail beim System eingeliefert wurde. Dies gilt auch für E-Mails, die auf dem System selbst erzeugt wurden.
- *Status*: In dieser Spalte wird der aktuelle Status der E-Mail angezeigt. Mögliche Werte sind:

  E-Mails im Zustand *Deferred* versucht das System noch zuzustellen. Entweder ist eine Wartezeit beim Versand eingestellt, oder der Mailserver des Empfängers bzw. der nächste Mailserver auf dem Weg dorthin kann die E-Mail im Moment nicht verarbeiten.

  E-Mails im Zustand *Active* werden momentan zugestellt. Eine E-Mail sollte sich eigentlich nur kurz in diesem Zustand befinden. Zu Zeitpunkten mit hohem Mailaufkommen kann es vorkommen, dass einige E-Mails mit diesem Zustand in der Mailqueue verweilen. Besteht dieser Zustand über einen längeren Zeitraum, liegt oft eine Störung im Mailsystem vor, und die Mail-Logdatei sollte auf mögliche Probleme hin untersucht werden.
- *Absender*: In dieser Spalte wird die die E-Mail-Adresse des Absenders angezeigt.
- *Absender-Domain*: In dieser Spalte wird die Domain des Absenders angezeigt.
- *Empfänger*: Hier werden die E-Mail-Adressen der Empfänger angezeigt. Mehrere Empfänger sind durch Kommata getrennt.
- *Empfänger-Domain*: In dieser Spalte werden die Domains der Empfänger angezeigt.
- *Kommentar*: Falls der Versand der E-Mail verzögert wurde, enthält dieses Feld die genaue Ursache der Verzögerung.

19.7.9.2 Aktionen für diesen Dialog

- *Aktualisieren*: Mit dieser Aktion wird der aktuelle Stand der Warteschlange angezeigt. Bisher als *aktiv* markierte E-Mails sollten dann aus der Warteschlange verschwunden (zugestellt) oder in einen anderen Status übergegangen sein.
- *Alle E-Mails löschen*: Mit dieser Aktion werden alle E-Mails aus der Mailqueue ohne Rückfrage gelöscht. Diese Aktion kann erforderlich sein, falls nach ausführen von *Zustellen* oder *Requeue* E-Mails in der Mail-Queue verbleiben, die aufgrund eines Fehlers nicht zustellbar sind.
- *Zustellen*: Mit dieser Aktion wird das Zustellen aller versandfertigen E-Mails veranlasst. E-Mails werden ohne Berücksichtigung der Wartezeit versendet.
- *Requeue*: Mit dieser Aktion wird ein erneuter Zustellversuch angestoßen und alle E-Mails durchlaufen nochmals die Filterkette. Es ist dadurch möglich, dass E-Mails nochmals ausgefiltert und somit angehalten werden. Zusätzlich werden Zähler des Mailsystems zurückgesetzt. Üblicherweise ist diese Aktion nur dann erforderlich, falls Einstellungen des Servers verändert wurden, um den E-Mail-Transport zu verbessern.

19.8 GUI-Referenz: Auswertungen

19.8.1 *Systeminformationen*

(Dieser Dialog befindet sich unter *Überwachung/Auswertung – Auswertungen – Systemstatistik*)

Das System ermittelt zur Laufzeit verschiedene statistische Angaben und speichert diese für einen Zeitraum von einem Jahr ab. Über diesen Dialog sind graphische Auswertungen dieser Daten abrufbar.

Zunächst muss unter *Zeige Daten für* ausgewählt werden, für welchen Zeitraum die Grafiken erstellt werden sollen. Wird *für eine Woche* oder *für einen Monat* gewählt, erscheint ein weiteres Feld, in dem die Woche oder der Monat festgelegt werden können.

Unter *Zeige Graphen für* wird das Subsystem ausgewählt, für welches die Grafik erstellt wird. Zum Vergleich können weitere Subsysteme ausgewählt werden.

