



A MITEL
PRODUCT
GUIDE

Unify OpenScape 4000

Installation, Configuration and Migration

Installationsanleitung

08/2024

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Europe Limited. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos, and graphics (collectively “Trademarks”) appearing on Mitel’s Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively “Mitel”), Unify Software and Solutions GmbH & Co. KG or its affiliates (collectively “Unify”) or others. Use of the Trademarks is prohibited without the express consent from Mitel and/or Unify. Please contact our legal department at iplegal@mitel.com for additional information. For a list of the worldwide Mitel and Unify registered trademarks, please refer to the website: <http://www.mitel.com/trademarks>.

© Copyright 2024, Mitel Networks Corporation

All rights reserved

Inhalt

1 Vorbereitungen.....	7
1.1 Voraussetzungen.....	7
1.2 Verwendung von Drittanbieterprodukten.....	7
1.3 Anschließen eines Service-PCs an das System.....	7
1.3.1 USB-Treiber und limesch.....	8
1.3.2 BIOS-Einstellungen.....	8
1.3.3 Service-Zugang über Management-Port.....	10
1.4 Standardeinstellungen für Anmeldungen und Netzwerkkonfiguration.....	12
2 Erstinstallation.....	13
2.1 Wichtige Hinweise.....	13
2.2 Remote Major Update (RMU).....	14
2.2.1 Planung der IP-Adressen/Bereitstellung (Deployment).....	14
2.2.1.1 Hostname.....	14
2.2.1.2 Corosync LAN.....	14
2.2.1.3 Sind Kunden-LAN und IPDA-LAN im selben Subnetz oder in verschiedenen Subnetzen?.....	15
2.2.1.4 IP-Adressen.....	15
2.2.1.5 Atlantic LAN.....	16
2.2.1.6 Planungstabellen.....	16
2.2.2 Wie Sie ein bootfähiges 4K-ISO-Image auf einen USB-Stick brennen.....	36
2.2.3 Installation und Konfiguration von SLES und Konfiguration von OpenScape 4000.....	38
2.2.3.1 Mögliche Bereitstellung je nach Festplattengröße.....	38
2.2.3.2 Vorbereitung.....	38
2.2.3.3 Vorbereitung eines USB-Sticks für die Installation.....	39
2.2.3.4 Erste Installation mit Auto GENDB.....	40
2.2.3.5 Installationsvorgang mit Monitor/Tastatur	41
2.2.3.6 Installation nur mit dem OLED-Display und der "ON" -Taste	52
2.2.3.7 Empfohlener GSD-Installationsablauf.....	54
2.3 Manuelle Konfiguration des OpenScape 4000 SoftGate.....	54
2.4 Zero Local-Konfiguration für Stand-Alone OpenScape 4000 SoftGate.....	57
2.4.1 Leistungsmerkmalbeschreibung.....	58
2.4.2 Serviceinformationen.....	59
2.4.3 Konfiguration (Beispiel).....	60
2.4.3.1 DHCP-Server-Konfiguration.....	60
2.4.3.2 Zero Local-Konfiguration bei getrenntem Kunden- und IPDA-LAN.....	63
2.4.3.3 Zeitsynchronisierung der Linux-Systemzeit.....	66
2.4.3.4 Konfigurieren der NGS IP-Adresse.....	68
2.4.3.5 Konfigurieren des NGS.....	69
2.5 Zero Local Konfiguration für Survivable OpenScape 4000 SoftGate.....	70
2.6 Protokolldateien.....	73
3 OpenScape 4000 Installation auf VMware ESXi.....	75
3.1 Wichtige Hinweise.....	75
3.2 Benötigte Software und Hardware.....	77
3.3 Benötigte Informationen vom Kunden.....	77
3.4 Service PC.....	77
3.5 Vorbereitung der VMware Umgebung.....	78
3.5.1 Vorbereitungen am ESXi Host.....	78
3.5.2 Vorbereitungen auf dem Service PC.....	85
3.6 Dimensionierung/Voraussetzungen der virtuellen Maschine.....	87
3.6.1 Dimensionierung.....	87

3.6.2 Hardwarevirtualisierung.....	87
3.7 Import einer OVF-Vorlage (Beispiel: Simplex).....	87
3.8 CPU Shares.....	93
3.9 Trennen nicht verwendeter Netzwerkadapter.....	96
3.10 Erst-Installations-XML-Datei erzeugen.....	97
3.10.1 MAC-Adresse.....	97
3.10.1.1 Automatische generierte MAC-Adresse übernehmen (Regelfall).....	97
3.10.1.2 Manuell generierte MAC-Adresse übernehmen (Staging Center).....	98
3.10.2 DNS-Server.....	99
3.11 Floppy Image mit dem Inhalt der firstinst-netw-*.xml erzeugen.....	99
3.12 Hotfix Installation vorbereiten.....	100
3.13 Hardware Virtualisierung auf dem ESXi Host aktivieren.....	100
3.13.1 Allgemeine Information.....	100
3.13.2 Hardwarevirtualisierung aktivieren mit vSphere Client.....	101
3.13.3 Hardwarevirtualisierung aktivieren mit vSphere Web Client.....	103
3.14 OpenScape 4000 Installation in der virtuellen Maschine.....	104
3.14.1 Vorbereitungen.....	104
3.14.2 Installation starten.....	107
3.15 Anpassungen nach der Installation.....	108
3.15.1 Zuordnung der LAN-Schnittstellen zu den Netzwerkschnittstellen.....	109
3.15.2 Umstellen des DVD-Laufwerkes auf "lokales Gerät".....	111
3.15.3 Auf die Fertigstellung der OpenScape 4000 Assistant Installation warten.....	112
3.15.4 Konfigurieren der Kundendaten.....	112
3.15.5 Systemstatus überprüfen.....	112
3.16 Staging Center Bereitstellung für den Endkunden.....	113
3.16.1 Export der virtuellen Maschine in eine OVF-Datei.....	113
3.16.2 Installation beim Endkunden.....	114
3.17 Hinweise und Mögliche Fehlerquellen.....	114
3.17.1 Log-Dateien während der Installation.....	114
3.17.2 Remote Major Update (RMU).....	115
3.17.3 Hardwarevirtualisierung nicht aktiviert.....	115
3.18 Re-Installation der OpenScape 4000 Software.....	116
4 Migration und Neuinstallation von älteren Systemen.....	120
4.1 Vorbereitung.....	120
4.2 Vor der Migration des HiPath 4000 V6 Host-Systems.....	121
4.2.1 Sichern der RMX-Datenbasis.....	121
4.2.2 Erstellen eines logischen Backups.....	121
4.2.3 Speichern des logischen Backups.....	123
4.2.4 Abschließende Schritte vor dem Schließen des HiPath 4000 V6 Hosts.....	123
4.3 Migration des OpenScape 4000 Host-Systems.....	124
4.3.1 Wiederherstellen der RXM-Datenbasis.....	124
4.3.2 Wiederherstellen von OpenScape 4000 Assistant anhand des logischen Backups.....	124
4.3.3 Konfiguration des OpenScape 4000 SoftGate bei aktivierter Signalisierungs- und Payload-Verschlüsselung.....	127
4.4 Reinstallation/Aktualisierung der Remote-Appliance (RAR).....	127
4.4.1 Wichtige Hinweise.....	127
4.4.2 Reinstallieren/Aktualisieren der Remote-Appliance (RAR).....	128
4.4.2.1 Teil 1: Vorbereitung der Remote Appliance.....	129
4.4.2.2 Teil 2: Vorbereitung des zentralen Hosts.....	130
4.4.2.3 Teil 3: Start des eigentlichen RAR-Vorgangs per Skript im Terminalfenster.....	131
4.4.2.4 Teil 4: Manuelle Überprüfung der reinstallierten Appliance über RAR.....	136
4.4.3 RAR Hilfe.....	138
4.5 Remote Major Update (RMU).....	140
4.5.1 Wichtige Hinweise.....	140
4.5.2 Ablauf des Remote Major Update (RMU).....	141

4.5.2.1 Teil 1: Vorbereiten des zweiten Systems.....	141
4.5.2.2 Teil 2: Erstellen des Recovery ISO-Backups.....	141
4.5.2.3 Teil 3: Starten des RMU-Prozesses.....	142
4.5.2.4 Teil 4: Manuelle Überprüfung nach RMU.....	143
4.6 Reinstallation vom Recovery ISO-Image.....	143
5 Update-/Upgrade-Prozess für OpenScape 4000.....	144
5.1 Aktualisieren von einem Minor Release auf ein anderes Minor Release.....	145
5.1.1 Voraussetzungen.....	145
5.1.2 Vorbereitung.....	148
5.1.3 Aktivierung.....	152
5.1.3.1 APE und Survivable SoftGate aktivieren.....	155
5.1.3.2 Standalone SoftGate aktualisieren.....	157
5.2 Major-Release-Upgrade.....	157
5.2.1 Kürzere Downtime für LoadWare-Hotfixes.....	158
6 Ändern der Plattformkonfiguration.....	159
6.1 Wichtige Hinweise.....	159
6.2 Verwenden des OpenScape 4000 Plattform Administration-Portals.....	160
6.2.1 Ändern der IP-Adresse des Kunden-LAN.....	160
6.2.1.1 OpenScape 4000, Plattform Administration (Portal).....	160
6.2.1.2 Ändern der IP-Adresse des OpenScape 4000 Assistant.....	160
6.2.1.3 Ändern der IP-Adresse des OpenScape 4000 CSTA.....	161
6.2.2 Ändern der Atlantic-Schnittstelle.....	161
6.2.3 Ändern der IP-Adresse des OpenScape 4000 SoftGate.....	161
6.3 Recovery/Reconfiguration Tool.....	162
6.3.1 Voraussetzungen auf dem System.....	163
6.3.2 Skriptausführung.....	163
6.3.2.1 Allgemeine Ausführungsschritte.....	164
6.3.2.2 Einzelknoten-Bereitstellungen.....	167
6.3.2.3 Mehrknoten-Bereitstellungen.....	168
6.3.2.4 Wiederherstellung von Mehrknoten-Bereitstellungen.....	171
6.4 Recover/Reconfiguration Tool verwenden.....	175
6.4.1 Standard-Gateway.....	175
6.4.2 Ändern der IP-Adresse des IPDA-Netzwerks.....	175
6.4.3 Ändern von Corosync-Hostname und -IP-Adresse.....	176
6.4.4 Atlantic-Schnittstelle.....	176
6.4.5 Änderungen an OpenScape 4000 SoftGate / Enterprise Gateway.....	176
7 Lizenzierung.....	178
7.1 Übersicht.....	178
7.2 Übergangszeit und Installation der Lizenzdatei.....	179
7.3 Lizenz für OpenScape 4000 SoftGate and OpenScape Enterprise Gateway installieren.....	180
7.4 OpenScape 4000 Appliance Software Lizenz JeOS.....	181
7.4.1 Betriebssystem SUSE Linux Enterprise JeOS für OpenScape 4000.....	181
7.4.2 Grundsatz der JeOS Lizenzierung.....	182
7.4.2.1 Reporting.....	182
7.4.2.2 Ablauf der Lizenzen und Kontrolle.....	182
7.4.3 OpenScape 4000 - JeOS.....	182
7.4.4 Central License Server (CLS).....	183
7.4.5 Systemzustände abhängig von der Lizenz.....	184
7.4.5.1 Zustände und Hinweismeldungen.....	184
7.4.5.2 JeOS Verlängerung.....	185
7.4.6 Bestellprozess.....	185
7.4.6.1 Erstbestellung über Hardware.....	185
7.4.6.2 Verlängerung der JeOS Lizenz um 3 Jahre.....	185
7.4.7 Zusammenfassung der JeOS Aktivitäten.....	186

7.4.7.1 Erneuerung JeOS Lizenz.....	186
7.4.7.2 Erweiterung um OpenScape 4000 SoftGates.....	186
8 Zeitsynchronisation.....	187
8.1 Network Time Protocol-Server.....	187
8.1.1 Größere Vorwärts-Sprünge der Systemzeit.....	188
8.1.2 Wichtige Informationen zum Einstellen oder Ändern der Uhrzeit.....	188
8.2 Konfiguration der Zeit in allen Servern.....	190
8.3 Konfiguration der Zeitzonen mit OpenScape 4000 Assistant.....	190
8.3.1 Einstellung von Zeitzone und Sommerzeit für OpenScape 4000 Assistant und RMX.....	190
8.3.2 Einstellung von Zeitzone und Sommerzeit am Access Point/OpenScape 4000 SoftGate.....	191
8.3.3 Einstellung der Zeitzone für OpenScape 4000 CSTA.....	192
9 Anhang A: Tabellen für die Infrastrukturplanung.....	193
10 Anhang B: Erstinstallationsskript und XML-Konfigurationsdatei.....	195
10.1 Einführung.....	195
10.2 Erstinstallationsskript - Befehlszeilenoptionen.....	195
10.3 XML-Konfigurationsdatei.....	202
10.3.1 Format.....	203
10.3.1.1 Verzeichnis der XML-Datei.....	203
10.3.1.2 Name der XML-Datei.....	203
10.3.1.3 Struktur der XML-Datei.....	203
10.3.2 Mögliche Parameter und ihre Werte.....	205
10.3.2.1 Allgemeiner Abschnitt.....	205
10.3.2.2 Knotenabschnitt.....	211
10.3.3 Regeln.....	218
10.3.3.1 Regeln für Simplex-Bereitstellungen.....	218
10.3.3.2 Regeln für Duplex/Separated Duplex-Bereitstellungen.....	218
10.3.3.3 Regeln für die Schnittstellenkonfiguration.....	218
10.3.3.4 Regeln für die Routenkonfiguration.....	222
10.3.4 Netzmaske und Präfixlänge.....	223
10.3.5 Zeitzonenwerte.....	223
11 Appendix C: Bond- und VLAN-Konfiguration.....	227
11.1 Bond-Konfiguration.....	227
11.2 Atlantik-Konfiguration.....	228
12 Anhang D: Wie Sie eine XML-Datei automatisch erstellen.....	230
13 Anhang E: Häufig gestellte Fragen (FAQ).....	231
13.1 Konnektivität und Installation.....	231
13.1.1 Konnektivität.....	231
13.1.2 Installation und Upgrades.....	232
13.2 Backup & Restore.....	237
13.3 Hotfix-Installation.....	237
13.4 Zeiteinstellung / Zeitsynchronisation.....	238
13.5 Lizenzierung.....	239
13.6 Hardwarefehler.....	240
14 Glossar.....	241
Index.....	242

1 Vorbereitungen

1.1 Voraussetzungen

- Informationen zur Dokumentation: Alle Dokumente, die in E-Doku zur Verfügung stehen, stehen auch im Unify Partner Portal zur Verfügung. Wenn Sie keinen Zugriff auf E-Doku haben, verwenden Sie bitte das Partner Portal.
- (keine andere Applikation darf co-located auf der Maschine laufen, z.B. Viren-Scanner) (siehe auch [Section 1.2, "Verwendung von Drittanbieterprodukten"](#)).
- Informationen zur Hardwarekompatibilität der OpenScape 4000 Software finden Sie im Kapitel 2, "OpenScape 4000 Bereitstellungen" der OpenScape 4000 Leistungsmerkmalbeschreibung.
- Verwenden Sie die Security Checkliste, um die erforderlichen Sicherheitseinstellungen für die einzelnen Produkte zu übernehmen / zu prüfen.

1.2 Verwendung von Drittanbieterprodukten

Verwenden von Drittanbietersoftware auf OpenScape 4000

- Es ist nicht erlaubt, Software von Drittanbietern auf OpenScape 4000 zu installieren. OpenScape 4000 verwendet das Appliance-Modell für das Betriebssystem Linux. Dies bedeutet, dass nur die erforderlichen Betriebssystemkomponenten verwendet werden, was das System nicht nur schlanker - also effizienter - sondern auch sicherer macht. Erforderliche SUSE Linux Betriebssystem-Updates werden im Rahmen unseres Fix Release/Hotfix-Konzepts angewendet.
- Antiviren-Scanner oder andere Angriffserkennungssysteme sind ebenfalls nicht erlaubt. Dies hat folgende Gründe:
 - Als Linux-System ist der Server an sich schon weniger von Viren, Würmern und anderen Angriffen bedroht als ein Windows-System. Darüber hinaus wird das Risiko durch seine Firewall-Konfigurationen und den sorgfältig kontrollierten Administrationszugriff weiter minimiert.
 - Die Ausführung solcher Scanner kann zu einer erheblichen Steigerung der CPU-Auslastung führen und andere Kapazitätsberechnungen zunichte machen. Die Umsetzung einer Unternehmensrichtlinie, die den Einsatz von Virenscannern auf allen Computern fordert, ist bei diesem speziellen Servertyp nicht angebracht und sollte in diesem Fall ausnahmsweise ausgesetzt werden.

Stattdessen ist es sinnvoller, die Software vor der Installation zu scannen.

1.3 Anschließen eines Service-PCs an das System

Wenn keine Tastatur, keine Maus und kein Monitor verfügbar sind, kann über USB ein Service-PC an den EcoServer und EcoBranch angeschlossen werden.

Für den Anschluss eines Service-PCs müssen folgende Vorbereitungen getroffen werden:

1.3.1 USB-Treiber und liesmich

Für die Installation der USB1-Konsole auf DSCXL2, EcoServer und EcoBranch werden die WHQL USB-Treiber des Herstellers MosChip benötigt.

Wichtig: Unify übernimmt keine Verantwortung für die Verwendung/Installation dieser USB-Treiber, sondern stellt lediglich beim Erstellen des Image die WHQL-Treiber von der Website des Herstellers in der aktuellen Version bereit.

Informationen zum Konsolenzugriff (Terminalemulation) finden Sie unter `USB_INSTALL_README.pdf`. Diese Datei ist Teil des ISO-Image und befindet sich im Pfad `\DriversAndTools\USB_Driver\`.

Aktuelle Treiber sollten direkt von der Seite des Herstellers heruntergeladen werden und werden nicht mit der OpenScape 4000 ISO Datei zur Verfügung gestellt:

EcoServer/Branch:

<http://www.ftdichip.com/Drivers/VCP.htm>

Gemeldete Probleme bei der Treiberinstallation

Es wurde von Problemen berichtet, die dazu führen, dass die neu installierten USB-Geräte im Windows-Gerätemanager mit einem gelben Ausrufezeichen gekennzeichnet werden. Klicken Sie in diesem Fall im Windows-Gerätemanager mit der rechten Maustaste auf das Gerät und weisen Sie ihm auf der Registerkarte "Eigenschaften" einen ungenutzten COM-Port zu (z. B. COM 10 & COM 11).

1.3.2 BIOS-Einstellungen

NOTICE: In BIOS ab Version 4 sind keine Änderungen an den BIOS-Einstellungen erforderlich.

Es gibt drei Möglichkeiten, wie das BIOS im **BIOS MENÜ** konfiguriert werden kann. Unter **Erweiterte Fernzugriff > Konfiguration** und der **Umleitung nach BIOS POST** müssen übereinstimmen, sonst kann schwarzer Text auf schwarzem Hintergrund angezeigt werden!

Terminal-Typ=ANSI -Farbumleitung nach BIOS POST=Boot Loader Putty-Einstellungen Empfehlung: Die Rücktaste "Control-H" Funktionstasten und Tastatur "ESC)n~"

Terminal-Typ=VT100 - Nur schwarz und weiß. Umleitung nach BIOS Post = Immer Putty-Einstellungen Empfehlung: Die Rücktaste "Control-H" Funktionstasten und Tastatur "VT100"

Terminal-Typ=VT-UTF8 -Empfohlen und wird BIOS-Standard sein. Umleitung nach BIOS POST=Boot Loader Putty-Einstellungen Empfehlung: Die Rücktaste "Control-H" Funktionstasten und Tastatur "Linux"

NOTICE: Die Parameter der Tastatur-/Terminal-Emulation müssen je nach Konfiguration möglicherweise angepasst werden.

Nun können Sie Ihren Service-PC wie folgt mit dem EcoServer/EcoBranch verbinden:

- Schließen Sie einen Service-PC an die USB1-Schnittstelle der EcoServer/EcoBranch-Platine an.



Figure 1: TAP-Verbindung auf dem EcoServer



Figure 2: TAP-Verbindung bei EcoBranch

- Konfigurieren Sie den ersten neuen COM-Port. Installieren Sie den Port mit 115200, 8, None, 1.

Wichtige Informationen

- Terminalemulationsprogramm
- Für die Installation/Konfiguration über den USB-Konsolenport wird ein Terminalemulationsprogramm benötigt (z. B. HyperTerminal/PuTTY/TeraTerm). ComWin ist nicht ausreichend, da dieses Programm die erforderliche Terminalemulation für den BIOS-Aufruf nicht unterstützt. PuTTY wird empfohlen, da dieses Programm in der Regel auch für SSH-Verbindungen verwendet wird.

- Für die Installation der USB1-Konsole werden SB-Treiber vom Hersteller benötigt.

ATOS übernimmt keine Verantwortung für die Verwendung/Installation der USB-Treiber und empfiehlt nur die neuesten WHQL-Treiber.

Tatsächliche Treiber sollten direkt von der Hersteller-Website heruntergeladen werden und werden nicht mit der OpenScape4000 ISO geliefert:

- EcoServer:
<http://www.ftdichip.com/Drivers/VCP.htm>
- EcoBranch:
<http://www.ftdichip.com/Drivers/VCP.htm>

1.3.3 Service-Zugang über Management-Port

NOTICE: Der Zweck des Management-Ethernets besteht darin, bei der Fehlersuche eine direkte Verbindung zum internen vLAN-Switch bzw. zur Bridge herzustellen. Ein PC kann direkt angeschlossen werden und bekommt eine IP-Adresse aus dem internen IP-Segment zugewiesen.



WARNING: Eine permanente Verbindung des Management-Ports mit einem IT-Netzwerk (z. B. Management-Netzwerk) ist nicht erlaubt, ebenso wenig wie eine Verbindung mit anderen EcoServern, da dies die Systemstabilität beeinträchtigt.