19.8.1.1 Tab *Graphen*, Abschnitt *Graphen*
Felder in diesem Abschnitt

- *1. Graph*: Hier wird der Graph des ausgewählten Subsystems angezeigt. Es können bis zu sechs Graphen angezeigt und verglichen werden.

19.8.2 *FTP*

(Dieser Dialog befindet sich unter *Überwachung/Auswertung – Auswertungen – FTP*)

Hier sind die Auswertungen für den FTP-Server abrufbar.

19.8.2.1 Abschnitt *Hinweis*

Felder in diesem Abschnitt

- *Die Logauswertung ist nicht aktiviert*: Damit die Logauswertung genutzt werden kann, muss sie bei der Konfiguration der entsprechenden Dienste aktiviert werden. Die Logauswertung ist verfügbar für die Dienste HTTP, FTP, Mail und HTTP-Proxy.

19.8.2.2 Abschnitt *Auswertungen für ...*

Felder in diesem Abschnitt

- *Auswertungen für ...*: Hier wird der Dienst ausgewählt, für den die Logauswertung angezeigt werden soll.

  Hinweis: Bei der FTP-Auswertung werden nur Transaktionen angezeigt. Anmeldungen am FTP-Server ohne Transaktionen werden nicht angezeigt.

19.8.2.3 Aktionen für diesen Dialog

- *Anzeigen*: Zeigt die Auswertung an.

19.8.3 *System-Logdateien*

(Dieser Dialog befindet sich unter *Überwachung/Auswertung – Logdateien – System-Logdateien*)

19.8.4 Felder in diesem Dialog

- *Livelog*: Mit dieser Option kann die gewünschte Logdatei im Livelog-Modus angezeigt werden. Der „Follow-Mode“ ermöglicht es, die neuesten Systemmeldungen zu verfolgen.
- *Datum*: Hier wird eingestellt, aus welchem Zeitraum die Einträge aus der Logdatei angezeigt werden sollen. Über *andere* kann ein frei definierbarer Zeitraum angezeigt werden.
- *Stunde(n)*: Hier wird eingestellt, wie viele Stunden rückwirkend die angezeigte Logdatei reichen soll.
- *Ab Datum*: Hier kann ein Anfangsdatum für die Anzeige vorgegeben werden. Bleibt das Feld leer, startet die Anzeige mit dem ersten Eintrag in der Logdatei.
- *Ab Uhrzeit*: Hier kann eine Startzeit für die Anzeige vorgegeben werden. Bleibt das Feld leer, startet die Anzeige mit dem ersten Eintrag in der Logdatei.
- *Bis Datum*: Hier wird das Datum angegeben, bis zu dem Einträge angezeigt werden sollen. Bleibt das Feld leer, werden alle Einträge bis zum Ende der Logdatei angezeigt.
- *Bis Uhrzeit*: Hier kann die Zeit angegeben werden, bis zu der die Daten angezeigt werden.
- *Subsystem*: Die Anzeige der Logdateien kann auf einzelne *Subsysteme* beschränkt werden. Wird kein Subsystem ausgewählt, werden die Informationen von allen Subsystemen angezeigt.
- *Programm*: Mit diesem Feld kann auf die Logdatei ein Filter

angewandt werden, der nur Einträge von einer bestimmten Software anzeigt.
- *Message-ID*: Wenn als Subsystem *Mail* ausgewählt wurde, kann mit diesem Filter die Anzeige auf Einträge zu einer bestimmten Message-ID eingeschränkt werden.
- *Textformat benutzen*: Wird diese Option aktiviert, erfolgt die Ausgabe als Text und nicht als HTML-Tabelle. Manche Browser haben Probleme mit der Darstellung von großen Tabellen, in diesen Fällen sollte die Option aktiviert werden.

19.8.5 Aktionen für diesen Dialog

- *Anzeigen*: Zeigt die Einträge in der Logdatei an.
- *Download*: Startet einen Download der Logdateieinträge.

19.8.6 Logdateikonfiguration

Für die einzelnen Logdateien im System kann eingestellt werden, nach welcher Zeitspanne sie jeweils „rotiert“ werden. Dabei wird die aktuelle Logdatei umbenannt und eine neue, leere Logdatei erstellt. Durch entsprechende Umbenennung aller gespeicherten Logdateien bleibt eine Historie der letzten Tage oder Wochen zur Fehleranalyse vorhanden.