- Konfiguration

Auf ausgewählten HW-Plattformen (EcoServer und Branch) gibt es auf der Rückseite der Box einen speziellen Ethernetport, der mit einem Schraubenschlüsselsymbol gekennzeichnet ist; dies ist der sog. Management-Port. Dieser Anschluss wird für den Service-Zugang zum Web Based Management, ComWin, Assistant, Portal, CSTA und SSH des OpenScape 4000-Systems verwendet.

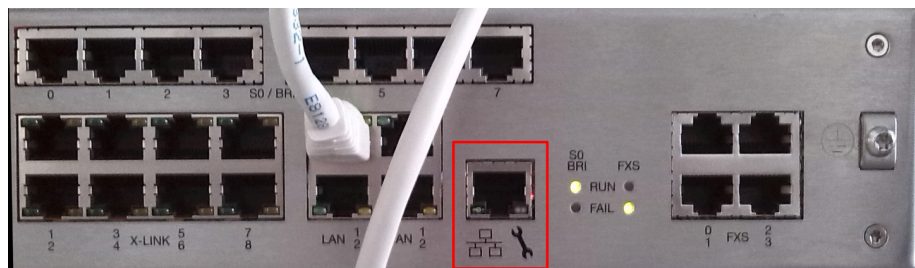


Figure 3: Management-Port bei der OpenScape 4000 Branch

Der Service-Zugang über den Management-Port ist standardmäßig aktiviert. Die Aktivierung/Deaktivierung erfolgt über Portal > LAN Wizard > Bereich Internes LAN > Kontrollkästchen "Management-Port aktivieren (eth10)". Bitte

beachten Sie, dass dieses Kontrollkästchen nur dann verfügbar ist, wenn die EcoServer- oder Branch-Hardware korrekt erkannt wurde.

Figure 4: Kontrollkästchen zur Aktivierung des Management-Ports

Sie können den Status des Management-Ports am blauen LCD-Display auf der Seite "Mgmt Port" überprüfen:



Figure 5: LCD-Display mit Anzeige des Management-Port-Status - Enabled (aktiviert) / Disabled (deaktiviert)

NOTICE: Wenn Sie den Service-PC an den Management-Port anschließen, wechselt die Anzeige auf dem LCD-Display von "Enabled" auf "Connected" (verbunden) (die Mgmt Port-Seite auf dem Display wird nicht automatisch aktualisiert).

- Verwendung
 - 1) Überprüfen Sie am LCD-Display, ob der Management-Port aktiviert ist (Enabled).
 - 2) Verwenden Sie ein Ethernet-Kabel, um Ihren Laptop mit dem Management-Port zu verbinden.
 - 3) Richten Sie Ihre Netzwerkkarte so ein, dass die IP-Adresse automatisch über DHCP bezogen wird.
 - 4) Warten Sie, bis die IP-Adresse vom DHCP-Server zugeteilt wurde. Der Management-Port nutzt dieselbe Subnetzadresse wie das interne LAN. Standardmäßig liegen die ILAN-Adressen im Bereich 192.168.187.100-150, Netzmaske 255.255.255.0. Ihnen wird eine IP-Adresse aus diesem Bereich zugeteilt.
 - 5) Ab jetzt können Sie die Dienste mittels Webbrowser, ComWin oder SSH-Client über die internen LAN-Adressen des Portal, Assistant und CSTA erreichen. Diese Adressen werden auf dem LCD-Display angezeigt.

Vorbereitungen

Standardeinstellungen für Anmeldungen und Netzwerkkonfiguration

1.4 Standardeinstellungen für Anmeldungen und Netzwerkkonfiguration

EcoServer/EcoBranch wird mit vorinstallierter Appliance-Software mit folgenden Standardeinstellungen für Anmeldungen und Netzwerkkonfiguration ausgeliefert.

- Logins:

Tabelle 1: Standardeinstellungen für Logins

Anwendung	Benutzer	Kennwort
Linux / RMX	root	hicom
Linux	linuser	hicom
OpenScape 4000 Plattform Administration (Portal) / OpenScape 4000 Assistant	engr	4K-admin
OpenScape 4000 CSTA	root	4K-admin
CSTA CBAAdmin	Admin	Admin

Anmerkung: Bei Ihrer ersten Anmeldung werden Sie aufgefordert, das Standardkennwort zu ändern. Das Passwort für OpenScape 4000 Assistant wird auch für die OpenScape 4000 Plattform Administration (Portal) verwendet.

- Netzwerkkonfiguration:

Tabelle 2: Standardeinstellungen für die Netzwerkkonfiguration

Schnittstelle LAN 1 - eth0	IP-Adresse
Physikalische IP	192.168.0.2 / 24
OpenScape 4000, Plattform Administration (Portal)	192.168.0.3 / 24
Standard-GW/Router	192.168.0.1

- Nach der Installation des Image wird ein Standardserver im Mehrbenutzermodus mit Netzwerkverbindung (init 3) gestartet.

Wichtig: OpenScape 4000 systems dürfen nur in Linux runlevel 3 (init3) laufen.

2 Erstinstallation

IMPORTANT: Die Erstinstallation ohne XML wird ab V10R1 nicht mehr unterstützt.

2.1 Wichtige Hinweise

Wichtig: Während der Installation wird der verfügbare Speicherplatz auf der Festplatte geprüft, um die möglichen Bereitstellungsvarianten zu bestimmen. Weitere Informationen zur benötigten Festplattengröße finden Sie in [Section 2.2.3.1](#), "Mögliche Bereitstellung je nach Festplattengröße".

Wichtig: Wenn eine physische Trennung des LANs nicht möglich ist und Infrastrukturkomponenten verwendet werden um die Knoten zu verbinden (z. B. Netzwerk-Switches), dann muss der Verkehr von den verschiedenen Schnittstellen (Customer, IPDA, Corosync, Atlantic LANs) über vLANS getrennt werden. Das kann entweder in den Infrastrukturkomponenten selbst oder in der OpenScape 4000-Netzwerkkonfiguration konfiguriert werden.

Deployment	Options	DSCXL/DSCXL2 - S30122-K7732-X S30122-X8004-X39	OSA500 S30807-U6649-X100-11 S30807-U6649-X101 S30807-U6649-X101-G1 S30807-U6649-X101-8 S30807-U6649-X300-11 S30807-U6649-X301 S30807-U6649-X301-H1 S30807-U6649-X101-9	VMware®	OS 4000 EcoServer S30122-K7754-X S30122-K7754-X100 S30122-K7754-X200	OS 4000 Branch S30122-K7758-X	OS EcoServer (ECO2) S30122-K7760-X	OS EcoBranch (Branch2) S30122-K7761-X
Simplex	without SoftGate	n/r	n/r	✓	✓ [1]	n/r	✓ [1]	n/r
	with SoftGate	n/r	✓	✓ [2]	✓ [1]	✓ [1]	✓ [1]	✓ [1]
Duplex	Duplex	n/r	n/p	n/p	✓	n/p	✓	n/p
	with SoftGate	n/p	n/p	n/p	✓ [2] [5]	n/p	✓ [2] [5]	n/p
Separated Duplex (GSD)	Node A & B	n/r	n/r	✓	✓	n/r	✓	n/r
	Node A & B with SoftGate	n/p	n/r	n/r	✓ [2] [5]	n/r	✓ [2] [5]	n/r
	Quorum	n/r	✓	✓	✓	✓	✓	✓
	Quorum with SoftGate	n/r	✓	✓ [2]	✓	✓	✓	✓
APE		✓ [4]	n/p [3]	n/p [3]	n/p [3]	n/p [3]	n/p [3]	n/p [3]
Survivable	without SoftGate	n/r	✓	✓	✓ [1]	✓ [1]	✓ [1]	✓ [1]
	with SoftGate	n/p	✓	✓ [2]	✓ [1]	✓ [1]	✓ [1]	✓ [1]
Standalone SoftGate	Standalone SoftGate	n/r	✓	✓ [2]	n/r	n/p	n/r	✓
Enterprise Gateway	without SoftGate	n/p	n/p	n/p	✓ [1]	✓	✓ [1]	n/p
	with SoftGate	n/p	n/p	n/p	✓ [1] [2]	n/p	✓ [1] [2]	n/p
Survivable Enterprise Gateway	without SoftGate	n/p	n/p	n/p	✓ [1]	n/p	✓ [1]	n/p
	with SoftGate	n/p	n/p	n/p	✓ [1] [2]	n/p	✓ [1] [2]	n/p
Manager		n/p	n/p	✓	n/p	n/p	✓	n/p

✓ = possible

n/p = not possible; The firstinst-netw.sh blocks the installation. Portal LAN Wizard configuration not possible.

n/r = not released; The firstinst-netw.sh allows the installation, but a warning is displayed. Portal LAN Wizard configuration is allowed, but a warning is displayed.

[1] Installation/Activation of Hosted OpenScape Session Border Controller (hSBC) is supported

[2] Xlink connectivity to Access modules is not supported for VMware deployments, or hosted SoftGates (meaning iSG on Enterprise Gateways and node A or B of Duplex/GSD)

[3] For APE select Survivable deployment and don't configure the SoftGate.

[4] The DSCXL HW will be discontinued starting with SW version V10R1.

[5] Starting with V10R1

Abbildung 6: OpenScape 4000 V10 Deployment Matrix

2.2 Remote Major Update (RMU)

Mit dem Remote Major Update-Prozess kann ein zentrales Host-System, auf dem HiPath 4000 V7R2 ausgeführt wird, aus der Ferne auf OpenScape 4000 V10 aktualisiert werden.

Bei diesem Vorgang wird ein zweites System desselben Hardware-Typs wie das Remote-System verwendet, um ein Recovery ISO-Image vorzubereiten und zu erstellen, das die OpenScape 4000 V10R1 -Software sowie die komplette Systemkonfiguration enthält.

Dieses ISO-Image wird sodann an das Remote-Host-System übertragen und für den Remote Major Update-Prozess verwendet.

2.2.1 Planung der IP-Adressen/Bereitstellung (Deployment)

Als erstes muss die Konfiguration der Infrastruktur geplant werden. Sie hängt von der Netzwerkstruktur ab und beinhaltet die IP-Adressen des OpenScape 4000 Systems.

2.2.1.1 Hostname

Erstellen Sie einen eindeutigen, gültigen Hostnamen (der Hostname muss mit einem Buchstaben beginnen, kann Buchstaben, Ziffern und Bindestriche enthalten und darf nicht mit einem Bindestrich enden):

Bei Duplex-/Separated-Duplex-Szenarien sind separate Hostnamen für alle Knoten erforderlich.

Bitte beachten Sie, dass der System-Hostname im Falle von Simplex der Hostname ist, der der Kundenschnittstelle zugewiesen wurde, und im Falle von Duplex-Bereitstellungen der Corosync-Hostname.

2.2.1.2 Corosync LAN

Wichtig: Corosync-LAN darf für die [Einzelknoten-Deployment](#) nicht konfiguriert werden!

Wählen Sie den/die Hostnamen des Corosync-LAN (muss mit dem Hostnamen der Maschine übereinstimmen).

Der Hostname des Corosync-LAN darf nicht mit dem Hostnamen des Kunden-LAN identisch sein.

Beispiel: soco2-sys1, soco2-sys2 und soco2-quorum

Der Domain-Name muss also nicht anders sein.

2.2.1.3 Sind Kunden-LAN und IPDA-LAN im selben Subnetz oder in verschiedenen Subnetzen?

Überprüfen Sie nun, ob das Kunden-LAN und das IPDA-LAN demselben Subnetz oder unterschiedlichen Subnetzen angehören.

Kunden-LAN und IPDA-LAN gehören demselben Subnetz an

Wichtig: Wenn das Kunden-LAN und das IPDA-LAN demselben Subnetz angehören (z. B. 218.1.17.0 /24), muss für beide dieselbe physikalische Schnittstelle (z. B. eth0) verwendet werden. Es dürfen keinesfalls unterschiedliche Schnittstellen verwendet werden, da dies zu Routing-Problemen führen würde.

- Kunden-LAN und IPDA-LAN

Wählen Sie den/die Host-Namen des Kunden-LAN/IPDA-LAN.

Bei Duplex-Bereitstellungen darf der Hostname des Kunden-LAN/IPDA-LAN nicht mit dem Hostnamen des Corosync-LAN identisch sein.

Beispiel: soco2-sys1-cust, soco2-sys2-cust und soco2-quorum-adm

Kunden-LAN und IPDA-LAN gehören unterschiedlichen Subnetzen an:

Wichtig: Wenn das Kunden-LAN und das IPDA-LAN unterschiedlichen Subnetzen angehören (z. B. Kunden-LAN 218.1.17.0 /24 und IPDA-LAN 172.16.2.0 /24), müssen zwei separate physikalische Schnittstellen (z. B. eth0 und eth2) verwendet werden.

- Kunden-LAN

Wählen Sie den/die Host-Namen des Kunden-LAN.

Bei Duplex-Bereitstellungen darf der Hostname des Kunden-LAN nicht mit dem Hostnamen des Corosync-LAN identisch sein.

Beispiel: soco2-sys1-cust, soco2-sys2-cust und soco2-quorum-adm

- IPDA LAN

Wählen Sie den/die Host-Namen des IPDA-LAN.

Beispiel: soco2-sys1-ipda und soco2-sys2-ipda

Bei Duplex-Bereitstellungen darf der Hostname des IPDA-LAN nicht mit dem Hostnamen des Corosync-LAN identisch sein.

2.2.1.4 IP-Adressen

- Alle IP-Adressen müssen eindeutig sein.
- Die physikalischen Netzwerkkarten des Kunden-LAN und des IPDA-LAN müssen eindeutige IP-Adressen aufweisen.
- Es dürfen nur physische Adressen als IP-Adressen verwendet werden, z. B. CCA/CCB.
- Supernetting wird für die IPDA-Schnittstellen nicht unterstützt.

2.2.1.5 Atlantic LAN

Bisher wurden für die Atlantic LAN-Schnittstelle benachbarte Paare (z. B. 6&7) verwendet. Dies entspricht jedoch nicht unserer Empfehlung für Bonding, falls der Kunde später Bonding konfigurieren möchte.

2.2.1.6 Planungstabellen

Leere Planungstabellen für Ihre Infrastrukturplanung finden Sie in [Chapter 9, "Anhang A: Tabellen für die Infrastrukturplanung"](#).

Beispiele für die einzelnen Bereitstellungen finden Sie in den folgenden Abschnitten:

- [Simplex](#)
- [Simplex mit integriertem SoftGate](#)
- [Duplex](#)
- [Separated Duplex](#)
- [Separated Duplex mit integriertem SoftGate](#)
- [APE](#)
- [Standalone SoftGate](#)
- [Survivable](#)
- [Enterprise Gateway](#)
- [OpenScape Enterprise Gateway Survivable](#)

Simplex

Wichtig: Die folgenden Beispiele beziehen sich auf OpenScape 4000-Software, die auf DSCXL2//EcoServer und EcoBranch ausgeführt wird.

Beispiel: Kunden-LAN und IPDA-LAN befinden sich im selben Subnetz.

Tabelle 3: Simplex: Infrastrukturplanung - Kunden-LAN und IPDA-LAN im selben Subnetz

ETH0	Kunden-LAN und IPDA-LAN		
	IP-Adresse	Netzmaske	Hostname
phys. IP (YaST)	218.1.17.100	255.255.255.0	soco2-sys1
OpenScape 4000, Plattform Administration (Portal)	218.1.17.102		
OpenScape 4000 Assistant	218.1.17.103		
OpenScape 4000 CSTA	218.1.17.104		
CCA	218.1.17.105		
Default Gateway/Router	218.1.17.254		
NGS	218.1.17.107		

ETH5 & ETH6LAN	Atlantic
----------------	----------

Beispiel: Kunden-LAN und IPDA-LAN befinden sich in unterschiedlichen Subnetzen.

Tabelle 4: Simplex: Infrastrukturplanung - Kunden-LAN und IPDA-LAN in unterschiedlichen Subnetzen

ETH0	Kunden-LAN		
	IP-Adresse	Netzmaske	Hostname
phys. IP (YaST)	218.1.17.100	255.255.255.0	soco2-sys1-cust
OpenScape 4000, Plattform Administration (Portal)	218.1.17.102		
OpenScape 4000 Assistant	218.1.17.103		
OpenScape 4000 CSTA	218.1.17.104		
Default Gateway/Router	218.1.17.254		
ETH2,	IPDA LAN		
	IP-Adresse	Netzmaske	Hostname
phys. IP (YaST)	172.16.2.100	255.255.255.0	soco2-sys1-ipda
CCA	172.16.2.105		
Default Router	172.16.2.254		
NGS	172.16.2.107		
ETH5 & ETH6	Atlantic LAN		

Simplex mit integriertem SoftGate

Wichtig: Nur "direct link" OpenScape 4000 Softgate können in ein Simplex Server Deployment integriert werden.

Beispiel: Kunden-LAN und IPDA-LAN befinden sich im selben Subnetz.

**Tabelle 5: Simplex mit integriertem OpenScape 4000 SoftGate
Infrastrukturplanung - Kunden-LAN und IPDA-LAN im selben Subnetz**

ETH0	Kunden-LAN und IPDA-LAN		
	IP-Adresse	Netzmaske	Hostname
phys. IP (YaST)	218.1.17.100	255.255.255.0	soco2-sys1
OpenScape 4000, Plattform Administration (Portal)	218.1.17.102	255.255.255.0	
OpenScape 4000 Assistant	218.1.17.103		

OpenScape 4000 CSTA	218.1.17.104		
CCA	218.1.17.105		
NGS	218.1.17.107		
Default Gateway/Router	218.1.17.254		
	SoftGate-Konfigurationsdaten		
NCUI	218.1.17.123		
AP-interne IP (DL)	192.168.1.23	255.255.255.0	
ETH5 & ETH6	Atlantic LAN		

Beispiel: Kunden-LAN und IPDA-LAN befinden sich in unterschiedlichen Subnetzen.

Tabelle 6: Simplex mit integriertem OpenScape 4000 SoftGate Infrastrukturplanung - Kunden-LAN und IPDA-LAN in unterschiedlichen Subnetzen

ETH0	Kunden-LAN		
	IP-Adresse	Netzmaske	Hostname
phys. IP (YaST)	218.1.17.100	255.255.255.0	soco2-sys1
OpenScape 4000, Plattform Administration (Portal)	218.1.17.102		
OpenScape 4000 Assistant	218.1.17.103		
OpenScape 4000 CSTA	218.1.17.104		
Default Gateway/Router	218.1.17.254		
ETH2,	IPDA LAN		
	IP-Adresse	Netzmaske	Hostname
phys. IP (YaST)	172.16.2.100	255.255.255.0	soco2-sys1-ipda
CCA	172.16.2.105		
NGS	172.16.2.107		
Default Router	172.16.2.254		
	SoftGate-Konfigurationsdaten		
NCUI	172.16.2.108		
AP-interne IP (DL)	192.168.1.23	255.255.255.0	
ETH5 & ETH6	Atlantic LAN		

Duplex

Beispiel: Kunden-LAN und IPDA-LAN befinden sich im selben Subnetz.

Tabelle 7: Duplex: Infrastrukturplanung - Kunden-LAN und IPDA-LAN im selben Subnetz

ETH0	Kunden-LAN und IPDA-LAN		
	IP-Adresse	Netzmaske	Hostname
phys. IP Knoten 1 (YaST)	218.1.17.100	255.255.255.0	soco2-sys1-cust
phys. IP Knoten 2 (YaST)	218.1.17.101		soco2-sys2-cust
OpenScape 4000, Plattform Administration (Portal)	218.1.17.102		
OpenScape 4000 Assistant	218.1.17.103		
OpenScape 4000 CSTA	218.1.17.104		
CCA	218.1.17.105		
CCB	218.1.17.106		
NGS	218.1.17.107		
Default Gateway/Router	218.1.17.254		
ETH4,	Corosync LAN		
	IP-Adresse	Netzmaske	Hostname
phys. IP Knoten 1 (YaST)	10.1.187.1	255.255.255.0	soco2-sys1
phys. IP Knoten 2 (YaST)	10.1.187.2		soco2-sys2
ETH5 & ETH6	Atlantic LAN		

Beispiel: Kunden-LAN und IPDA-LAN befinden sich in unterschiedlichen Subnetzen.

Tabelle 8: Duplex: Infrastrukturplanung - Kunden-LAN und IPDA-LAN in unterschiedlichen Subnetzen

ETH0	Kunden-LAN		
	IP-Adresse	Netzmaske	Hostname
phys. IP Knoten 1 (YaST)	218.1.17.100	255.255.255.0	soco2-sys1-cust
phys. IP Knoten 2 (YaST)	218.1.17.101		soco2-sys2-cust
OpenScape 4000, Plattform Administration (Portal)	218.1.17.102		
OpenScape 4000 Assistant	218.1.17.103		
OpenScape 4000 CSTA	218.1.17.104		
Default Gateway/Router	218.1.17.254		
ETH2,	IPDA LAN		

	IP-Adresse	Netzmaske	Hostname
phys. IP Knoten 1 (YaST)	172.16.2.100	255.255.255.0	soco2-sys1-ipda
phys. IP Knoten 2 (YaST)	172.16.2.101		soco2-sys2-ipda
CCA	172.16.2.105		
CCB	172.16.2.106		
NGS	172.16.2.107		
Default Router	172.16.2.254		
ETH4,	Corosync LAN		
	IP-Adresse	Netzmaske	Hostname
Schnittstelle			
phys. IP Knoten 1 (YaST)	10.1.187.1	255.255.255.0	soco2-sys1
phys. IP Knoten 2 (YaST)	10.1.187.2		soco2-sys2
ETH5 & ETH6	Atlantic LAN		

Separated Duplex

Beispiel: Kunden-LAN und IPDA-LAN befinden sich im selben Subnetz.

Tabelle 9: Separated Duplex Infrastrukturplanung - Kunden-LAN und IPDA-LAN im selben Subnetz

Kunden-LAN und IPDA-LAN				
	IP-Adresse	Netzmaske	Hostname	Schnittstelle
OpenScape 4000, Plattform Administration (Portal)	218.1.17.102			
OpenScape 4000 Assistant	218.1.17.103			
OpenScape 4000 CSTA	218.1.17.104			
CCA	218.1.17.105			
CCB	218.1.17.106			
NGS	218.1.17.107			
Default Gateway/ Router	218.1.17.254			

phys. IP Knoten 1 (YaST)	218.1.17.100	255.255.255.0	soco2-sys1-cust	ETH0/ BOND0/
phys. IP Knoten 2 (YaST)	218.1.17.101		soco2-sys2-cust	VLAN100
phys. IP Quorum (YaST)	218.1.17.99		soco2-quorum-adm	ETH1
Corosync LAN				
	IP-Adresse	Netzmaske	Hostname	Schnittstelle
phys. IP Knoten 1 (YaST)	10.1.187.1	255.255.255.0	soco2-sys1	ETH4/ BOND2/
phys. IP Knoten 2 (YaST)	10.1.187.2		soco2-sys2	VLAN300
phys. IP Quorum (YaST) ¹	10.1.187.3		soco2-quorum	ETH0
Atlantic LAN				
				Schnittstelle
Schnittstelle				ETH5/ BOND3
Schnittstelle				ETH6/ BOND3

Beispiel: Kunden-LAN und IPDA-LAN befinden sich in unterschiedlichen Subnetzen.

Tabelle 10: Separated Duplex Infrastrukturplanung - Kunden-LAN und IPDA-LAN in unterschiedlichen Subnetzen

Kunden-LAN				
	IP-Adresse	Netzmaske	Hostname	Schnittstelle
OpenScape 4000, Plattform Administration (Portal)	218.1.17.102			
OpenScape 4000 Assistant	218.1.17.103			
OpenScape 4000 CSTA	218.1.17.104			
Default Gateway/ Router	218.1.17.254			

¹ Für Quorum kann eine geeignete Schnittstelle gewählt werden, z. B. eth0

phys. IP Knoten 1 (YaST)	218.1.17.100	255.255.255.0	soco2-sys1-cust	ETH0/ BOND0/ VLAN100
phys. IP Knoten 2 (YaST)	218.1.17.101		soco2-sys2-cust	
phys. IP Quorum (YaST)	218.1.17.99		soco2-quorum-adm	ETH1
IPDA LAN				
	IP-Adresse	Netzmaske	Hostname	Schnittstelle
phys. IP Knoten 1 (YaST)	172.16.2.100	255.255.255.0	soco2-sys1-ipda	ETH2/ BOND1/ VLAN200
phys. IP Knoten 2 (YaST)	172.16.2.101		soco2-sys2-ipda	
CCA	172.16.2.105			
CCB	172.16.2.106			
NGS	172.16.2.107			
Default Router	172.16.2.254			
Corosync LAN				
	IP-Adresse	Netzmaske	Hostname	Schnittstelle
phys. IP Knoten 1 (YaST)	10.1.187.1	255.255.255.0	soco2-sys1	ETH4/ BOND2/ VLAN300
phys. IP Knoten 2 (YaST)	10.1.187.2		soco2-sys2	
phys. IP Quorum (YaST) ²	10.1.187.3		soco2-quorum	ETH0
Atlantic LAN				
				Schnittstelle
Schnittstelle				ETH5/ BOND3
Schnittstelle				ETH5/ BOND3

Separated Duplex mit integriertem SoftGate

Anmerkung: Die SoftGate-Funktion "SIP Load Balancer" wird in diesem Szenario nicht unterstützt. (Die "SIP Load Balancer"-Funktion ist nur bei einer "SoftGate Standalone"-Bereitstellung verwendbar).

² Für Quorum kann eine geeignete Schnittstelle gewählt werden, z. B. eth0

Beispiel: Kunden-LAN und IPDA-LAN befinden sich im selben Subnetz.

Tabelle 11: Separated Duplex Infrastrukturplanung - Kunden-LAN und IPDA-LAN im selben Subnetz

Kunden-LAN und IPDA-LAN				
	IP-Adresse	Netzmaske	Hostname	Schnittstelle
OpenScape 4000, Plattform Administration (Portal)	218.1.17.102	255.255.255.0	soco2-sys1-cust	ETH0/ BOND0/ VLAN100
OpenScape 4000 Assistant	218.1.17.103			
OpenScape 4000 CSTA	218.1.17.104			
CCA	218.1.17.105			
CCB	218.1.17.106			
NGS	218.1.17.107			
Default Gateway/ Router	218.1.17.254			
phys. IP Knoten 1 (YaST)	218.1.17.100	255.255.255.0	soco2-sys1-cust	ETH0/ BOND0/ VLAN100
phys. IP Knoten 2 (YaST)	218.1.17.101		soco2-sys2-cust	VLAN100
phys. IP Quorum (YaST)	218.1.17.99		soco2-quorum-adm	ETH1
SoftGate-Konfigurationsdaten				
NCUI	218.1.17.108			
AP-interne IP (DL)	192.168.1.23	255.255.255.0		
Corosync LAN				
	IP-Adresse	Netzmaske	Hostname	Schnittstelle
phys. IP Knoten 1 (YaST)	10.1.187.1	255.255.255.0	soco2-sys1	ETH4/ BOND2/ VLAN300
phys. IP Knoten 2 (YaST)	10.1.187.2		soco2-sys2	VLAN300
phys. IP Quorum (YaST) ³	10.1.187.3		soco2-quorum	ETH0
Atlantic LAN				

³ Für Quorum kann eine geeignete Schnittstelle gewählt werden, z. B. eth0

		Schnittstelle
Schnittstelle		ETH5/ BOND3
Schnittstelle		ETH6/ BOND3

Beispiel: Kunden-LAN und IPDA-LAN befinden sich in unterschiedlichen Subnetzen.

Tabelle 12: Separated Duplex Infrastrukturplanung - Kunden-LAN und IPDA-LAN in unterschiedlichen Subnetzen

Kunden-LAN				
	IP-Adresse	Netzmaske	Hostname	Schnittstelle
OpenScape 4000, Plattform Administration (Portal)	218.1.17.102			
OpenScape 4000 Assistant	218.1.17.103			
OpenScape 4000 CSTA	218.1.17.104			
Default Gateway/ Router	218.1.17.254			
phys. IP Knoten 1 (YaST)	218.1.17.100	255.255.255.0	soco2-sys1-cust	ETH0/ BOND0/
phys. IP Knoten 2 (YaST)	218.1.17.101		soco2-sys2-cust	VLAN100
phys. IP Quorum (YaST)	218.1.17.99		soco2-quorum-adm	ETH1
IPDA LAN				
	IP-Adresse	Netzmaske	Hostname	Schnittstelle
phys. IP Knoten 1 (YaST)	172.16.2.100	255.255.255.0	soco2-sys1-ipda	ETH2/ BOND1/
phys. IP Knoten 2 (YaST)	172.16.2.101		soco2-sys2-ipda	VLAN200
CCA	172.16.2.105			
CCB	172.16.2.106			
NGS	172.16.2.107			
Default Router	172.16.2.254			

	SoftGate-Konfigurationsdaten			
NCUI	172.16.2.108			
AP-interne IP (DL)	192.168.1.23	255.255.255.0		
Corosync LAN				
	IP-Adresse	Netzmaske	Hostname	Schnittstelle
phys. IP Knoten 1 (YaST)	10.1.187.1	255.255.255.0	soco2-sys1	ETH4/ BOND2/
phys. IP Knoten 2 (YaST)	10.1.187.2		soco2-sys2	VLAN300
phys. IP Quorum (YaST) ⁴	10.1.187.3		soco2-quorum	ETH0
Atlantic LAN				
				Schnittstelle
Schnittstelle				ETH5/ BOND3
Schnittstelle				ETH5/ BOND3

APE

Anmerkung: Ab V8 wird APE nur auf der DSCXL-Hardware unterstützt.

Beispiel: Kunden-LAN und IPDA-LAN befinden sich im selben Subnetz.

Wichtig: Die für APE angegebene NGS-IP-Adresse muss der IP-Adresse entsprechen, die auf dem Hostsystem eingegeben wurde.

Tabelle 13: APE: Infrastrukturplanung - Kunden-LAN und IPDA-LAN im selben Subnetz

ETH0	Kunden-LAN und IPDA-LAN		
	IP-Adresse	Netzmaske	Hostname
phys. IP (YaST)	218.1.17.110	255.255.255.0	APE-23
OpenScape 4000, Plattform Administration (Portal)	218.1.17.112		
OpenScape 4000 Assistant	218.1.17.113		

⁴ Für Quorum kann eine geeignete Schnittstelle gewählt werden, z. B. eth0

OpenScape 4000 CSTA	218.1.17.114		
CCAP (APESU des Hostsystems)	218.1.17.115		
NGS (des Host)	218.1.17.117		
Default Gateway/Router	218.1.17.254		
	IP-Adressen des Hostsystem		
CCA	218.1.17.105		
ETH5 & ETH6	Atlantic LAN		

Beispiel: Kunden-LAN und IPDA-LAN befinden sich in unterschiedlichen Subnetzen.

Tabelle 14: APE: Infrastrukturplanung - Kunden-LAN und IPDA-LAN in unterschiedlichen Subnetzen

ETH0	Kunden-LAN		
	IP-Adresse	Netzmaske	Hostname
phys. IP (YaST)	218.1.17.110	255.255.255.0	APE-23
OpenScape 4000, Plattform Administration (Portal)	218.1.17.112		
OpenScape 4000 Assistant	218.1.17.113		
OpenScape 4000 CSTA	218.1.17.114		
Default Gateway/Router	218.1.17.254		
ETH2,	IPDA LAN		
	IP-Adresse	Netzmaske	Hostname
phys. IP (YaST)	172.16.2.110	255.255.255.0	APE-23-ipda
CCAP (APESU des Hostsystems)	172.16.2.115		
NGS (des Host)	172.16.2.117		
Default Gateway/Router	172.16.2.254		
	IP-Adressen des Hostsystem		
CCA	172.16.2.105		
ETH5 & ETH6	Atlantic LAN		

Standalone SoftGate

Anmerkung: Bei der OpenScape 4000 EcoBranch gibt es zwei redundante LAN/WAN-Ports. Alle Einstellungen und Funktionen entsprechen denen von OpenScape Access.

Anmerkung: Die Konfiguration der OpenScape 4000 Plattform Administration (Portal) ist in einigen Bereitstellungen optional. Wenn die IP-Adresse der OpenScape 4000 Plattform Administration (Portal) nicht konfiguriert ist, kann unter der NCUI IP-Adresse auf diese zugegriffen werden: **https://ncui_ip_address:8443**

Beispiel: Kunden-LAN und IPDA-LAN gehören demselben Subnetz an (Direktverbindung).

Tabelle 15: Standalone SoftGate: Infrastrukturplanung - Kunden-LAN und IPDA-LAN im selben Subnetz (Direktverbindung)

ETH0	Kunden-LAN und IPDA-LAN		
	IP-Adresse	Netzmaske	Hostname
phys. IP (YaST)	218.1.17.110	255.255.255.0	OpenScapeAccess
OpenScape 4000 Plattform Administration (Portal) - optional	218.1.17.106		
Default Gateway/Router	218.1.17.254		
	SoftGate-Konfigurationsdaten		
NCUI	218.1.17.123		
AP-interne IP (DL)	198.168.1.23	255.255.255.0	
	IP-Adressen des Hostsystem		
CCA	218.1.17.105		
ETH1	Atlantic LAN		

Beispiel: Kunden-LAN und IPDA-LAN gehören demselben Subnetz an (Netzwerkverbindung)

Tabelle 16: Standalone SoftGate: Infrastrukturplanung - Kunden-LAN und IPDA-LAN im selben Subnetz (Netzwerkverbindung)

ETH0	Kunden-LAN und IPDA-LAN		
	IP-Adresse	Netzmaske	Hostname
phys. IP (YaST)	218.1.17.110	255.255.255.0	OpenScapeAccess

OpenScape 4000 Plattform Administration (Portal) - optional	218.1.17.106		
Default Gateway/Router	218.1.17.254		
	SoftGate-Konfigurationsdaten		
NCUI	218.1.17.123	255.255.255.0	
	IP-Adressen des Hostsystem		
CCA	172.16.2.105		
ETH1	Atlantic LAN		

Beispiel: Kunden-LAN und IPDA-LAN gehören unterschiedlichen Subnetzen an (Direktverbindung)

Tabelle 17: Standalone SoftGate: Infrastrukturplanung - Kunden-LAN und IPDA-LAN in unterschiedlichen Subnetzen (Direktverbindung)

ETH0	Kunden-LAN		
	IP-Adresse	Netzmaske	Hostname
phys. IP (YaST)	218.1.17.110	255.255.255.0	OpenScapeAccess
OpenScape 4000 Plattform Administration (Portal) - optional	218.1.17.105		
Default Gateway/Router	218.1.17.254		
ETH1	IPDA LAN		
	IP-Adresse	Netzmaske	Hostname
phys. IP (YaST)	172.16.2.110	255.255.255.0	OpenScapeAccess-ipda
Default Gateway/Router	172.16.2.254		
	SoftGate-Konfigurationsdaten		
NCUI	172.16.2.123		
AP-interne IP (DL)	198.168.1.23	255.255.255.0	
	IP-Adressen des Hostsystem		
CCA	172.16.2.105		

Beispiel: Kunden-LAN und IPDA-LAN gehören unterschiedlichen Subnetzen an (Netzwerkverbindung)

Tabelle 18: Standalone SoftGate: Infrastrukturplanung - Kunden-LAN und IPDA-LAN in unterschiedlichen Subnetzen (Netzwerkverbindung)

ETH0	Kunden-LAN		
	IP-Adresse	Netzmaske	Hostname
phys. IP (YaST)	218.1.17.110	255.255.255.0	OpenScapeAccess
OpenScape 4000 Plattform Administration (Portal) - optional	218.1.17.105		
Default Gateway/Router	218.1.17.254		
ETH1	IPDA LAN		
	IP-Adresse	Netzmaske	Hostname
phys. IP (YaST)	172.168.2.110	255.255.255.0	OpenScapeAccess-ipda
Default Gateway/Router	172.168.2.254		
	SoftGate-Konfigurationsdaten		
NCUI	172.168.2.123	255.255.255.0	
	IP-Adressen des Hostsystem		
CCA	172.16.2.105		

Survivable

Anmerkung: Bei der OpenScape 4000 EcoBranch gibt es zwei redundante LAN/WAN-Ports. Alle Einstellungen und Funktionen entsprechen denen von OpenScape Access.

Wichtig: Einige Bedingungen erfordern eine Neuinstallation der Software auf OSA500. Wenn OSA500 als Survivable SoftGate verwendet werden soll, muss das installierte System (Plattform) die gleiche Basisversion (Minor Release/Fix Release-Version) haben wie die OpenScape 4000 (z. B. bei einem R0.6.0 Switch muss auch die OSA500 mit R0.6.0 installiert werden). Ist dies nicht der Fall, schlägt OpenScape Backup & Restore vom Assistant (HBR) für AP-Emergency fehl. Es handelt sich hier um ein normales Verhalten (wie es für APE und Backup & Restore üblich ist) und nicht um einen Fehler. Der umgekehrte Fall ist ebenfalls möglich, also wenn die auf dem Switch installierte Version niedriger ist als die auf der ausgelieferten OSA500 vorinstallierte Softwareversion. In diesem Fall muss der Switch hochgerüstet werden, bevor die Synchronisation über HBR aktiviert wird.

Beispiel: Kunden-LAN und IPDA-LAN gehören demselben Subnetz an (Direktverbindung).

Tabelle 19: Survivable: Infrastrukturplanung - Kunden-LAN und IPDA-LAN im selben Subnetz (Direktverbindung)

ETH0	Kunden-LAN und IPDA-LAN		
	IP-Adresse	Netzmaske	Hostname
phys. IP (YaST)	218.1.17.110	255.255.255.0	Surv-OpenScapeAccess
OpenScape 4000, Plattform Administration (Portal)	218.1.17.112		
OpenScape 4000 Assistant	218.1.17.113		
OpenScape 4000 CSTA	218.1.17.114		
CCA (APESU des Hostsystems)	218.1.17.115		
NGS (des Host)	218.1.17.117		
	SoftGate-Konfigurationsdaten		
NCUI	172.16.2.123		
AP-interne IP (DL)	192.168.1.23	255.255.255.240	
	IP-Adressen des Hostsystem		
CCA	218.1.17.105		
ETH1	Atlantic LAN		

Beispiel: Kunden-LAN und IPDA-LAN gehören demselben Subnetz an (Netzwerkverbindung)

Tabelle 20: Survivable: Infrastrukturplanung - Kunden-LAN und IPDA-LAN im selben Subnetz (Netzwerkverbindung)

ETH0	Kunden-LAN und IPDA-LAN		
	IP-Adresse	Netzmaske	Hostname
phys. IP (YaST)	218.1.17.110	255.255.255.0	Surv-OpenScapeAccess
OpenScape 4000, Plattform Administration (Portal)	218.1.17.112		
OpenScape 4000 Assistant	218.1.17.113		
OpenScape 4000 CSTA	218.1.17.114		
CCA (APESU des Hostsystems)	218.1.17.115		
NGS (des Host)	172.16.2.117		

	IP-Adressen des Hostsystem	
CCA	172.16.2.105	
ETH1	Atlantic LAN	

Beispiel: Kunden-LAN und IPDA-LAN gehören unterschiedlichen Subnetzen an (Direktverbindung)

Tabelle 21: Survivable: Infrastrukturplanung - Kunden-LAN und IPDA-LAN in unterschiedlichen Subnetzen (Direktverbindung)

ETH0	Kunden-LAN		
	IP-Adresse	Netzmaske	Hostname
phys. IP (YaST)	218.1.17.110	255.255.255.0	Surv-OpenScapeAccess
OpenScape 4000, Plattform Administration (Portal)	218.1.17.112		
OpenScape 4000 Assistant	218.1.17.113		
OpenScape 4000 CSTA	218.1.17.114		
ETH1	IPDA LAN		
phys. IP (YaST)	172.16.2.110	255.255.255.0	Surv-OpenScapeAccess-ipda
CCA (APESU des Hostsystems)	172.16.2.115		
NGS (des Host)	172.16.2.112		
Default Gateway/Router	172.16.2.254		
	IP-Adressen des Hostsystem		
CCA	172.16.2.105		

Beispiel: Kunden-LAN und IPDA-LAN gehören unterschiedlichen Subnetzen an (Netzwerkverbindung)

Tabelle 22: Survivable: Infrastrukturplanung - Kunden-LAN und IPDA-LAN in unterschiedlichen Subnetzen (Netzwerkverbindung)

ETH0	Kunden-LAN		
	IP-Adresse	Netzmaske	Hostname
phys. IP (YaST)	218.1.17.110	255.255.255.0	Surv-OpenScapeAccess
OpenScape 4000, Plattform Administration (Portal)	218.1.17.112		

OpenScape 4000 Assistant	218.1.17.113		
OpenScape 4000 CSTA	218.1.17.114		
ETH1	IPDA LAN		
phys. IP (YaST)	172.16.2.110	255.255.255.0	Surv-OpenScapeAccess-ipda
CCA (APESU des Hostsystems)	172.16.2.115		
NGS (des Host)	192.168.20.112		
Default Gateway/Router	172.16.2.254		
	IP-Adressen des Hostsystem		
CCA	172.16.2.105		

Enterprise Gateway

Beispiel: Kunden-LAN und IPDA-LAN gehören demselben Subnetz an (Direktverbindung).

Tabelle 23: Enterprise Gateway: Infrastrukturplanung - Kunden-LAN und IPDA-LAN im selben Subnetz (Direktverbindung)

ETH0	Kunden-LAN und IPDA-LAN		
	IP-Adresse	Netzmaske	Hostname
phys. IP (YaST)	218.1.17.110	255.255.255.0	EnterpriseGW
OpenScape 4000 Plattform Administration (Portal) - optional	218.1.17.106		
Default Gateway/Router	218.1.17.254		
	Enterprise Gateway-Konfigurationsdaten		
NCUI	218.1.17.123		
AP-interne IP (DL)	198.168.1.23	255.255.255.0	
	IP-Adressen des Hostsystem		
CCA	218.1.17.105		
ETH1	Atlantic LAN		

Beispiel: Kunden-LAN und IPDA-LAN gehören demselben Subnetz an (Netzwerkverbindung)

Tabelle 24: Enterprise Gateway: Infrastrukturplanung - Kunden-LAN und IPDA-LAN im selben Subnetz (Netzwerkverbindung)

ETH0	Kunden-LAN und IPDA-LAN		
	IP-Adresse	Netzmaske	Hostname
phys. IP (YaST)	218.1.17.110	255.255.255.0	EnterpriseGW
OpenScape 4000 Plattform Administration (Portal) - optional	218.1.17.106		
Default Gateway/Router	218.1.17.254		
	Enterprise Gateway-Konfigurationsdaten		
NCUI	218.1.17.123	255.255.255.0	
	IP-Adressen des Hostsystem		
CCA	172.16.2.105		
ETH1	Atlantic LAN		

Beispiel: Kunden-LAN und IPDA-LAN gehören unterschiedlichen Subnetzen an (Direktverbindung)

Tabelle 25: Enterprise Gateway: Infrastrukturplanung - Kunden-LAN und IPDA-LAN in unterschiedlichen Subnetzen (Direktverbindung)

ETH0	Kunden-LAN		
	IP-Adresse	Netzmaske	Hostname
phys. IP (YaST)	218.1.17.110	255.255.255.0	EnterpriseGW
OpenScape 4000 Plattform Administration (Portal) - optional	218.1.17.105		
Default Gateway/Router	218.1.17.254		
ETH1	IPDA LAN		
	IP-Adresse	Netzmaske	Hostname
phys. IP (YaST)	172.16.2.110	255.255.255.0	EnterpriseGWipda
Default Gateway/Router	172.16.2.254		
	SoftGate-Konfigurationsdaten		
NCUI	172.16.2.123		
AP-interne IP (DL)	198.168.1.23	255.255.255.0	
	IP-Adressen des Hostsystem		
CCA	172.16.2.105		

Beispiel: Kunden-LAN und IPDA-LAN gehören unterschiedlichen Subnetzen an (Netzwerkverbindung)

Tabelle 26: Enterprise Gateway: Infrastrukturplanung - Kunden-LAN und IPDA-LAN in unterschiedlichen Subnetzen (Netzwerkverbindung)

ETH0	Kunden-LAN		
	IP-Adresse	Netzmaske	Hostname
phys. IP (YaST)	218.1.17.110	255.255.255.0	EnterpriseGW
OpenScape 4000 Plattform Administration (Portal) - optional	218.1.17.105		
Default Gateway/Router	218.1.17.254		
ETH1	IPDA LAN		
	IP-Adresse	Netzmaske	Hostname
phys. IP (YaST)	172.168.2.110	255.255.255.0	EnterpriseGWipda
Default Gateway/Router	172.168.2.254		
	Konfigurationsdaten des OpenScape 4000 SoftGate		
NCUI	172.168.2.123	255.255.255.0	
	IP-Adressen des Hostsystem		
CCA	172.16.2.105		

OpenScape Enterprise Gateway Survivable

Beispiel: Kunden-LAN und IPDA-LAN gehören demselben Subnetz an (Direktverbindung).