Dabei kann eingestellt werden, wie viele Logdateien aufbewahrt bleiben sollen. Wird beispielsweise wöchentlich rotiert und werden vier Dateien aufgehoben, sind neben der aktuellen Logdatei die Dateien der letzten vier Wochen vorhanden. Die älteste davon wird nach Ablauf einer weiteren Woche gelöscht.

19.8.6.1 *System-Log*

(Dieser Dialog befindet sich unter *Logkonfiguration – System-Logs*)

Felder in diesem Dialog

- *System-Log neu anlegen*: Hier wird eingestellt, nach welcher Zeitspanne die System-Logdateien „rotiert“ werden.
- *Sicherungskopien vorheriger System-Logs*: In diesem Feld wird eingestellt, wie viele alte Versionen der Logdatei aufbewahrt werden.
- *Über Netzwerk loggen*: Durch das Aktivieren dieser Option kann auf einen „Syslog-Server“ im Netzwerk protokolliert werden. Dies gewährleistet den Zugriff auf die Logdateien eines Systems, selbst wenn dieses System vollständig beschädigt ist (Festplattenschaden o. ä.).
- *Protokoll*: Hier wird das Protokoll (TCP/UDP) eingestellt, mit dem die Syslog-Meldungen im Netz verschickt werden.

  Normale Syslog-Server unterstützen nur UDP. Mit dem neuen „syslog-ng“ auf dem Syslog-Server kann auch TCP für eine zuverlässige Übertragung genutzt werden.
- *Log-Port*: Hier muss der Zielport des Syslog-Servers eingegeben werden. Normalerweise läuft Syslog auf Port 514.
- *Log-Host*: Hier wird die IP-Adresse des Syslog-Servers angegeben.

19.8.6.2 *Ereignislog*

(Dieser Dialog befindet sich unter *Logkonfiguration – Ereignislog*)
Bei bestimmten Ereignissen kann das System selbständig eine E-

Mail an den Administrator schicken. Dabei wird beispielsweise bei Zugriffen von anderen Systemen deren IP-Adresse sowie die Uhrzeit mitgeschickt.

Felder in diesem Dialog

- *Ereignis*: In dieser Liste müssen die Ereignisse ausgewählt werden, bei deren Auftreten eine E-Mail verschickt wird.
- *Benachrichtigen per E-Mail*: In dieser Liste müssen die Ereignisse ausgewählt werden, bei deren Auftreten eine E-Mail verschickt wird.

20 Software neu installieren oder Auslieferungszustand wiederherstellen

Das Betriebssystem des V-Cube kann bei Bedarf in kurzer Zeit neu installiert werden. So kann der Server sozusagen in den Auslieferungszustand zurückgesetzt werden.

20.1 Brennen der ISO-Datei

- Bevor Sie die Installation beginnen, brennen Sie das heruntergeladene ISO-Image als Disk-Image auf ihren leeren Datenträger (DVD-Rohling).
- Nach dem Brennen der DVD legen Sie diese bitte in ein Bootfähiges DVD-Laufwerk und rebooten die Maschine.
- Alternativ kann das ISO-Imageauf einen USB-Stick kopiert werden, um mit diesem das System zu installieren. Die Vorgehensweise ist im Howto „Erstellen eines bootbaren USB-Sticks“ beschrieben.

20.2 Installation

WICHTIGER HINWEIS: Durch die Installation des Collax Servers werden ALLE AUF DEM SYSTEM BEFINDLICHEN DATEN GELÖSCHT. Verwenden Sie bitte eine dedizierte Maschine für Ihren Test bzw. für den späteren Betrieb.