Tabelle 27: Survivable Enterprise Gateway: Infrastrukturplanung - Kunden-LAN und IPDA-LAN im selben Subnetz (Direktverbindung)

ETH0	Kunden-LAN und IPDA-LAN		
	IP-Adresse	Netzmaske	Hostname
phys. IP (YaST)	218.1.17.110	255.255.255.0	SurvEnterpriseGW
OpenScape 4000, Plattform Administration (Portal)	218.1.17.112		
OpenScape 4000 Assistant	218.1.17.113		
OpenScape 4000 CSTA	218.1.17.114		
CCA (APESU des Hostsystems)	218.1.17.115		
NGS (des Host)	218.1.17.117		

	Enterprise Gateway-Konfigurationsdaten		
NCUI	172.16.2.123		
AP-interne IP (DL)	192.168.1.23	255.255.255.240	
	IP-Adressen des Hostsystem		
CCA	218.1.17.105		
ETH1	Atlantic LAN		

Beispiel: Kunden-LAN und IPDA-LAN gehören demselben Subnetz an (Netzwerkverbindung)

Tabelle 28: Survivable Enterprise Gateway: Infrastrukturplanung - Kunden-LAN und IPDA-LAN im selben Subnetz (Netzwerkverbindung)

ETH0	Kunden-LAN und IPDA-LAN		
	IP-Adresse	Netzmaske	Hostname
phys. IP (YaST)	218.1.17.110	255.255.255.0	SurvEnterpriseGW
OpenScape 4000, Plattform Administration (Portal)	218.1.17.112		
OpenScape 4000 Assistant	218.1.17.113		
OpenScape 4000 CSTA	218.1.17.114		
CCA (APESU des Hostsystems)	218.1.17.115		
NGS (des Host)	172.16.2.117.117		
	IP-Adressen des Hostsystem		
CCA	172.16.2.105		
ETH1	Atlantic LAN		

Beispiel: Kunden-LAN und IPDA-LAN gehören unterschiedlichen Subnetzen an (Direktverbindung)

Tabelle 29: Survivable Enterprise Gateway: Infrastrukturplanung - Kunden-LAN und IPDA-LAN in unterschiedlichen Subnetzen (Direktverbindung)

ETH0	Kunden-LAN		
	IP-Adresse	Netzmaske	Hostname
phys. IP (YaST)	218.1.17.110	255.255.255.0	SurvEnterpriseGW
OpenScape 4000, Plattform Administration (Portal)	218.1.17.112	255.255.255.0	
OpenScape 4000 Assistant	218.1.17.113		

OpenScape 4000 CSTA	218.1.17.114		
ETH1	IPDA LAN		
phys. IP (YaST)	172.16.2.110	255.255.255.0	SurvEnterpriseGWipda
CCA (APESU des Hostsystems)	172.16.2.115		
NGS (des Host)	172.16.2.112		
Default Gateway/Router	172.16.2.254		
	IP-Adressen des Hostsystem		
CCA	172.16.2.105		

Beispiel: Kunden-LAN und IPDA-LAN gehören unterschiedlichen Subnetzen an (Netzwerkverbindung)

Tabelle 30: Survivable Enterprise Gateway: Infrastrukturplanung - Kunden-LAN und IPDA-LAN in unterschiedlichen Subnetzen (Netzwerkverbindung)

ETH0	Kunden-LAN		
	IP-Adresse	Netzmaske	Hostname
phys. IP (YaST)	218.1.17.110	255.255.255.0	SurvEnterpriseGW
OpenScape 4000, Plattform Administration (Portal)	218.1.17.112		
OpenScape 4000 Assistant	218.1.17.113		
OpenScape 4000 CSTA	218.1.17.114		
ETH1	IPDA LAN		
phys. IP (YaST)	172.16.2.110	255.255.255.0	SurvEnterpriseGWipda
CCA (APESU des Hostsystems)	172.16.2.115		
NGS (des Host)	192.168.20.112		
Default Gateway/Router	172.16.2.254		
IP-Adressen des Hostsystem			
CCA	172.16.2.105		

2.2.2 Wie Sie ein bootfähiges 4K-ISO-Image auf einen USB-Stick brennen

Voraussetzungen: USB-Stick mit 8 GB Mindestkapazität, aber maximal 16 GB.

Benutzer können ihre bevorzugte Handhabung für USB-Sticks wählen, wobei sowohl unetbootin als auch rufus erfolgreich getestet wurden.

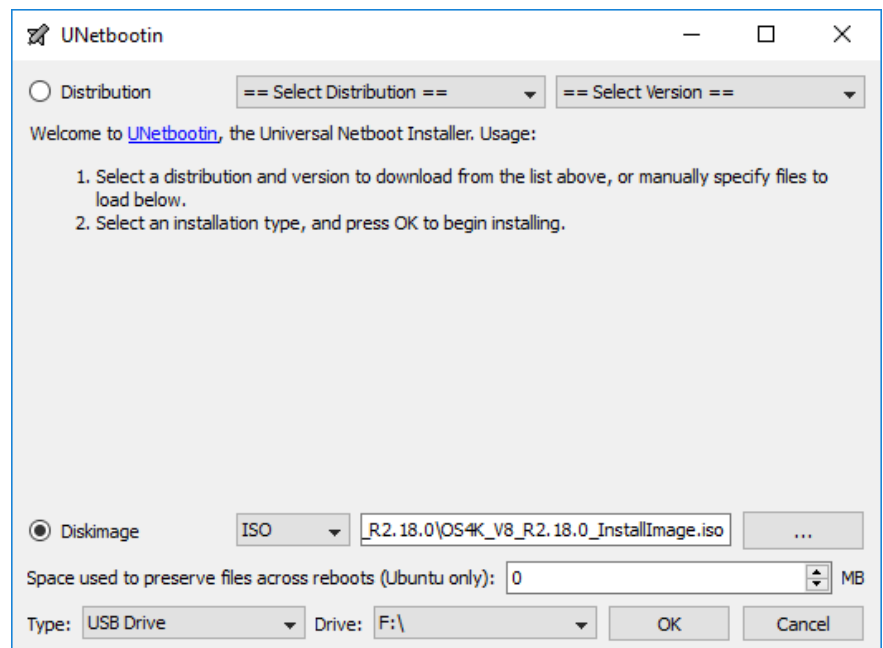
- Unetbootin sollte eine Mindestversion von unetbootin-windows-585.exe verwenden, da in früheren Versionen Prüfsummenprobleme festgestellt wurden.
- HPUSBDisk funktioniert ab Windows 10 nicht mehr und kann aus lizenzrechtlichen Gründen nicht mehr ausgeliefert werden. Eine Anleitung für die Windows-Formatierung ist auf dem ISO-Stick unter folgendem Pfad zu finden: ISO_Root_Dir\DriversAndTools\USB_Flash_Tools\HowTo_write_bootable_ISO_Image_on_USB_Stick.pdf
- Das Tool Rufus (nicht in der ISO-Installation enthalten) bietet sowohl Formatierungs- als auch ISO-Brennfunktionen. Die minimale laborgeprüfte Version war V2.11.

Wichtig: Wählen Sie dabei "FAT32" als Dateisystem. Wenn der USB-Stick bereits mit NTFS formatiert ist, formatieren Sie ihn bitte neu mit FAT32. Benutzer können ihre bevorzugte Handhabung für USB-Sticks wählen, wobei sowohl unetbootin als auch rufus erfolgreich getestet wurden.

Beispiel:

1) Starten Sie das Programm unetbootin-windows-625.exe und

- Wählen Sie die Option "DiskImage" aus.
- Übernehmen Sie die Auswahl für die Option "ISO".
- Klicken Sie auf die Schaltfläche "..." und wählen Sie aus der OpenScape 4000-Installation die 4K-Installations-ISO aus.
- Lassen Sie unter "Typ" die Option "USB Drive" (USB-Laufwerk) aktiviert.
- Achten Sie unter Drive (Laufwerk) darauf, den Laufwerksbuchstaben des USB-Sticks auszuwählen.



- Klicken Sie auf OK.
 - Warten Sie, bis der Vorgang abgeschlossen ist.
 - Klicken Sie auf Exit (Beenden).
- #### 2) Verwenden Sie "Safely Remove Hardware" (Hardware sicher entfernen), um den Stick zu entfernen.

- 3) Entfernen Sie den Stick, nachdem Sie die Meldung erhalten, dass ein sicheres Entfernen nun möglich ist.

2.2.3 Installation und Konfiguration von SLES und Konfiguration von OpenScape 4000

In diesem Abschnitt werden folgende Aufgaben beschrieben:

- 1) Installation und
- 2) Konfiguration von OpenScape 4000.

Alle diese Schritte werden in einer XML-Datei konfiguriert und anschließend automatisch gestartet und ausgeführt.

Anmerkung: Um von der alten Hardware auf die neue Hardware zu migrieren, müssen die XML-Konfigurationsdateien aus dem bestehenden System generiert und die alte MAC-Adresse durch die MAC-Adresse aus der neuen Hardware ersetzt werden.

2.2.3.1 Mögliche Bereitstellung je nach Festplattengröße

Tabelle 31: Mögliche Bereitstellung je nach Festplattengröße

Mögliche Bereitstellung	Größe der Festplatte [GB]		
	>= 250	75 - 250	30 - 75
Alle Bereitstellungen	x	---	---
Standalone SoftGate ⁵	x	x	---
Quorum	x	x	x

2.2.3.2 Vorbereitung

- 1) Erfassen Sie eine MAC-Adresse einer beliebigen LAN-Schnittstelle der Hardware, die installiert werden soll.
- 2) Füllen Sie die XML-Konfigurationsdatei aus.

Informationen zur XML -Datei finden Sie in [Abschnitt 10.3, "XML-Konfigurationsdatei"](#).

Vorlagen und Beispiele für verschiedene XML-Konfigurationsdateien für alle Bereitstellungstypen sind im XML Config File Generator (unter Datei > Laden von Dateien) enthalten, die mit der neuesten ComWin-Version verfügbar sind.

⁵ Gilt auch für das SoftGate auf dem Quorumsknoten

- 3) Kopieren Sie die komplett ausgefüllte(n) XML-Datei(en) in den Ordner **config** auf dem Installationsmedium.

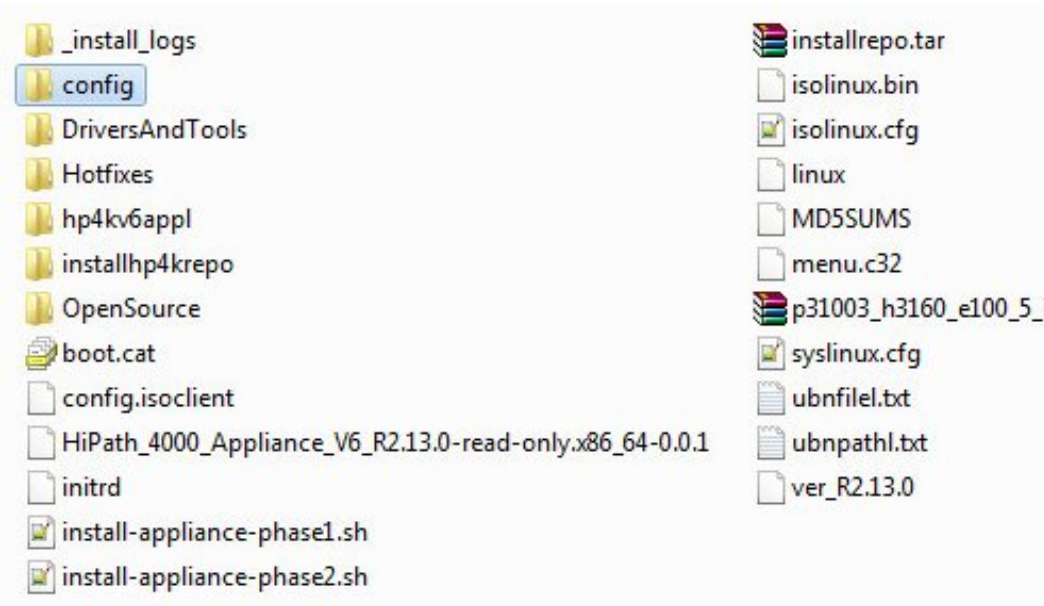


Figure 7: XML-Dateispeicherort auf dem Installationsmedium

Das ist der Fall für die folgenden Deployments:

- Standalone OpenScape 4000 SoftGate
- Simplex mit integriertem OpenScape 4000 SoftGate (kann auf OSA500, ESX VMware, EcoServer und Branch installiert werden)
- OpenScape Access 500/OpenScape 4000 Branch
- Survivable OpenScape 4000 SoftGate
- OpenScape Access 500/OpenScape 4000 Branch mit Survivable OpenScape 4000 SoftGate

NOTICE: Für die manuelle OpenScape 4000 SoftGate-Konfiguration (keine intialcfg-Datei/softGateInitialConfiguration-Abschnitt in der Konfiguration XML-Datei) finden Sie in [Abschnitt 2.3, "Manuelle OpenScape 4000 SoftGate-Konfiguration"](#).

2.2.3.3 Vorbereitung eines USB-Sticks für die Installation

Im Rahmen der Erstinstallation ist es möglich, eine oder mehrere HotFixes zu übertragen und/oder zu aktivieren.

Hier ist eine Übersicht über die HotFix-Typen und die von ihnen jeweils unterstützten Aktionen:

Tabelle 32: HotFix-Typen und ihre unterstützten Aktionen

HotFix Type	Supported Actions
Assistant HotFix	Automatic activation (default), manual activation

HotFix Type	Supported Actions
CSTA HotFix	Automatic activation (default), manual activation
Loadware HotFix	Automatic activation
RMX HotFix	Manual activation
Platform HotFix	Automatic activation

Zum Einbinden von HotFixes in den Installationsvorgang müssen diese in den HotFixes-Ordner des Installationsmediums kopiert werden. Die ZIP-/TAR-HotFix-Dateien dürfen nicht extrahiert werden. Sie müssen so nach / Hotfixes auf das Installationsmedium kopiert werden, wie sie von SWS heruntergeladen wurden. Stellen Sie sicher, dass die folgende Zeile in der *.XML-Installationsdatei enthalten ist:

assistantHF=auto, cstaHF=auto, rmxHF=auto

Assistant- und CSTA-HotFixes können bei Bedarf auch lediglich auf das System übertragen und nicht automatisch aktiviert werden. (Dies wird in der oben stehenden Tabelle als "manuelle Aktivierung" bezeichnet.)

Bei manueller Aktivierung werden die HotFixes in der Assistant Software Activation-GUI angezeigt, sobald die Installation von OpenScape 4000 und alle anderen automatischen HotFix-Aktivierungsvorgänge abgeschlossen sind.

2.2.3.4 Erste Installation mit Auto GENDB

Ab V8 R1 kann eine RMX-REGEN-Datei verwendet werden, um die RMX-DB automatisch während des FI-Prozesses zu generieren.

Die REGEN-Datei hat dasselbe Format wie das System, wenn AMO STA-REGEN verwendet wird.

Ein CODEW kann in der REGEN-Datei vorhanden sein, anderenfalls wird der von Assistant generierte CODEW der Zahlungsfrist verwendet.

Die RMX-Generierung wird parallel zur Assistant-Installation gestartet. Status und Fortschritt können in der Benutzeroberfläche des Plattform-Portals im Menü Status -> "Installationsstatus" überprüft werden.

USB-Installationen:

Die RMX REGEN-Datei muss auf den USB-Stick in das "config"-Verzeichnis neben die erste Installations-XML kopiert werden und muss im Namen eine MAC-Adresse enthalten, die mit einer LAN-Schnittstelle des Systems und der Erweiterung ".samtxt" übereinstimmt, z. B.:


MAC-Adresse.samtxt

Computer > Removable Disk (E:) > config			
Share with ▾ New folder			
Name ^	Date modified	Type	Size
.bl	26-Jul-17 12:23	BL File	2 KB
.inv.cfgxmls	26-Jul-17 12:23	CFGXMLS File	2 KB
always_autoinstall	26-Jul-17 12:23	File	0 KB
firstinst-netw.sh	26-Jul-17 12:23	SH File	318 KB
firstinst-netw-SYS1_00-20-ce-fb-02-d9.xml	03-Aug-17 14:46	XML Document	3 KB
REGEN_SYS1_V8R1.17_00-20-ce-fb-02-d9.samtxt	03-Aug-17 14:47	SAMTXT File	242 KB

VMware ESXi-Installationen:

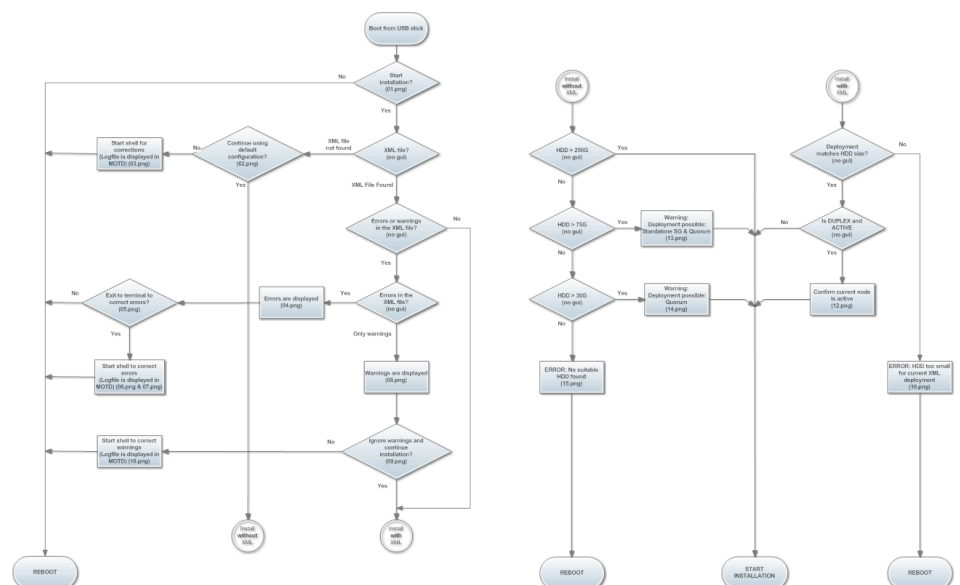
Bei Installationen auf virtuellen Maschinen muss die RMX-REGEN-Datei in das Disketten-Image eingefügt werden.

Anmerkung: Wegen der Größenbeschränkungen für Disketten-Images muss die REGEN-Datei zusätzlich im ZIP-Format komprimiert werden und die Erweiterung ".samtxt.zip" haben, d. h. der Dateiname muss wie folgt lauten: *MAC-address*.samtxt.zip

 REGEN_SYS1_V8R1.17_00-20-ce-fb-02-d9.samtxt.zip	03-Aug-17 14:47	Compressed (zipped) Folder	242 KB
---	-----------------	----------------------------	--------

Anmerkung: Bei Floppy-Nutzung sehen Sie sich bitte Folgendes an: OpenScape 4000 V8 Installation, Konfiguration und Migration -> 3.5 Service PC & 3.6.2 Vorbereitungen auf dem Service PC

2.2.3.5 Installationsvorgang mit Monitor/Tastatur



Installationsverfahren - Überblick

- 1) Öffnen Sie das Boot Menü um das Boot Device auszuwählen.
 - DSCXL: F11 direkt, F11 Konsole
 - EcoServer/Branch: F11 direkt, F11 Konsole
 - OSA500: F10,
- 2) Achtung: Wenn Sie F11 verwenden, um im BIOS das Boot Device auszuwählen, wird das verwendete USB-Gerät ggf. zweimal angezeigt (d. h. einmal mit UEFI-Präfix und einmal ohne). Wählen Sie das Boot Device ohne UEFI-Präfix aus.

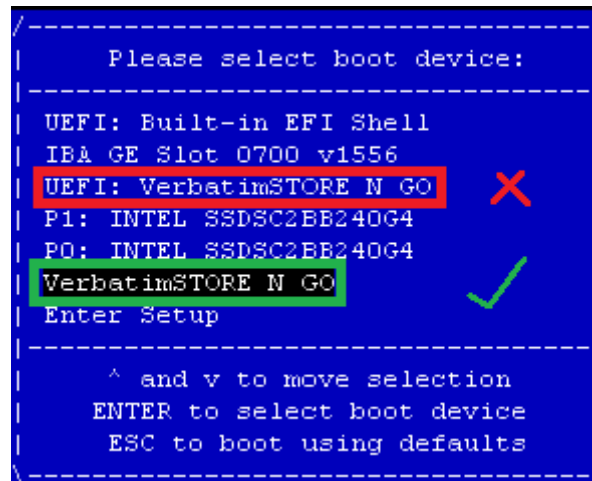


Abbildung 8: Boot Device-Auswahl im BIOS

- 3) Starten Sie den Rechner vom Installationsmedium (USB-Stick). Sie werden aufgefordert, die Installation zu starten oder den Rechner neu zu booten.

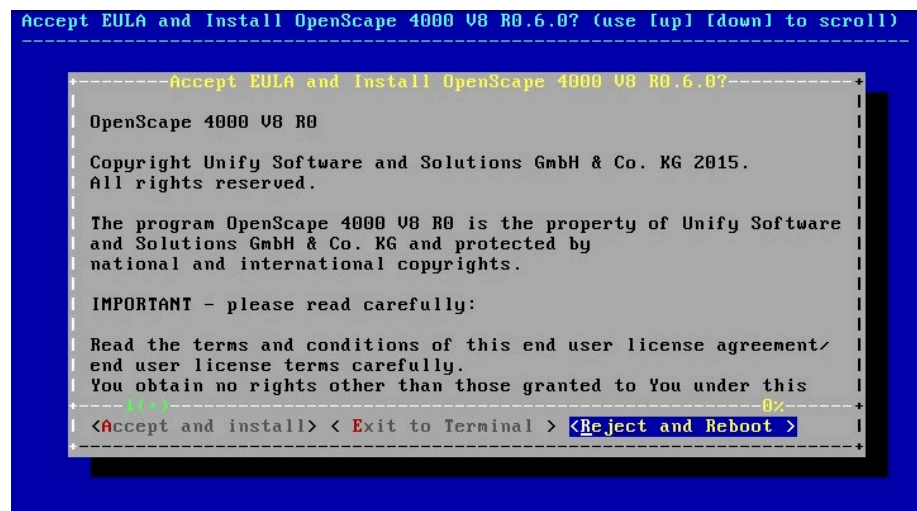


Abbildung 9: Erstinstallation - EULA akzeptieren

4) Überprüfen Sie, ob eine kompatible XML-Konfigurationsdatei verfügbar ist.

Wenn Sie **Yes** (Ja, Installation starten) wählen, wird geprüft, ob der **config**-Ordner auf dem Installationsmedium eine mit der Hardware kompatible XML-Datei enthält.

Fall 1: XML-Konfigurationsdatei gefunden

Wenn eine XML-Konfigurationsdatei mit der MAC-Adresse einer der Schnittstellen des Systems gefunden wird, wird diese XML-Datei auf Fehler hinsichtlich der Linux-Konfigurationsdaten überprüft.

Fall 1-1: XML-Konfigurationsdatei enthält keine Fehler/Warnungen

Während der Installation wird der verfügbare Speicherplatz auf der Festplatte geprüft, um festzustellen, ob die Bereitstellung zur Größe des Festplattenspeichers passt.

Weitere Informationen finden Sie in [5 on page 55](#).

Fall 1-2: XML-Konfigurationsdatei enthält Fehler

Wenn die XML-Datei Fehler enthält, wird die Installation mit Fehlermeldungen abgebrochen und ein Fehlerprotokoll im Ordner **_install_logs** des Installationsmediums angelegt.

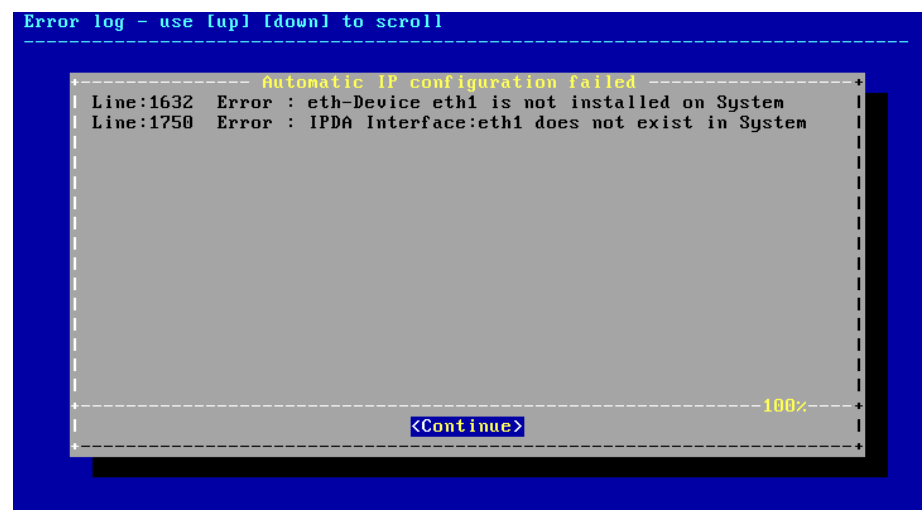


Abbildung 10: Erstinstallation - XML-Konfigurationsdatei mit Fehlern

Klicken Sie auf **Continue** (Weiter).

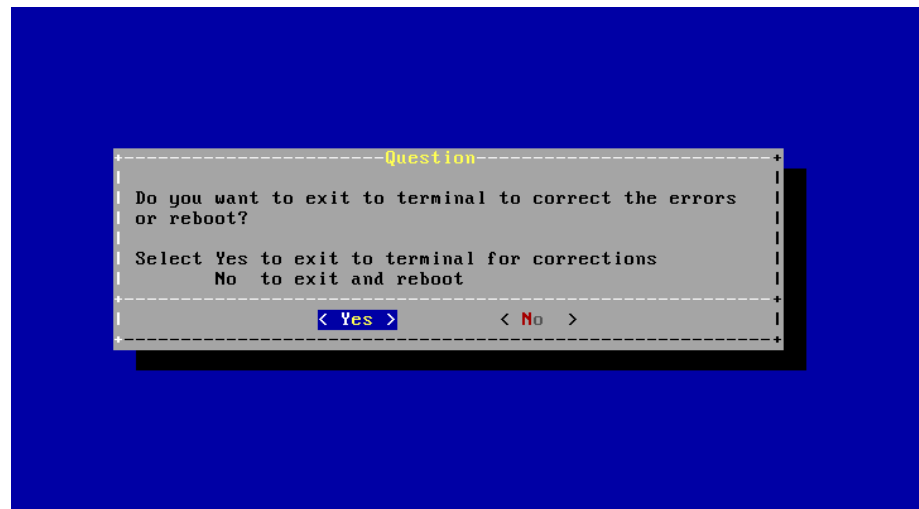


Abbildung 11: Erstinstallation - XML-Konfigurationsdatei mit Fehlern

Wählen Sie **Yes** (Ja), um zum Terminal zu gelangen, damit Sie die erforderlichen Änderungen vornehmen und den Rechner anschließend neu starten können, oder **No** (Nein), um die Installation zu beenden und den Rechner neu zu starten.

Wenn Sie **Yes** (Ja) wählen, wird die Protokolldatei angezeigt.

5) Beispiele:

- a) Mehrere entsprechende XML-Konfigurationsdateien mit einer MAC-Adresse dieses Servers:

```
ERROR: Automatic IP configuration returned error code 1. The logfile is :
Line:3409 Error :There are more than one XML-File, that corresponds with a
MAC-Address from this Server.

File 1 : /var/opt/firstinstall/firstinst-netw-SepDup_inst.xml
File 2 : /var/opt/firstinstall/firstinst-netw-test_inst1.xml

Please copy only the right one into the directory and remove all others.

You can use vi to edit the XML file (e.g. firstinst-netw-Duplex_D1.xml).
The system will reboot after exiting this shell.
To exit this shell type exit and press <ENTER>.

linux-hipath4000v6:/livecd/config #
```

Abbildung 12: Erstinstallation - Protokolldatei für eine XML-Konfigurationsdatei mit Fehlermeldungen

- b) Falsche Bereitstellung in XML-Konfigurationsdatei

```
ERROR: Automatic IP configuration returned error code 1. The logfile is :
Line:3783 Error : Deployment simplex is not defined Please use one of
following Deployment

The installation has detected the following XML file matching the system:
firstinst-netw-test_inst1.xml.
You can use vi to edit this XML file.
To exit this shell type exit and press <ENTER>.

linux-hipath4000v6:/livecd/config #
```

Abbildung 13: Erstinstallation - Protokolldatei für eine XML-Konfigurationsdatei mit Fehlermeldungen

Fall 1-3: XML-Konfigurationsdatei enthält Warnungen

Wenn nur Warnungen in der XML-Konfigurationsdatei gefunden werden, werden diese angezeigt.

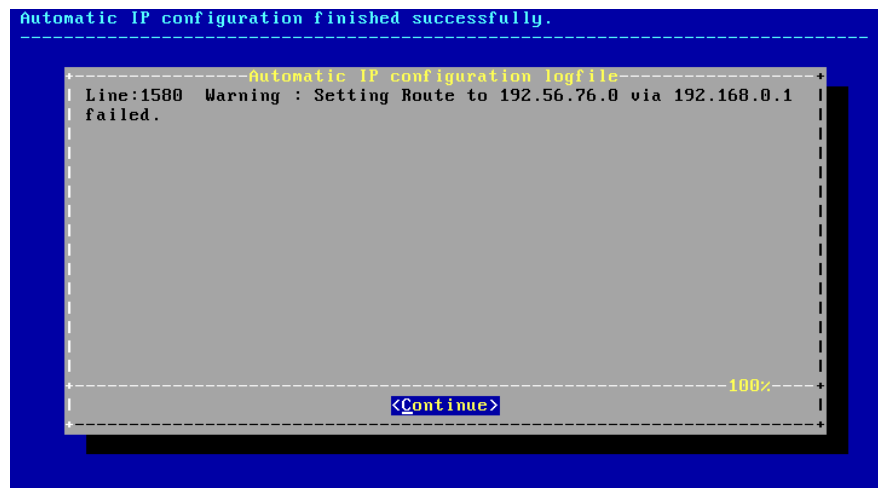


Abbildung 14: Erstinstallation - XML-Konfigurationsdatei mit Warnungen

Klicken Sie auf **Continue** (Weiter). Der folgende Bildschirm wird angezeigt:

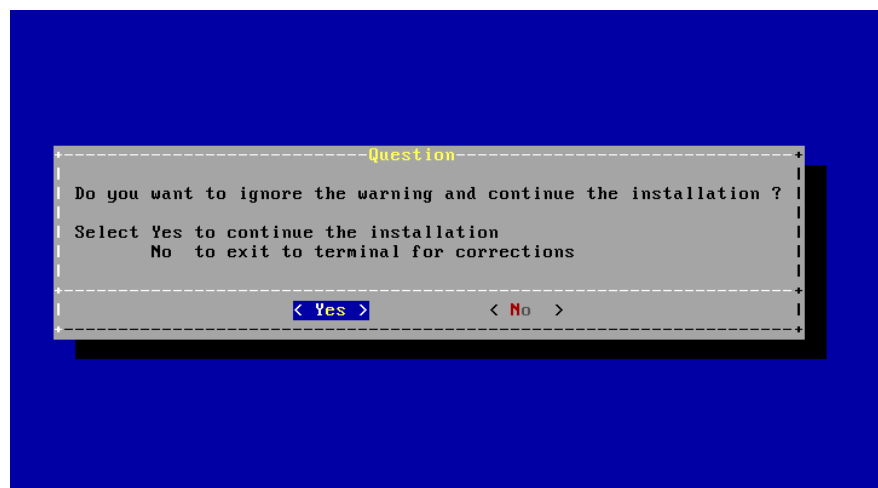


Abbildung 15: Erstinstallation - XML-Konfigurationsdatei mit Warnungen

Sie können **Yes** (Ja) wählen, um die Warnung zu ignorieren und mit der Installation fortzufahren, oder **No** (Nein), um eine Terminalsitzung zu öffnen und die entsprechenden Korrekturen vorzunehmen.

Wenn Sie **Yes** (Ja) wählen, wird der verfügbare Speicherplatz auf der Festplatte geprüft, um festzustellen, ob die Bereitstellung zur Größe des verfügbaren Festplattenspeichers passt.

Weitere Informationen finden Sie in [5 on page 55](#).

Wenn Sie **No** (Nein) wählen, wird der folgende Bildschirm angezeigt:

```
Automatic IP configuration finished successfully.
Warning: Automatic IP configuration logfile contains some warnings :
Line:1580 Warning : Setting Route to 192.56.76.0 via 192.168.0.1 failed.

Use vi to edit the XML file (e.g. firstinst-netw-test_inst1.xml).
The system will reboot after exiting this shell.
To exit this shell type exit and press <ENTER>.

simplex6:/livecd/config #
```

Abbildung 16: Erstinstallation - Protokolldatei für eine XML-Konfigurationsdatei mit Warnungen

Fall 2: Keine XML-Konfigurationsdatei gefunden

Wenn keine XML-Konfigurationsdatei mit der MAC-Adresse der Hardware vorhanden ist, auf der die Installation ausgeführt wird, können Sie den Installationsvorgang mithilfe einer Standardkonfiguration fortsetzen oder die Shell starten, um die erforderlichen Korrekturen vorzunehmen.

Bei Angabe eines falschen *.XML-Dateinamens erscheint die Warnmeldung "No corresponding XML file... (Keine entsprechende XML-Datei...)". Der Dateiname muss mit firstinst-netw-*.xml beginnen.

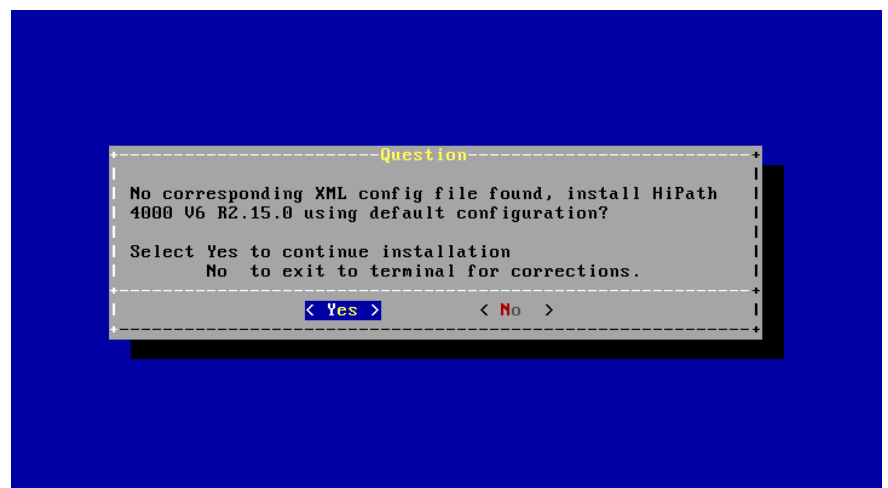


Abbildung 17: Erstinstallation - XML-Konfigurationsdatei nicht gefunden

Fall 2-1: Installation mit Standardkonfiguration

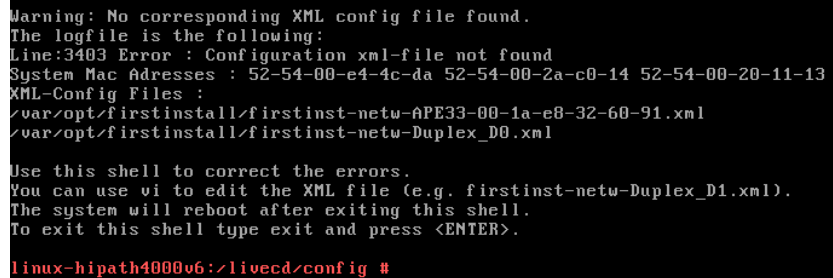
Wenn Sie **Yes** (Ja) wählen, wird die Installation gestartet, aber eine Standard-IP-Adresse für eth0 konfiguriert (IP-Adresse **192.168.0.2 /24**).

In diesem Fall wird empfohlen, die Installation mit einer ordnungsgemäß konfigurierten XML-Datei zu wiederholen.

Während der Installation wird nun der verfügbare Speicherplatz auf der Festplatte geprüft, um die möglichen Bereitstellungsvarianten zu bestimmen (weitere Informationen finden Sie im Abschnitt [5 on page 55](#)).

Fall 2-2: Shell starten und Korrekturen vornehmen

Wenn Sie **No** (Nein) wählen, wird die folgende Warnung angezeigt. Sie haben die Möglichkeit, den Fehler zu beheben.



```
Warning: No corresponding XML config file found.
The logfile is the following:
Line:3403 Error : Configuration xml-file not found
System Mac Addresses : 52-54-00-e4-4c-da 52-54-00-2a-c0-14 52-54-00-20-11-13
XML-Config Files :
/var/opt/firstinstall/firstinst-netw-APE33-00-1a-e8-32-60-91.xml
/var/opt/firstinstall/firstinst-netw-Duplex_D0.xml

Use this shell to correct the errors.
You can use vi to edit the XML file (e.g. firstinst-netw-Duplex_D1.xml).
The system will reboot after exiting this shell.
To exit this shell type exit and press <ENTER>.

linux-hipath4000v6:/livecd/config #
```

Abbildung 18: Erstinstallation - Warnung, keine entsprechende XML-Konfigurationsdatei gefunden

Anmerkung: Überprüfen Sie, ob die XML-Datei im richtigen Verzeichnis vorhanden ist. Ist dies der Fall, dann Sie überprüfen bitte, ob sie die korrekte MAC-Adresse des Knotens enthält. Die XML-Datei kann mit dem Editor vi bearbeitet werden.

c) Überprüfung des verfügbaren Festplattenspeichers

Fall 1: Installation mit XML-Konfigurationsdatei: Passt die Bereitstellung zum verfügbaren Festplattenspeicher?

Fall 1-1: Bereitstellung passt zum verfügbaren Festplattenspeicher

Wenn die Festplatte für die Bereitstellung der XML-Konfigurationsdatei geeignet ist, wird überprüft, ob es sich bei der aktuellen Bereitstellung um

eine Duplex- oder eine Separated Duplex-Bereitstellung handelt (siehe [6 on page 57](#)).

Fall 1-2: Bereitstellung passt nicht zum verfügbaren Festplattenspeicher

Wenn die Festplatte zu klein für die Bereitstellung der XML-Konfigurationsdatei ist, wird die folgende Fehlermeldung angezeigt und der Rechner neu gestartet.



Abbildung 19: Erstinstallation - Festplattengröße entspricht nicht der Bereitstellung

Fall 2: Installation ohne XML-Konfigurationsdatei: Größe der Festplatte?

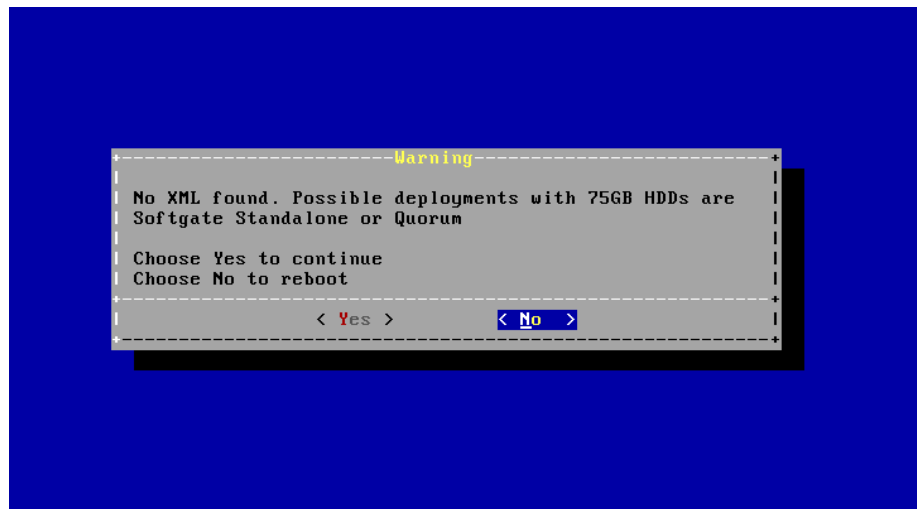
Fall 2-1: Festplattengröße beträgt mindestens 250 GB

Alle Bereitstellungen sind möglich und die Installation wird gestartet.

Fall 2-2: Festplattengröße zwischen 75 GB und 250 GB

Es sind nur die Bereitstellungen Standalone SoftGate, SoftGate on Quorum und Quorum möglich. Die folgende Warnung wird angezeigt.

Abbildung 20: Erstinstallation - Bereitstellungen mit Festplatte zwischen 75 GB und 250 GB



Wenn die Bereitstellung der XML-Konfigurationsdatei zu der festgestellten Festplattengröße passt, wählen Sie **Yes** (Ja). Die Installation wird gestartet. Andernfalls wählen Sie **No** (Nein). Der Rechner wird neu gestartet.

Fall 2-3: Festplattengröße zwischen 30 GB und 75 GB

Die einzig mögliche Bereitstellung ist Quorum.

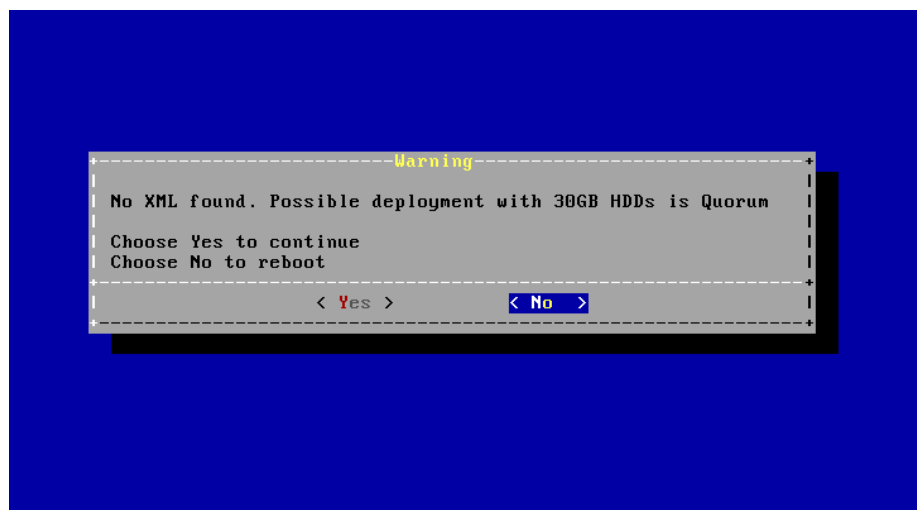


Abbildung 21: Erstinstallation - Bereitstellung mit Festplattengröße zwischen 30 GB und 75 GB

Wenn es sich bei der Bereitstellung der XML-Konfigurationsdatei um einen Quorum-Knoten handelt, wählen Sie **Yes** (Ja). Die Installation wird gestartet. Andernfalls wählen Sie **No** (Nein). Der Rechner wird neu gestartet.

Fall 2-4: Keine geeignete Festplatte gefunden

Wenn keine geeignete Festplatte vorhanden ist, wird die folgende Meldung angezeigt und der Rechner neu gestartet.