- Legen Sie die DVD ein, booten Sie und folgen Sie den Anweisungen.
- Sie können die vorgeschlagene IP-Adresse akzeptieren oder eine IP-Adresse mit der entsprechenden Netzmaske aus Ihrem Netz vergeben.
- Nach der Installation erscheint die Meldung „Fertig“. Starten Sie den Rechner neu. Der erste Boot-Vorgangdauert etwas länger.
- Sobald die Login-Aufforderung kommt, können Sie Monitor und Tastatur abhängen.

Der Collax Server ist jetzt einsatzbereit.

20.3 Administration

- Verbinden Sie sich zum Collax Server über einen Browser.
- Folgen Sie den ersten Schritten hier (S. 10)

Index

Access Control List (ACL) 286, 292
Account deaktivieren 61
Active Directory (ADS) 96
Address Resolution Protocol (ARP) 151
Administration *7*
Administrator-Passwort *70*
Adressauflösung 150
Adresse 6, 190
ADS *87*
AES 109
Aktive Überwachung 486
Alarmintervall 492
Alias 62, 122, 134, 162, 166, 170, 262, 281
ARP (Address Resolution Protocol) 151
arpa 228
Arpwatch 489
Ausfall von Diensten 486
Auslieferungszustand *571*
Auswertung 219, 564
Authentifizierung 34, 60, 414
Benutzer exportieren 19
Benutzungsrichtlinien *33*
Bridge 181
Broadcast-Domain 181
Certificate Authority (CA) *102*
Certificate Authority (CA), Laufzeit 109
Certificate Authority, CRL 129
Certificate Revocation List (CRL) *129*
CPU 185
Dashboard *8*
Datensicherung *297*
DER *123*
DHCP 235
Dienste-Übersicht 549
DNS *229*
Domain 226
Domänen-Controller *84*
Failover 184, 201
Fax-Nummer 63
Fehlersuche 523
Fileserver 283
Firewall 34
FQDN *229*
Freigabe 283
Fully Qualified Domain Name *229*
Gruppe 33, *50, 409*

Hardware, Konfiguration 185
Hostname 225
IP-Adresse 162, 166, 169, 190, 201, 204, 225, 488, 523, *550,* 555, 568
IPMI 187
KDC *93*
Kerberos *93*
Kodierung von Dateinamen 86
Konfiguration importieren 18
Kryptographie *99*
Laufzeit Zertifikat *109*
Laufzeit 547
LDAP *79*
Lizenz *509*
Load-Balancing 184
Logical Volume Management (LVM) *528*
Login 61
Lokale Domain 234
MAC-Adresse 225, 258
Mail-Queue 561
Modem, Schnittstelle 188
Nameserver 231
Netzwerküberwachung *485*
Neustart 539
Notstromversorgung *501*
NTP *481*
Parent 250
Passive Überwachung 489
Passwort 63
PDC *84*
PEM *123*
PGP 111
Ping 523
PKCS12 *123*
Primary DNS 232
Primäre E-Mail-Adresse 62
Private Key 100
Prozessliste 549
Public Key 100
redundante Netzwerkverbindung 198
Restore 571
Reverse-Lookup *233*
Reverse-Zone 254
Root-Bridge 182
Root-Zone 229
Round Robin 184
RSA Public Key 118
Rückwärtsauflösung *233*
Schlüssellänge *108*
Schnittstellen 181
Secondary DNS 232
Serielle Konsole 188
Serielle Schnittstelle, Konfiguration 187
Share 283
SNMP *487*

Softwareinstallation *571*
Spanning Tree Protocol
(STP) 182, 197
Subdomain *228*
Suchliste 244
System herunterfahren 539
Systemzeit *481*
Top-Level-Domain (TLD)
226
Trunking 198
Update *517*
Update über Proxy 521
UPS *501*
Uptime 547
USB-Adapter 185
USV *501*
USV, Schnittstelle 188
Verschlüsselung *99*
VLAN 182, 194
Voreinstellung *6*
Werkzeugkasten 523
WINS *86*
X.509-Standard 103
X.509-Zertifikat *115*
Zeitraum *67*
Zertifikat zurückziehen 127
Zertifikat, Laufzeit *109*
Zertifikate 102
Zonentransfer 249
Zugriff 50, 409
Überwachung 264