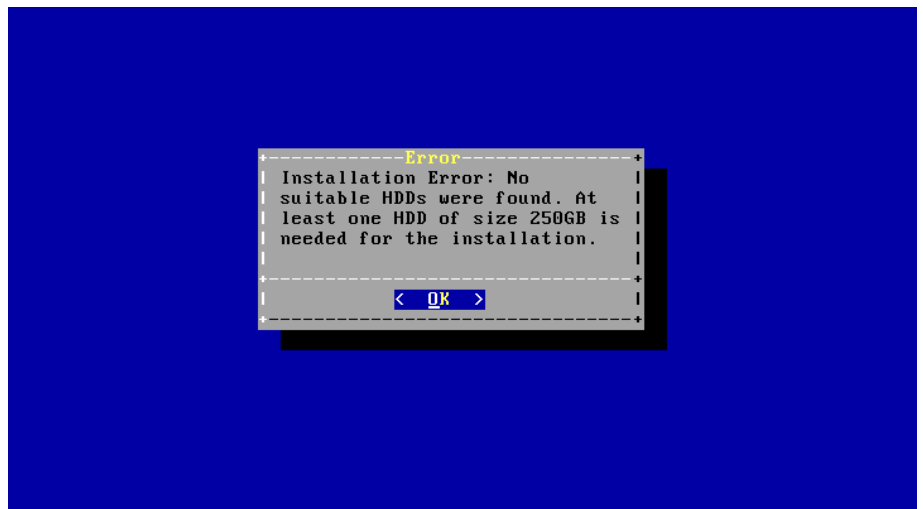


Abbildung 22: Erstinstallation - keine geeignete Festplatte gefunden

6) Duplex-/Separated Duplex-Bereitstellung:

Im Falle einer Duplex- oder Separated Duplex-Bereitstellung wird der folgende Bildschirm angezeigt:

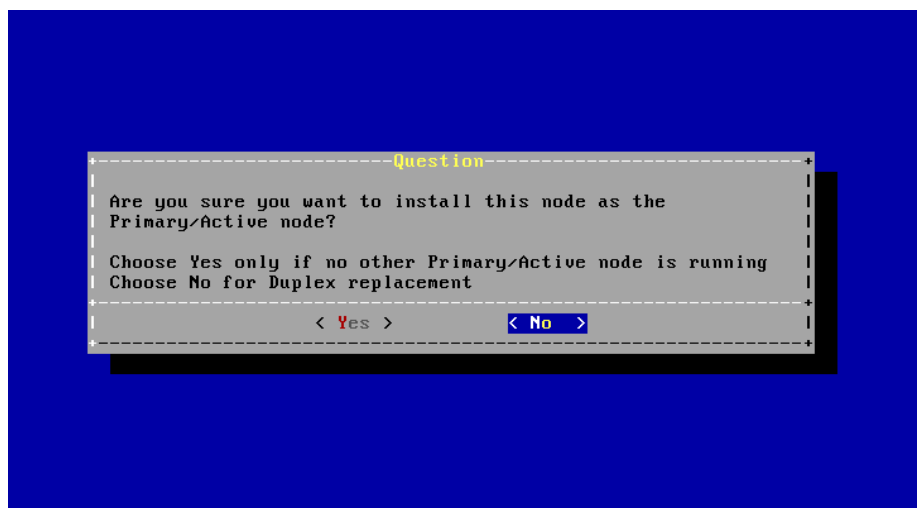


Abbildung 23: Erstinstallation - Duplex/Separated Duplex-Bereitstellung

Wenn Sie **Yes** (Ja) wählen, ist der aktuelle Knoten nach dem Systemstart der [Aktiver/m Knoten](#).

Wichtig: Wählen Sie nur dann **Yes** (Ja), wenn kein anderer primärer/aktiver Knoten vorhanden ist.

Für eine Duplex-Ersatzinstallation müssen Sie **No** (Nein) wählen.

- 7) Wenn die Installation erfolgreich abgeschlossen wurde, werden Sie in einer Meldung aufgefordert, das Installationsmedium zu entfernen und OK zu drücken, um das System neu zu starten.



Abbildung 24: Installation erfolgreich abgeschlossen

- 8) Nach dem Neustart wird das System von der installierten Software auf der Festplatte gestartet und ist unter den für die angeschlossenen LAN-Schnittstellen konfigurierten IP-Adressen erreichbar.

2.2.3.6 Installation nur mit dem OLED-Display und der "ON" -Taste

Ab V8 R1.19 kann die OpenScape 4000-Installation auf DSCXL (nur APE-Bereitstellung)/EcoServer/EcoBranch nur noch mit dem OLED-Display und der links davon platzierten Taste "ON" durchgeführt werden. Es ist nicht notwendig, einen Monitor oder eine Tastatur anzuschließen, da die notwendigen Installationsschritte durch einen einzigen Knopf bestätigt werden.

Anmerkung: Bei DSCXL HW trägt die Schaltfläche "ON" die Bezeichnung "DISPLAY ON".

Schritte für die Installation mit OLED:

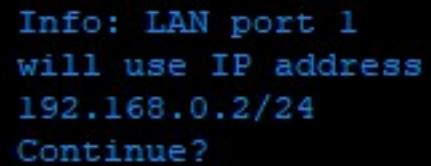
1. Stecken Sie den USB-Stick ein, entfernen Sie alle HGs/SSDs und schalten Sie den EcoServer/ EcoBranch ein. Warten Sie ca. 2-3 Minuten, bis das System "Installation Startup" anzeigt.	
2. Das OLED-Display sollte die Meldung "EULA akzeptieren?" anzeigen. Drücken Sie die Taste "ON".	
3. Warten Sie auf die nächste Eingabeaufforderung, in der der Benutzer aufgefordert wird, die Installation mit OLED fortzusetzen.	

Drücken Sie die Taste "ON" und warten Sie, bis die folgende Meldung in der OLED angezeigt wird:	<pre>Detected disks: 0 Insert disk(s) and press OLED to continue ...</pre>
<p>4. Fügen Sie an dieser Stelle abhängig von Ihrer Bereitstellung ein oder zwei HDs/SSDs ein. Warten Sie, bis die richtige Anzahl von Festplatten auf der OLED angezeigt wird. Drücken Sie die "ON" -Taste, um mit der Installation fortzufahren</p> <p>Hinweis: Die Anzeige wird alle 30 Sekunden automatisch aktualisiert.</p>	<pre>Detected disks: 1 Insert disk(s) and press OLED to continue ...</pre>
<p>Hinweis: Im Falle von Duplex- oder GSD-Systemen muss der in der XML-Datei als primär konfigurierte Knoten bestätigt werden. Drücken Sie zur Bestätigung die "ON" -Taste.</p>	<pre>Choose Primary? Input required</pre>
<p>Hinweis: Falls in der XML-Datei ein Fehler entdeckt wurde (z. B. fehlende Pflichtparameter), wird Folgendes angezeigt:</p>	<pre>Error in XML. For more details remove USB device and check logs</pre>
Während der Installation von OpenScape 4000 zeigt die OLED die folgende Meldung an:	<pre>Install progress 0% Installation started</pre>
5. Nach Abschluss der Installation entfernen Sie das USB-Laufwerk und drücken erneut die Taste "ON", um das OpenScape4000-System zum ersten Mal neu zu starten und zu starten.	<pre>INSTALLATION FINISHED Remove media now and reboot Input required</pre>
Wenn eine Installation ohne XML durchgeführt wird, zeigt die OLED die folgende Meldung an. Drücken Sie die "ON" -Taste, um ohne XML mit der Installation fortzufahren	<pre>No XML found. Continue? Input required</pre>

Erstinstallation

Manuelle Konfiguration des OpenScape 4000 SoftGate

Bei einer Installation ohne XML zeigt das OLED die IP-Adresse an, die der ersten physikalischen LAN-Schnittstelle des Eco Server/ EcoBranch zugewiesen wird. Sie können die erste physische LAN-Schnittstelle mit einem Netzwerk verbinden, in dem DHCP Server ausgeführt wird, und dann versucht der Eco-Server/Branch, eine IP-Adresse zu erhalten. Dies wird zur Verifizierung auf der OLED angezeigt. Fahren Sie fort, indem Sie die Taste "ON" drücken. Am Ende der Installation ist das OpenScape4000 Platform Portal über diese IP-Adresse erreichbar. Wenn keine DHCP-Antwort empfangen wird, lautet die Standard-IP-Adresse/Netzmaske 192.168.0.2/255.255.255.0.



```
Info: LAN port 1
will use IP address
192.168.0.2/24
Continue?
```

Anmerkung: Im Falle eines Fehlers entfernen Sie den USB Stick, überprüfen Sie die Protokolle im Verzeichnis "usb_stick_root/_install_logs", korrigieren Sie das Problem und starten Sie erneut mit Schritt 1. Es wird empfohlen, den ECO Server/EcoBranch vor Schritt 1 abzuschalten und für DSCXL2 alle HDs zu entfernen, den USB Stick anzuschließen und die HW Reset Taste zu verwenden, um zu Schritt 1 zurückzukehren.

2.2.3.7 Empfohlener GSD-Installationsablauf

Empfohlener und effizientester Ablauf der Erstinstallation für Separated Duplex:

- Installation des Quorum-Knotens
- Installation von Knoten B
- Installation von Knoten A als aktiver Knoten.

2.3 Manuelle Konfiguration des OpenScape 4000 SoftGate

Wenn zum Zeitpunkt der Installation des Systems auf dem Installationsmedium keine initialcfg-Datei/softGateInitialConfiguration Abschnitt in der XML-Konfigurationsdatei vorhanden war, können Sie nun das OpenScape 4000 SoftGate in der OpenScape 4000 Plattform Administration (Portal) manuell konfigurieren.

NOTICE: Bitte verwenden Sie XML, um während der Installation das Bonding zu konfigurieren, und weisen Sie den Bond statt eth als zu verwendende Schnittstelle zu. Wenn das SG bereits installiert ist, können Sie den Bond über das Tool „recover-H4K.sh“ konfigurieren und ihn anschließend

über das WBM zuweisen. Für weitere Details siehe [Kapitel 6](#), „Wiederherstellungs-/Rekonfigurationswerkzeug verwenden“.

Starten Sie die OpenScape 4000 Plattform Administration (Portal) und rufen Sie den LAN-Assistenten auf:

System > LAN-Konfiguration > LAN#Assistent:

SoftGate Node 1 IPDA Settings (basic)

Type of Hardware	EcoServer ▾
Enable AP Emergency	<input type="checkbox"/>
Direct Link for signalling	<input checked="" type="checkbox"/>
IP Address of the AP in the OpenScape 4000 LAN Segment	10.9.44.60
Netmask of the OpenScape 4000 LAN Segment	255.255.255.0
IP Address of the SoftGate Default Gateway	10.9.44.254
IP Address of the CC-A	10.9.44.100
IP Address of the CC-B	10.9.44.101
IP Address for the AP Emergency	0.0.0.0
IP Address of the AP in the AP internal Net Segment	192.168.108.60
Netmask of the AP internal Net Segment	255.255.255.0
Enable OpenScape Access Xlink	<input type="checkbox"/> Not possible for Duplex
Xlink Network Address	0.0.0.0

Figure 25: OpenScape 4000 SoftGate-Konfiguration - Grundlegende IPDA-Einstellungen

SoftGate IPDA Settings (advanced)

Enable VLAN Tagging

☐

VLAN ID

0

TOS-Byte for sig.proc. over Ethernet LAN

104

Server Port for signalling connection

4000

Basic LAN Redundancy

☐ For LAN Redundancy a bond should now be used.

Basic LAN Interface

eth0

OpenScape Access Xlink LAN Interface

eth2

Management LAN Redundancy

☐ For Management LAN Redundancy a bond should now be used.

Management LAN Interface

Where a bond is required, but none is available, please create one via XML and the Recovery Tool.

Back

Cancel

Next

Figure 26: OpenScape 4000 SoftGate-Konfiguration - Erweiterte IPDA-Einstellungen

SoftGate IPv6 Settings

IP Stack

IPv4 and IPv6 (dual stack)

IPv6 Address of the AP in the OpenScape 4000 LAN Segment

::

IPv6 Prefix of the AP in the OpenScape 4000 LAN Segment

64

IP address of the NGS server [IPv4 or IPv6]

0.0.0.0

LTU

60

SoftGate Master Encryption Key (MEK) Management

Master Encryption Key (MEK):

Note:

All resources will be restarted.
Portal will be unavailable for a while.

Back

Cancel

Submit

Figure 27: OpenScape 4000 SoftGate-Konfiguration - Grundlegende IPDA-Einstellungen

NOTICE:

Bei OpenScape 4000 V8 R2 oder höher gilt das oben beschriebene Verfahren auch für die Konfiguration eines Integrated SoftGate auf Enterprise Gateway, nachdem es unter System>LAN-Konfiguration>System aktiviert wurde.

Bei OpenScape 4000 V10 R1 oder höher gilt das oben beschriebene Verfahren auch für die Konfiguration eines

Integrated SoftGate auf einem Duplex-System, nachdem es unter System > LAN-Konfiguration > System aktiviert wurde.

HW Platform

OpenScape 4000 Communication Server (EcoServer)

Deployment Separated Duplex ▾ *

Integrated SoftGate on Node 1 ☒

Integrated SoftGate on Node 2 ☐

Integrated SoftGate on Quorum Node ☒

RTM (Rear Transition Module) not configured ▾ *

Next

Figure 28: OpenScape 4000 SoftGate-Konfiguration - Integrated SoftGate

2.4 Zero Local-Konfiguration für Stand-Alone OpenScape 4000 SoftGate

2.4.1 Leistungsmerkmalbeschreibung

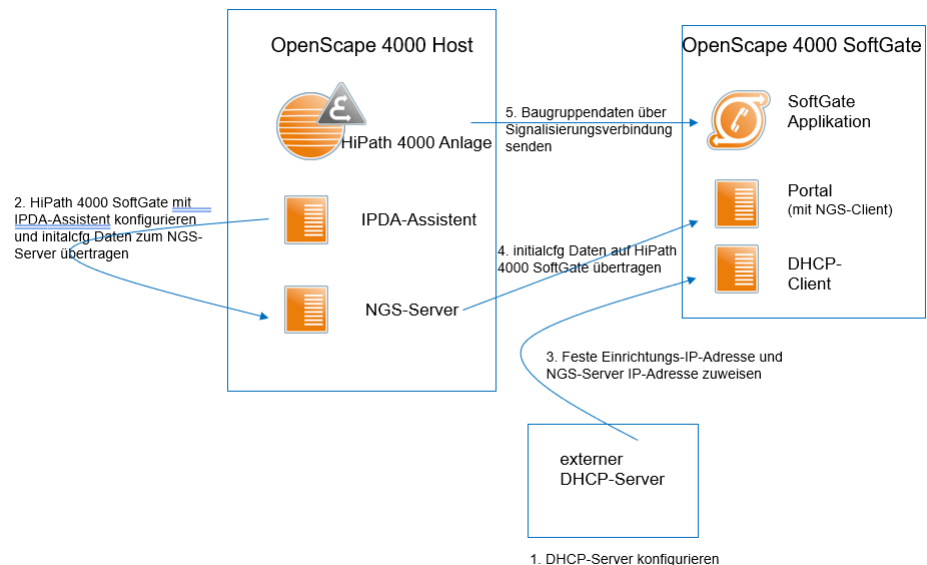


Abbildung 29: Konfigurationsüberblick für Zero Local Konfiguration

Mit dem Leistungsmerkmal "Zero Local Konfiguration" wird die Erstinstallation eines stand-alone OpenScape 4000 SoftGate ohne jegliche lokale Konfiguration ermöglicht. Das OpenScape 4000 SoftGate kann an ein bestehendes System angeschlossen werden. Es wird dann, sobald die Verbindung zum Host-System besteht, automatisch ohne weiteres manuelles Eingreifen installiert und konfiguriert.

Hierfür wird unter anderem ein externer DHCP-Server benötigt. Zusätzlich wurde der NGS dahingehend erweitert, dass er neben der Datenverteilung von IPv6-Adressen nun auch das Leistungsmerkmal "Zero Local Konfiguration" unterstützt.

Voraussetzungen:

- DHCP-Server

Hierfür muss ein externer DHCP-Server zur Verfügung stehen. Diesem muss die MAC-Adresse des OpenScape 4000 SoftGates bekannt sein, an Hand derer er eine feste IPv4-Adresse für das OpenScape 4000 SoftGate zur Verfügung stellt. Diese IPv4-Adresse ist die Einrichtungs-IP-Adresse des OpenScape 4000 SoftGates, also die IP-Adresse mit der später auch die OpenScape 4000 Plattform Administration (Portal) erreicht werden kann.

Für die korrekte Konfiguration des DHCP-Servers beachten Sie bitte [Section 2.4.3, "Konfiguration \(Beispiel\)"](#).

- Die Konfiguration des OpenScape 4000 SoftGate muss über den IPDA-Assistenten erfolgen. Der IPDA-Assistent speichert die Daten für die Erstinstallation (initialcfg.xml) mit der Einrichtungs-IP-Adresse in der Datenbank des NGS-Servers im OpenScape 4000 Host ab.

Erstinstallation - Ablauf

Beim Starten des OpenScape 4000 SoftGate wird eine DHCP-Anforderung (DHCP Discover-Nachricht mit Option 60) für den Abruf der IP-Adresse

der OpenScape 4000 Plattform Administration (Portal) des OpenScape 4000 SoftGate gesendet. Wenn vom DHCP-Server eine IP-Adresse mit der herstellerspezifischen Option 43 übermittelt wird, die die NGS IP-Adresse enthält, kontaktiert das OpenScape 4000 SoftGate den NGS-Server und ruft seine Erstinstallationsdaten (initialcfg.xml) mit Hilfe der Einrichtungs-IP-Adresse ab. Schlägt der Start der Erstinstallation fehl, versucht das OpenScape 4000 SoftGate, aktualisierte Erstinstallationsdaten abzurufen (sofern vorhanden).

Wenn der NGS-Server nicht erreichbar ist, wird der Verbindungsversuch wiederholt, bis der NGS-Server erreichbar ist oder die Erstinstallationsdaten von Hand auf dem System bereitgestellt/erstellt werden.

Anschließend wird der Start des OpenScape 4000 SoftGate normal fortgesetzt. Das OpenScape 4000 SoftGate erhält die aktuellen Baugruppendaten über die Signalisierungsverbindung.

Weitere Szenarien

Abgesehen von der Erstinstallation sind noch weitere Szenarien möglich, da bei Konfigurationsänderungen, die die initialcfg-Datei betreffen, diese nicht nur wie üblich auf dem OpenScape 4000 SoftGate aktualisiert, sondern auch auf den NGS-Server übertragen wird.

- Austausch von Hardware

Beim Austausch von Hardware können die neuesten Installationsdaten für OpenScape 4000 SoftGate bereitgestellt werden.

Wenn die OpenScape 4000 SoftGate-Hardware ausgetauscht werden muss, stellt der NGS-Server die neuesten Erstinstallationsdaten bereit. Hierbei ist jedoch zu beachten, dass der DHCP-Server auch an die neue MAC-Adresse des OpenScape 4000 SoftGate angepasst werden muss.

- Fehlerhafte Konfiguration eines OpenScape 4000 SoftGate

Die Erstinstallationsdaten eines falsch konfigurierten OpenScape 4000 SoftGate können zurückgesetzt werden.

Wenn ein OpenScape 4000 SoftGate falsch konfiguriert ist, kann die initialcfg-Datei überschrieben werden. Dieser Vorgang wird durch den IPDA-Assistenten eingeleitet.

2.4.2 Serviceinformationen

- Dieses Leistungsmerkmal ist für Standalone OpenScape 4000 SoftGates freigegeben (OpenScape Access 500 oder OpenScape 4000 Branch).
- Dieses Leistungsmerkmal ist nur für IPv4-Adressen freigegeben.
- Es muss ein externer DHCP-Server zur Verfügung stehen, der folgende Anforderungen erfüllt:
 - Er muss in der Lage sein eine feste IPv4-Adresse mit der herstellerspezifischen Option 43 bereitzustellen.
 - Er muss eine IPv4-Adresse (Einrichtungs-IP-Adresse des OpenScape 4000 SoftGate) **und** einen Hostnamen für das OpenScape 4000 SoftGate an das OpenScape 4000 SoftGate liefern.
 - Die NGS IP-Adresse muss vom DHCP-Server als herstellerspezifische Option 43 bereitgestellt werden. Wenn die Herstelleroption nicht auf dem DHCP-Server konfiguriert ist, können die Erstinstallationsdaten nicht automatisch abgerufen werden. In diesem Fall muss OpenScape 4000

SoftGate manuell mit Hilfe der OpenScape 4000 Plattform Administration (Portal) bzw. per XML-Datei eingerichtet werden.

- Für die Verwendung dieses Leistungsmerkmals muss das OpenScape 4000 SoftGate mit dem IPDA-Assistenten konfiguriert werden.

Die dem OpenScape 4000 SoftGate im DHCP-Server zugewiesene Einrichtungs-IP-Adresse muss im IPDA-Assistenten als zusätzliche Information eingegeben werden.

- Die NGS IP-Adresse muss im LAN-Assistenten der OpenScape 4000 Plattform Administration (Portal) auf dem zentralen OpenScape 4000-Host konfiguriert werden. Die IP-Adresse des NGS-Servers muss vom IPDA-Netz aus erreichbar sein.
- Alle in der OpenScape 4000 SoftGate-Konfigurationstabelle des NGS-Servers registrierten OpenScape 4000 SoftGates werden in der OpenScape 4000 Plattform Administration (Portal) angezeigt und können dort gelöscht werden. Löschen bedeutet, dass das entsprechende OpenScape 4000 SoftGate aus der Datenbank des NGS-Servers entfernt wird.

System > SoftGates > Delete (Schaltfläche "Löschen")

Wichtig: Löschen Sie nur solche OpenScape 4000 SoftGates, die nicht mehr verwendet werden/vorhanden sind, d. h. zum Beispiel vorher im IPDA-Assistenten gelöscht wurden.

- Bei Konfigurationsänderungen, die die Erstinstallationsdatei betreffen, wird die initialcfg-Datei nicht nur lokal auf dem OpenScape 4000 SoftGate gespeichert, sondern auch auf dem NGS-Server aktualisiert.
- Soll das OpenScape 4000 SoftGate in einer Netzwerkumgebung mit getrenntem Kunden-LAN und IPDA-LAN eingerichtet werden, so ist zu beachten, dass der NGS-Server nur im IPDA-LAN erreichbar ist. In diesem Fall ist es nötig sowohl im Kunden-LAN, als auch im IPDA-LAN einen DHCP Server zur Verfügung zu stellen. Der DHCP Server im Kunden-LAN vergibt die IP-Adresse, unter der die OpenScape 4000 Plattform Administration (Portal) erreichbar sein soll. Der DHCP Server im IPDA-LAN muss die Anforderungen, die für dieses Leistungsmerkmal nötig sind, erfüllen. Details zur Konfiguration siehe [Section 2.4.3.2, "Zero Local-Konfiguration bei getrenntem Kunden- und IPDA-LAN"](#).

2.4.3 Konfiguration (Beispiel)

2.4.3.1 DHCP-Server-Konfiguration

Die DHCP-**Option 60** ist der **Vendor Class Identifier (VCI)**. Sie wird zur Identifikation eines Clients am Server verwendet. Der DHCP-Server beantwortet diese Anfragen mit der **Option 43**, um herstellerspezifische Informationen an den Client zu übermitteln. Eine detaillierte Beschreibung dieser Optionen finden Sie in der RFC 2132.

Beim Leistungsmerkmal "Zero Local-Konfiguration" sendet das OpenScape 4000 SoftGate in der DHCP-Discovery-Anforderung den **VCI(Vendor Class Identifier)-String SEN.Softgate**. Der DHCP-Server muss in der DHCP-Offer die **NGS-IP-Adresse** als Inhalt der **Option 43** übermitteln.

Der DHCP-Server muss die folgenden Optionen zur Verfügung stellen (Pflichtparameter):

- host-name
- vendor-encapsulated-options
- IP und Subnetzmaske
- routers

Gegebenenfalls akzeptiert der DHCP-Client auch die folgenden Optionen (wahlfreie Parameter):

- broadcast-address
- domain-name
- domain-name-servers
- time-offset
- ntp-servers

Beispielkonfiguration eines Linux DHCP-Servers (ISC)

```
option space SEN-SG;
option SEN-SG.ngs-ip-address code 1 = ip-address;
default-lease-time 14400;
ddns-update-style none;
# log the vendor-id into the lease file
set vendor-string = option vendor-class-identifier;
# vendor specific information: these parameters are valid only for clients
# belonging to a particular vendor class. The vendor class is identified by
# the value that the client sends with the vendor class identifier option.
class "SEN-Softgate" {
option SEN-SG.ngs-ip-address 172.15.3.13;
match if option vendor-class-identifier = "SEN.Softgate";
vendor-option-space SEN-SG;
}
subnet 172.15.3.0 netmask 255.255.255.0 {
option broadcast-address 172.15.3.255;
option routers 172.15.3.1;
option time-offset 3600;
range 172.15.3.220 172.15.3.229;
}
host pcie3-SG41 {
option subnet-mask 255.255.255.0;
option routers 172.15.3.1;
option SEN-SG.ngs-ip-address 172.15.3.13;
option ntp-server 192.1.1.253
option host-name "pcie3-SG41";
```

```
option domain-name-servers 172.28.12.19, 172.28.12.20;
option domain-name "global-intra.net";
hardware ethernet 00:1a:e8:3c:e5:b6;
fixed-address 172.15.3.40;
option time-offset 3600;
}
```

In der DHCP Server Konfiguration gibt es verschiedene Möglichkeiten für die Konfiguration der IP-Adressen des NGS-Servers:

- 1) Sie können die Option **SEN-SG.ngs-ip-address** dem Class-Bereich hinzufügen, wenn Sie für alle OpenScape 4000 SoftGates dieselbe IP-Adresse verwenden wollen (wie ein Standardwert).
- 2) Sie können die Option **SEN-SG.ngs-ip-address** dem Host-Bereich hinzufügen. Wenn Sie verschiedene NGS-Server verwenden, ist dieses Vorgehen zu bevorzugen.
- 3) Sie können die beiden Möglichkeiten mischen, wenn Sie einen Standard-NGS-Server definieren wollen und wenn Sie ein OpenScape 4000 SoftGate mit einem anderen NGS-Server haben werden.

Beispielkonfiguration eines Cisco DHCP-Servers

```
ip dhcp excluded-address 172.15.3.1 172.15.3.219
ip dhcp excluded-address 172.15.3.230 172.15.3.254
!
ip dhcp pool 172-15-3
network 172.15.3.0 255.255.255.0
option 2 hex 0000.0E10
option 60 ascii "SEN.Softgate"
option 43 hex 0104.ac0f.020d
option 42 ip 192.1.1.253
default-router 172.15.3.1
lease 0 4
!
ip dhcp pool 172-15-3-40
host 172.15.3.40 255.255.255.0
hardware-address 001a.e83c.e03a
client-name pcie3-SG41
option 60 ascii "SEN.Softgate"
option 43 hex 0104.ac0f.030d
option 42 ip 192.1.1.253
dns-server 172.28.12.19 172.28.12.20
domain-name global-intra.net
lease 0 4
```

Beispielkonfiguration eines Windows DHCP-Servers

Die Konfiguration eines Windows DHCP-Servers ist von Windows-Version zu Windows-Version unterschiedlich.

Hinweise zur DHCP-Server-Konfiguration finden Sie in der Microsoft Server Dokumentation.

Beispiel für die Kommunikation eines DHCP-Servers und OpenScape 4000 SoftGate

Filter: bootp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xf6b18f40
2	35.026110	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x4593621f
3	35.027498	172.15.3.1	172.15.3.40	DHCP	368	DHCP Offer - Transaction ID 0x4593621f
4	39.992996	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x4593621f
5	39.994424	172.15.3.1	172.15.3.40	DHCP	368	DHCP ACK - Transaction ID 0x4593621f

Frame 5: 368 bytes on wire (2944 bits), 368 bytes captured (2944 bits)

Ethernet II, Src: Cisco_e2:cc:00 (00:0b:be:e2:cc:00), Dst: SiemensE_3c:e0:3a (00:1a:e8:3c:e0:3a)

Internet Protocol, Src: 172.15.3.1 (172.15.3.1), Dst: 172.15.3.40 (172.15.3.40)

User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)

Bootstrap Protocol

Message type: Boot Reply (2)
Hardware type: Ethernet
Hardware address length: 6
Hops: 0
Transaction ID: 0x4593621f
Seconds elapsed: 0

Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0 (0.0.0.0)
Your (client) IP address: 172.15.3.40 (172.15.3.40)
Next server IP address: 0.0.0.0 (0.0.0.0)
Relay agent IP address: 0.0.0.0 (0.0.0.0)
Client MAC address: SiemensE_3c:e0:3a (00:1a:e8:3c:e0:3a)
Client hardware address padding: 0000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP

Option: (t=53,l=1) DHCP Message Type = DHCP ACK
Option: (t=54,l=4) DHCP Server Identifier = 172.15.3.1
Option: (t=51,l=4) IP Address Lease Time = 4 hours
Option: (t=58,l=4) Renewal Time value = 2 hours
Option: (t=59,l=4) Rebinding Time value = 3 hours, 30 minutes
Option: (t=1,l=4) Subnet Mask = 255.255.255.0
Option: (t=12,l=10) Host Name = "pcie3-SG41"
Option: (t=60,l=12) Vendor class identifier = "SEN.Softgate"
Option: (t=43,l=6) Vendor-Specific Information
 Option: (43) Vendor-Specific Information
 Length: 6
 Value: 0104ac0f030d 172.15. 3. 13 NGS IP Addr.
Option: (t=42,l=4) Network Time Protocol Servers = 192.1.1.253
Option: (t=3,l=4) Router = 172.15.3.1
Option: (t=2,l=4) Time Offset = 1 hour
End option

Kommunikation zwischen DHCP-Server und OpenScape 4000 SoftGate

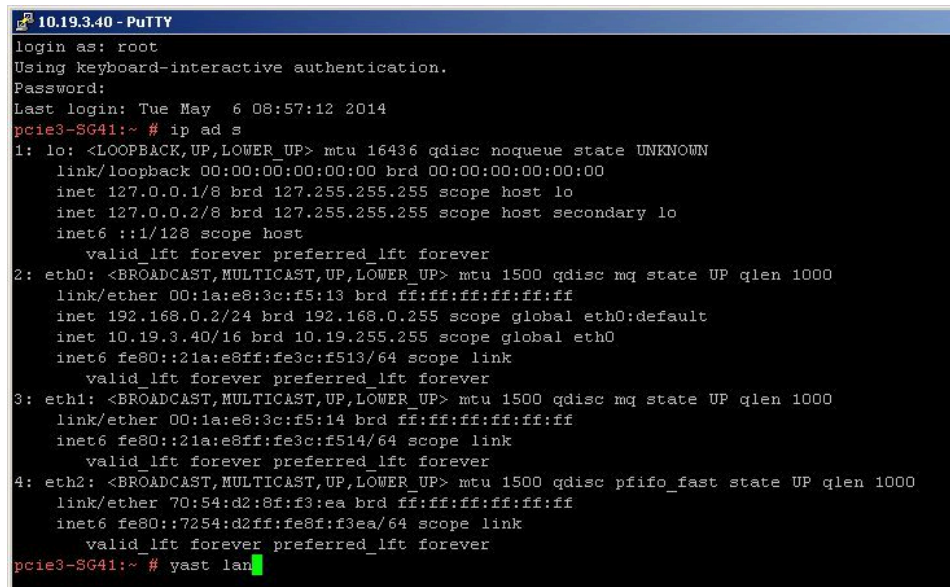
Tabelle 33: IP-Adressen

IP-Adresse des DHCP-Servers	172.15.3.1
Einrichtungs-IP-Adresse des OpenScape 4000 SoftGate (eth0)	172.15.3.40 (dem OpenScape 4000 SoftGate vom DHCP zugewiesen)
IP-Adresse des NGS-Servers	Die IP-Adresse des NGS-Servers ist im Abschnitt Vendor-specific Information enthalten. Sie wird immer hexadezimal dargestellt.

2.4.3.2 Zero Local-Konfiguration bei getrenntem Kunden- und IPDA-LAN

Die LAN-Schnittstelle eth0 wird dem Kunden-LAN zugeordnet. Die LAN-Schnittstelle eth1 wird dem IPDA-LAN zugeordnet.

Im Kunden-LAN wird ein DHCP Server benötigt, der dem OpenScape 4000 SoftGate die IP-Adresse für die OpenScape 4000 Plattform Administration (Portal) zuweist. Über diese IP-Adresse ist das OpenScape 4000 SoftGate dann im Netzwerk von Remote erreichbar. Nun kann eine SSH Verbindung zu dieser IP-Adresse z.B. mithilfe des Programms PuTTY hergestellt werden.



```

10.19.3.40 - PuTTY
login as: root
Using keyboard-interactive authentication.
Password:
Last login: Tue May  6 08:57:12 2014
pcie3-SG41:~ # ip ad s
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
    inet 127.0.0.2/8 brd 127.255.255.255 scope host secondary lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000
    link/ether 00:1a:e8:3c:f5:13 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.2/24 brd 192.168.0.255 scope global eth0:default
    inet 10.19.3.40/16 brd 10.19.255.255 scope global eth0
    inet6 fe80::21a:e8ff:fe3c:f513/64 scope link
        valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000
    link/ether 00:1a:e8:3c:f5:14 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::21a:e8ff:fe3c:f514/64 scope link
        valid_lft forever preferred_lft forever
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 70:54:d2:8f:f3:ea brd ff:ff:ff:ff:ff:ff
    inet6 fe80::7254:d2ff:fe8f:f3ea/64 scope link
        valid_lft forever preferred_lft forever
pcie3-SG41:~ # yast lan
  
```

Abbildung 30: SSH Verbindung zum OpenScape 4000 SoftGate

Anschließend muss mit Yast die Einstellung für die LAN-Schnittstelle eth1 auf DHCP geändert werden.

Network Devices > Network Settings > eth1 > Edit

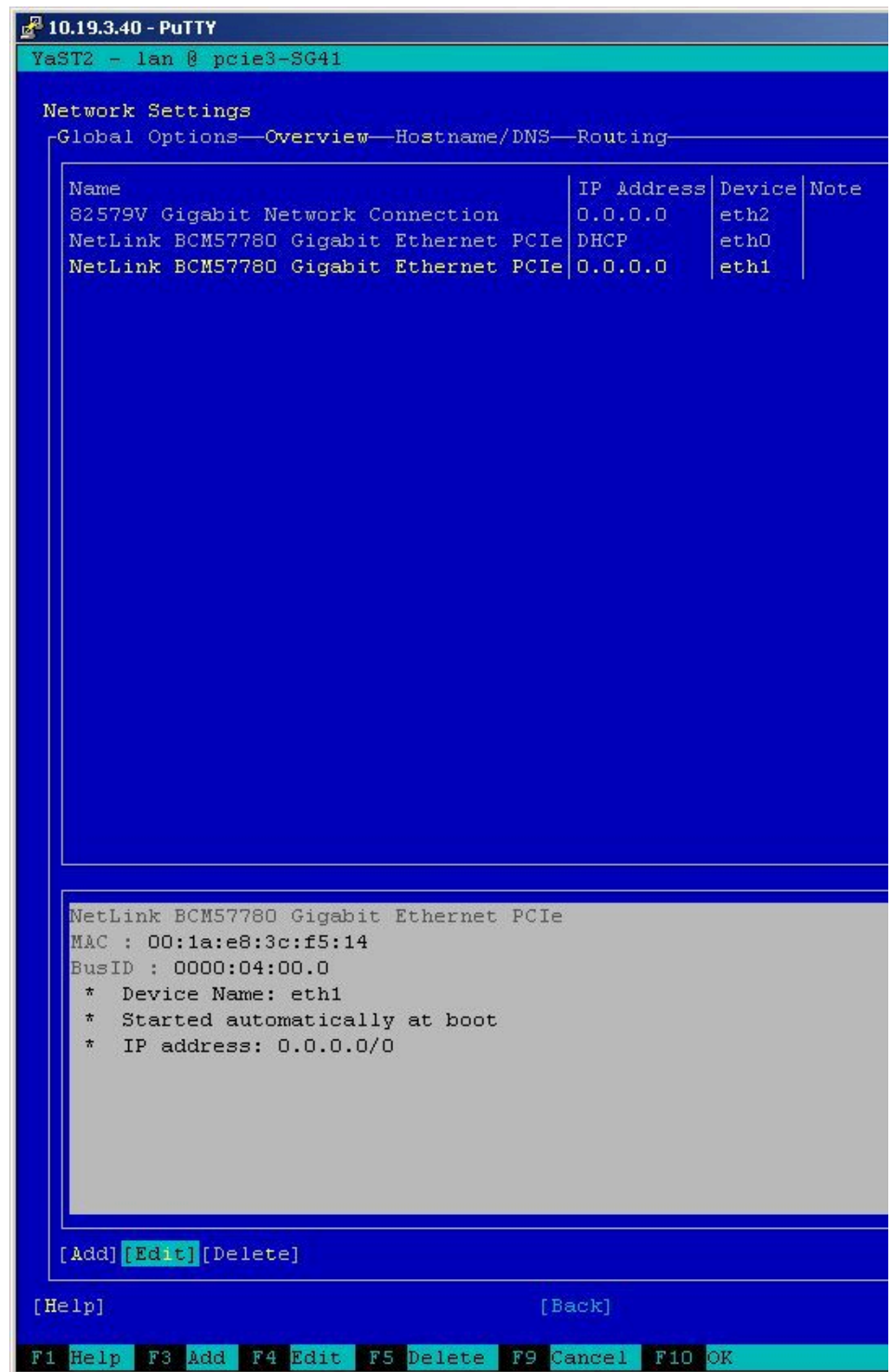


Abbildung 31: eth1 auf DHCP ändern

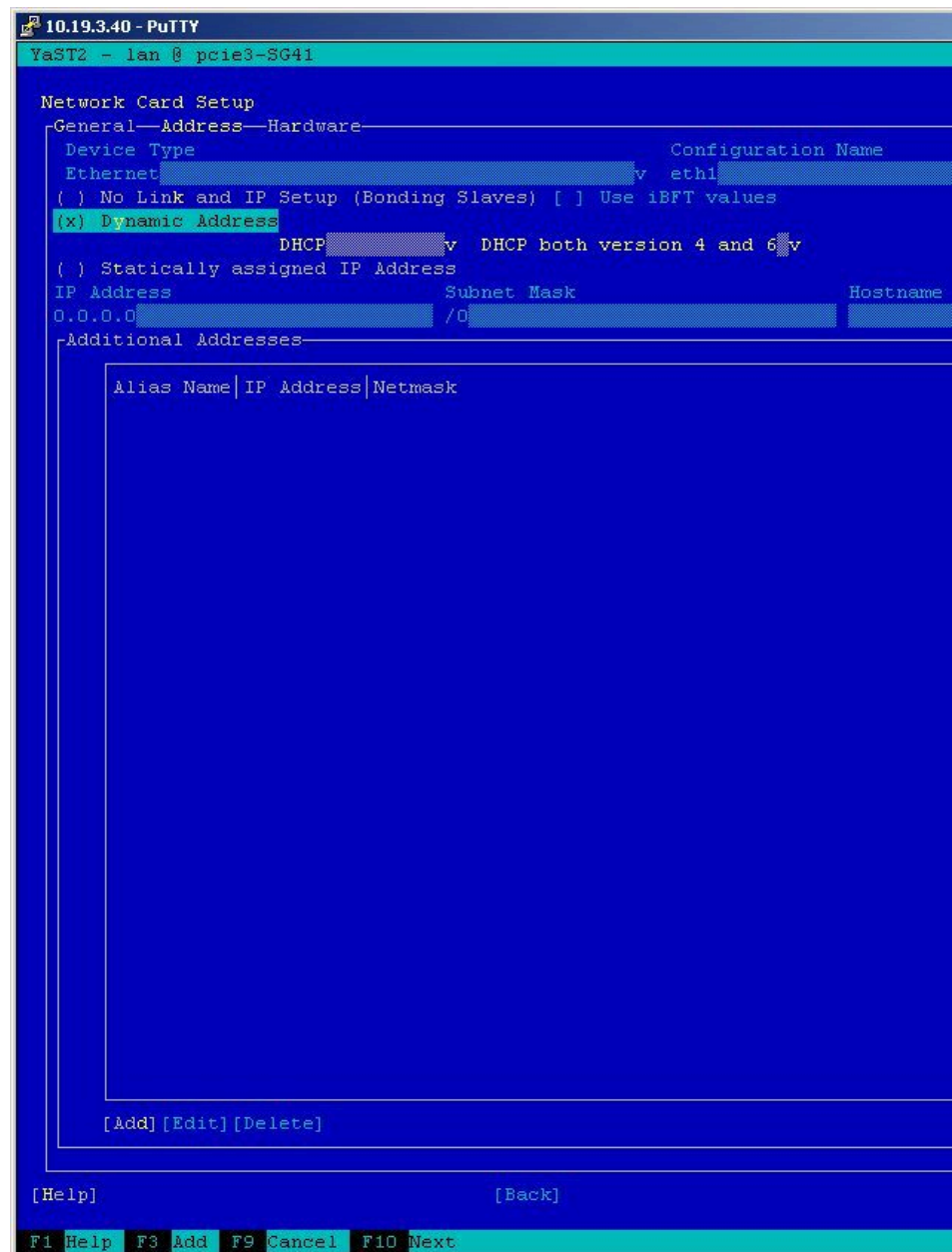


Abbildung 32: eth1 auf DHCP ändern

Wenn nun die Konfiguration des DHCP Servers im IPDA-LAN und die Konfiguration des OpenScape 4000 SoftGates gemäß den Anforderungen an dieses Leistungsmerkmal durchgeführt wurden, so erhält das OpenScape 4000 SoftGate seine Erstinstallationsdaten vom NGS-Server und startet automatisch.

2.4.3.3 Zeitsynchronisierung der Linux-Systemzeit

Anmerkung: Das OpenScape 4000 SoftGate erhält seine Zeiteinstellungen über den AMO SIPCO. Im Folgenden wird nur die Linux-Zeit konfiguriert.

Alle Länder, die Sommerzeit verwenden, müssen nach der Installation die Zeitzone in YaST konfigurieren, da der DHCP-Client keine Ländereinstellungen erlaubt.

System > Date and Time (Datum und Uhrzeit)

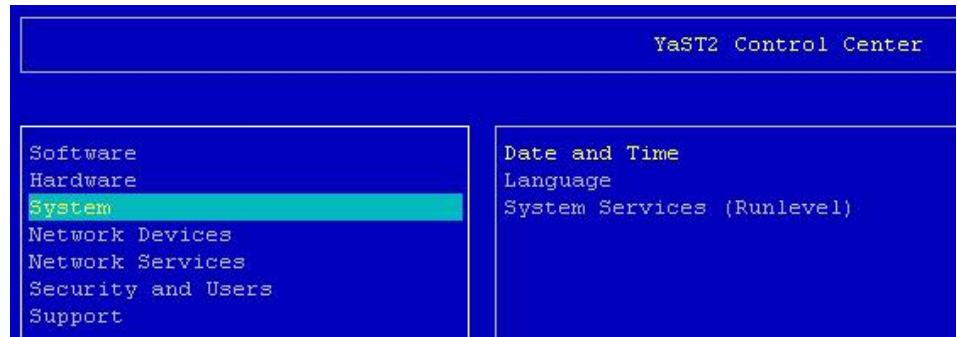


Abbildung 33: Zeitzonekonfiguration mit YaST

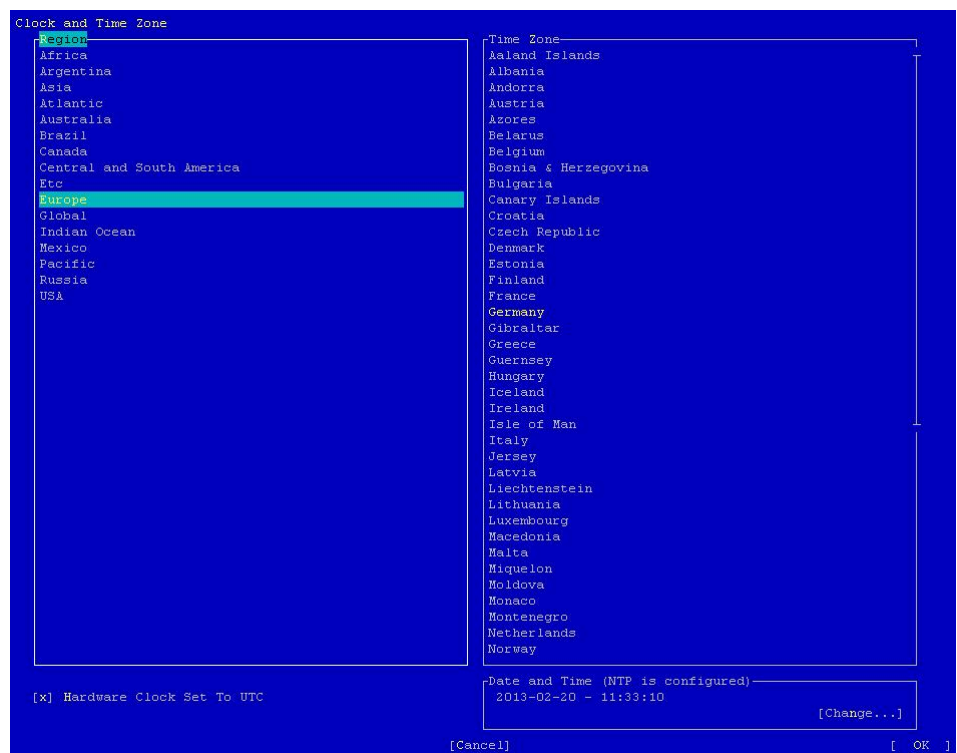


Abbildung 34: Zeitzonekonfiguration mit YaST

Wichtig: Die DHCP-Option **time-offset** kann zum Konfigurieren der lokalen Zeitzone in all den Ländern genutzt werden, die keine Sommerzeit verwenden. Der Zeitversatz wird wie gewohnt eingegeben (westlich von Greenwich mit negativem und östlich von Greenwich mit positivem Vorzeichen).

Wird die DHCP-Option **time-offset** zum Konfigurieren der lokalen Zeitzone verwendet, so muss beachtet werden, dass der Zeitversatz im Zielsystem gemäß POSIX (Portable Operating System Interface) angezeigt wird. POSIX

verwendet für den Zeitversatz im Gegensatz zur Schreibweise westlich von Greenwich positive Vorzeichen und östlich von Greenwich negative Vorzeichen.

Erläuterung

Ein mit der DHCP-Option time-offset "-14400", also einer Zeitzone 4 Stunden westlich von Greenwich, konfiguriertes System wird im POSIX Format mit der Zeitzone "UTC+4" eingerichtet. Dies ist z. B. bei der Ausgabe des Linux-Kommandos "date" sichtbar.

Beispiel

Ein OpenScape 4000 SoftGate in Moskau würde mit der DHCP-Option time-offset "144002" konfiguriert, also 4 Stunden östlich von Greenwich ("UTC +4"). Am OpenScape 4000 SoftGate wird dann die Zeitzone "UTC-4" (POSIX) eingerichtet.

2.4.3.4 Konfigurieren der NGS IP-Adresse

OpenScape 4000 Plattform Administration-Portal > LAN Wizard > IPDA LAN

Konfigurieren Sie die IP-Adresse des NGS-Servers (**NGS IP-Adresse**).

Customer LAN

Ethernet Interface CCA: vlan3126 *

Ethernet Interface CCB: vlan3126 *

IP Address of Portal: 10.140.126.111 *

Netmask: 255.255.255.0 *

IP Address of Assistant: 10.140.126.4 *

IP Address of CSTA: 10.140.126.45

Default Router: 10.140.126.254 *

IPDA LAN

Ethernet Interface CCA: vlan3944 *

Ethernet Interface CCB: vlan3944 *

Netmask: 255.255.255.0 *

IP Address configured In AMO SIPCO for CCA: 10.9.44.100 *

IP Address configured In AMO SIPCO for CCB: 10.9.44.101 *

Default Router: 10.9.44.254 *

NGS IP Address: 10.9.44.200

Atlantic LAN

Ethernet Interface 1 CCA: bond3 *

Ethernet Interface 1 CCB: bond3 *

Ethernet Interface 2 CCA: *

Ethernet Interface 2 CCB: *

Ethernet Interface 3 CCA: *

Ethernet Interface 3 CCB: *

Ethernet Interface 4 CCA: *

Ethernet Interface 4 CCB: *

Fields marked with * are mandatory.

Back Cancel Next

Abbildung 35: NGS IP-Adresse

2.4.3.5 Konfigurieren des NGS

IPDA Wizard > SoftGate Initial Configuration

Geben Sie in das Feld **Setup IP Address** die vom DHCP-Server zugewiesene IP-Adresse des OpenScape 4000 SoftGate (eth0) ein und aktivieren Sie das Kontrollkästchen **An NGS-Server übermitteln**.

Wichtig: Die Setup IP Adresse wird nur in der NGS-Datenbank gespeichert. Werden die Erstkonfigurationsdaten vor Inbetriebnahme des OpenScape 4000 SoftGates geändert (z.B bei einer fehlerhaften Konfiguration), so muss die Setup IP-Adresse erneut eingegeben werden, da sie vom IPDA-Wizard nicht gespeichert wird.

Softgate-Erstkonfiguration

Übermitteln Sie die Erstkonfigurationsdaten an den NGS-Server und/oder speichern Sie sie auf dem lokalen Computer.

☐ Auf lokalem Computer speichern

NGS Server

☒ An NGS-Server übermitteln

IP-Adresse für die Erstkonfiguration: 172 . 15 . 3 . 40

Abbildung 36: Zero Local-Konfiguration für OpenScape 4000 SoftGate

Die OpenScape 4000 SoftGates werden in der NGS-Serverdatenbank registriert. Alle diese OpenScape 4000 SoftGates werden in der OpenScape 4000 Plattform Administration (Portal) im Menü **System > SoftGates** angezeigt.

Home	System	Applications	Status	Maintenance	DSCXL Frontpanel	Assistant	Help	Documentation
HiPath 4000 system settings								
▶ Shell to Host								
▶ LAN Configuration								
▶ IPv6 Addresses								
▼ SoftGates								
▶ UPS								
▶ NGS Configuration								
▶ DSCXL Frontpanel								
▶ SWU Boot Devices								
SoftGates								
LTU	Setup IP Address	Last Update						
38	172.15.5.44	Dec 06 13:23:09 CET 2012		Delete				
41	172.15.3.40	Dec 10 11:28:38 CET 2012		Delete				

Abbildung 37: In der NGS-Datenbank registrierte OpenScape 4000 SoftGates

2.5 Zero Local Konfiguration für Survivable OpenScape 4000 SoftGate

Mit dem Leistungsmerkmal Zero Local Konfiguration kann auch ein Survivable OpenScape 4000 SoftGate installiert werden.

Hierzu muss zuerst die Erstinstallation eines Stand-Alone OpenScape 4000 SoftGate durchgeführt werden (siehe [Section 2.4, "Zero Local-Konfiguration für Stand-Alone OpenScape 4000 SoftGate"](#)).

Anschließend kann die OpenScape 4000 Plattform Administration (Portal) mit der vom DHCP Server zugewiesenen Einrichtungs-IP-Adresse geöffnet werden.

Wichtig: Wenn das OpenScape 4000 SoftGate mit getrenntem Kunden-LAN und IPDA LAN eingerichtet wurde, dann ist die OpenScape 4000 Plattform Administration (Portal) über die Kunden-LAN IP-Adresse erreichbar, die von einem DHCP Server im Kunden-LAN vergeben wurde.

Im Menü **OpenScape 4000 Plattform Administration (Portal) > LAN Konfiguration > LAN-Assistent** kann nun das Deployment von **Standalone SoftGate** auf **Survivable OpenScape 4000 SoftGate with local survivability unit SW(AP-E)** geändert werden.

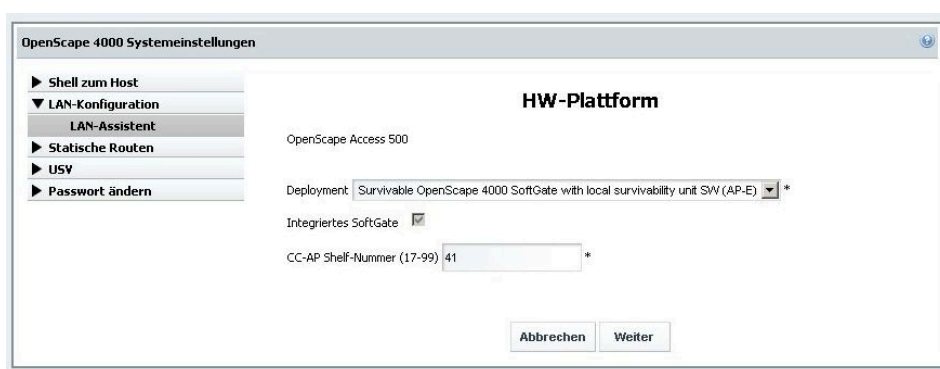


Abbildung 38: Zero Local Konfiguration - Deployment ändern

In den folgenden Masken werden alle für den AP-E Betrieb notwendigen Einstellungen abgefragt.

OpenScape 4000 Systemeinstellungen

▶ Shell zum Host

▼ LAN-Konfiguration

System

SoftGate

▶ Statische Routen

▶ IPv6-Adressen

▶ SoftGates

▶ USV

▶ DSCXL Frontpanel

▶ SWU Boot-Devices

Customer-LAN

Ethernet-Interface

eth0

*

IP-Adresse des Portals

10.19.3.41

*

Netzmaske

255.255.0.0

*

IP-Adresse des Assistants

10.19.3.43

*

IP-Adresse CSTA

Default-Router

10.19.1.1

*

IPDA-LAN

Ethernet-Interface

eth1

*

Netzmaske

255.255.255.0

*

IP Adresse konfiguriert in AMO APESU für CCAP

172.15.3.42

*

Default-Router

172.15.3.1

*

Zentrale NGS IP-Adresse (nur dann nötig, wenn IPV6 ODER SG Zero-Local-Config verwendet wird)

Atlantic-LAN

Ethernet-Interface-1

Ethernet-Interface-2

Ethernet-Interface-3

Ethernet-Interface-4

Zurück

Abbrechen

Weiter

OpenScape 4000 Systemeinstellungen

▶ Shell zum Host

▼ LAN-Konfiguration

LAN-Assistent

▶ Statische Routen

▶ USV

▶ Passwort ändern

Internes LAN

Listen IP-Adresse

192.168.187.0

*

Netzmaske

255.255.255.0

AMO-Initialisierungs-Kommandos senden☒

Zurück

Abbrechen

Weiter

OpenScape 4000 Systemeinstellungen

▶ Shell zum Host

▼ LAN-Konfiguration

System

SoftGate

▶ Statische Routen

▶ IPv6-Adressen

▶ SoftGates

▶ USV

▶ DSCXL Frontpanel

▶ SWU Boot-Devices

Internes LAN

Listen IP-Adresse

192.168.187.0

*

Netzmaske

255.255.255.0

AMO-Initialisierungs-Kommandos senden☒

!!! BITTE BEACHTEN: Ihre Auswahl wird das Senden von Initialisierungs-Kommandos erzwingen.
(EXEC-APC, ACTIVATE-APC, CHANGE-CPCI, EXEC-REST:SYSTEM,RELOAD,
[ADD-APESM, EXEC-UPDAT:UNIT=A1,SUSV=ALL , EXEC-REST:SYSTEM,RELOAD])
Diese Aktion wird zu einem System-Reload führen und sollte nur während einer Erstinstallation verwendet werden !!!

Die AMO-Initialisierung bei einer CCAP Konfiguration macht nur bei einem leeren RMX Image Sinn!
Wenn ein bereits konfigurierter CCAP geändert werden soll, dann sollte diese Option weggelassen werden.
Die CCAP-Nummer Änderung wird nach Drücken von [Abschicken] wirksam.

Abbrechen

OK

Zurück

Abbrechen

Weiter

72

A31003-H31A0-J100-10-0031, 08/2024
OpenScape 4000, Installation, Configuration and Migration, Installationsanleitung

Es folgen dann noch die Masken mit den OpenScape 4000 SoftGate Einstellungen, die bis auf die IP Adresse für AP Emergency bereits vollständig ausgefüllt sind.

OpenScape 4000 Systemeinstellungen

- Shell zum Host
- LAN-Konfiguration
 - LAN-Assistent
 - Statische Routen
 - USV
 - Passwort ändern

SoftGate IPDA Einstellungen (Basis)

Hardwaretyp: OpenScape Access 500a

Aktiviere AP Emergency: ☒

Direct Link für Signalisierung: ☒

IP-Adresse des AP im OpenScape 4000 LAN-Segment: 172.15.3.41

Netzmaske des OpenScape 4000 LAN-Segments: 255.255.255.0

IP-Adresse des SoftGate Default Routers: 172.15.3.1

IP-Adresse des CC-A: 172.15.3.11

IP-Adresse des CC-B: 0.0.0.0

IP-Adresse für AP Emergency: 172.15.3.42

IP-Adresse des AP im AP internen Netzsegment: 192.168.10.41

Netzmaske des AP internen Netzsegments: 255.255.255.0

OpenScape Access Xlink aktivieren: ☒

IP-Adresse des OpenScape Access Xlink: 10.100.0.0

Zurück Abbrechen Weiter

OpenScape 4000 Systemeinstellungen

- Shell zum Host
- LAN-Konfiguration
 - LAN-Assistent
 - Statische Routen
 - USV
 - Passwort ändern

SoftGate IPDA Einstellungen (Experte)

VLAN-Tagging verwenden: ☐

VLAN-ID: 0

Betriebsart der Ethernetschnittstelle: Auto

TOS-Byte für sig.proc. über Ethernet LAN: 104

Server Port für Signalisierungsverbindung: 4000

MTU Größe: 1500

Redundantes Basis-LAN: ☐

Basis-LAN-Interface: eth1

OpenScape Access Xlink LAN-Interface: eth2

Redundantes Management LAN: ☐

Management LAN Interface: eth0

Zurück Abbrechen Weiter

OpenScape 4000 Systemeinstellungen

- Shell zum Host
- LAN-Konfiguration
 - LAN-Assistent
 - Statische Routen
 - USV
 - Passwort ändern

SoftGate IPv6 Einstellungen

IP Stack: IPv4 und IPv6 (Dual Stack)

IPv6-Adresse des AP im OpenScape 4000 LAN-Segment: ::

IPv6-Präfix des AP im OpenScape 4000 LAN-Segment: 0

IP-Adresse des NG5-Servers [IPv4 oder IPv6]: 172.15.3.13

LTU: 41

SoftGate Master Encryption Key (MEK) Management

Master Encryption Key (MEK):

Zurück Abbrechen Abschicken

2.6 Protokolldateien

Die Installationsprotokolldateien befinden sich im Verzeichnis **_install_logs** des USB-Flash-Image (sofern die Installation nicht von einer DVD vorgenommen

wurde, in welchem Fall kein Schreibzugriff möglich ist) sowie auf dem System unter

- 1) /var/log/install-image.timestamp.log
- 2) • /var/log/kernel-messages.timestamp.log
 - /var/log/first-ha-config.timestamp.log

3 OpenScape 4000 Installation auf VMware ESXi

Die Installation als virtuelle Maschine ist für die folgenden Bereitstellungen von OpenScape 4000 möglich.

- Simplex
- Standalone OpenScape 4000 SoftGate
- OpenScape 4000 SoftGate auf Quorum
- Quorum
- Separated Duplex Quorum
- Simplex mit und ohne integriertes OpenScape 4000 SoftGate
- Survivable mit und ohne integriertes OpenScape 4000 SoftGate

3.1 Wichtige Hinweise

Allgemeine Informationen

- 1) Die VMware-Tools werden als Teil der Appliance-Software installiert und es ist nicht erlaubt diese zu aktualisieren, z.B. über die vSphere Administrations-Schnittstelle.

Unter bestimmten Umständen kann es vorkommen, dass die grafische Oberfläche von Sphere Administration eine Meldung ausgibt, die besagt, dass die Tools veraltet sind. Dies ist lediglich eine Displaymeldung in VMware und kann ignoriert werden.

- 2) Für die VMware-Installation werden ab OpenScape 4000 V7 R1 zusätzliche Tools benötigt.

Diese Tools befinden sich im Verzeichnis `\DriversAndTools\VMWare_Installation_Resources` und müssen auf Ihren lokalen Windows-PC kopiert werden.

- 3) VMware-Snapshots haben negative Auswirkungen auf Echtzeitsysteme und dürfen daher nicht verwendet werden. Mehr Informationen zu der Verwendung von Snapshots bei virtuellen Maschinen finden Sie in **OpenScape Solution Set, OpenScape Virtual Machine Resourcing and Configuration Guide > 3.5 General Statements and Best Practice Recommendations for Virtualization at Unify**. Der folgende E-Doku-Link funktioniert nur, wenn Sie Intranet-Zugang haben: <http://apps.gdms.com:8081/techdoc/en/P31003S1100S101017620/index.htm>
- 4) Weitere allgemeine Informationen und Tipps (z. B. Details zur Dimensionierung, allgemeine Produktinformationen, Kompatibilität mit VMware-Funktionen) finden Sie in **OpenScape Solution Set, OpenScape Virtual Machine Resourcing and Configuration Guide > 5 Virtualization Dimensioning Details > 5.4 OpenScape 4000**. Der folgende E-Doku-Link funktioniert nur, wenn Sie vollen Intranetzugang haben: <http://apps.gdms.com:8081/techdoc/en/P31003S1100S101017620/index.htm>
- 5) Hohe Swap-in-Latenz: Das Swap-in von Seiten ist teuer für eine virtuelle Maschine. Wenn der Hypervisor eine Gastseite auslagert und der Gast anschließend auf diese Seite zugreift, wird die VM blockiert, bis die Seite von der Festplatte ausgelagert wird. Eine hohe Swap-in-Latenz, die mehrere

Millisekunden betragen kann, kann die Leistung des Gastes erheblich beeinträchtigen.

Um RAM-Swapping-Effekte des Hypervisors zu vermeiden, lesen Sie bitte die VMware-Dokumentation zur Speicherverwaltung (https://www.vmware.com/files/pdf/techpaper/vsp_41_perf_memory_mgmt.png).

- 6) Stellen Sie sicher, dass **Forged Transmits** aktiviert ist - ohne diese Einstellung wird der RMX Standby-Prozessor nicht geladen.

NOTICE: Standard-ESXi-Switches verwenden als Default bereits **Accepted**, während ESXi Distributed Switches (VDS) verwenden als Default **Disabled**.

Installation des OpenScape 4000-Systems

- 1) Für OpenScape 4000 System ESXi-Installationen muss die Hardware-Virtualisierung (Virtualized Hardware Virtualization (VHV)) aktiviert werden (siehe [Abschnitt 3.14, "Aktivieren der Hardware-Virtualisierung auf dem ESXi-Host"](#)).
- 2) Ein gültiger und erreichbarer DNS-Server muss in der Datei `/etc/resolv.conf` auf allen Knoten der Linux-SOCO2-Plattform konfiguriert werden. Die Daten für den DNS-Server werden in der ersten Installations-XML-Datei eingetragen (siehe [Abschnitt 3.11.2, "DNS-Server"](#)).
- 3) Wenn eine Verbindung direkt über den Atlantic-LAN-Port hergestellt wird, muss der **Promiscuous Mode** unter ESXi nur für das Atlantic-LAN konfiguriert werden. Diese Einstellung ist auch für Duplex-Bereitstellungen erforderlich (siehe [Abschnitt 3.6.1, "Vorbereitungen auf dem ESXi-Host"](#)).

NOTICE: Die Einstellung ist nicht erforderlich, wenn der Zugriff über OpenScape 4000 Expert Access (Comwin) mit dem OpenScape 4000 Assistant erfolgt.

IMPORTANT: Der **Promiscuous Mode** darf für andere Schnittstellen nicht aktiviert werden. Dies würde die E/A für diese virtuellen Maschinen unnötig erhöhen.

NOTICE: Es ist optional, den in den OVF-Vorlagen enthaltenen USB-Controller nach der Installation zu entfernen, indem Sie die Einstellungen der virtuellen Maschine bearbeiten.

3.2 Benötigte Software und Hardware

- ESXi Umgebung mit mindestens Version V5.1

NOTICE:

Für V10R0 ist eine ESXi-Umgebung der Version V5.1 oder höher erforderlich.

ESXi-Umgebung Version V6.5 oder höher ist für V10R1 erforderlich.

IMPORTANT: vMotion ist mit ESXi kleiner als V5.1U3 nicht erlaubt. Wenn Sie vMotion nutzen wollen, müssen Sie ESXi V5.5 verwenden.

- Die CPU-Hardware muss Intel VT-x/EPT oder AMD-V/RVI Technologie unterstützen.
- Service-PC mit Windows 7 und vSphere Client
- ISO-Datei vom SWS (ZIP-Datei extrahiert zum ISO)

Weitere Informationen zu den Software- und Hardwareanforderungen finden Sie im OpenScape Solution Set V10, OpenScape Virtual Machine Resourcing and Configuration Guide, Service Documentation, Kapitel 5.4 OpenScape 4000.

3.3 Benötigte Informationen vom Kunden

- Namen der Netzwerkbezeichnungen
z. B.: Management, Voice, Atlantic
- Erst-Installationsdatei `firstinst-netw-XXXXX.xml` (inklusive der Konfigurationsdaten für OpenScape 4000 Softgate, wenn dieses vorhanden ist)
- REGEN-Datei für die RMX-Konfiguration
- Freie IP-Adresse aus dem Kunden-Adress-Bereich für den Service PC (Aufgaben des Service PC siehe [Section 3.5, "Service PC"](#)).
- Eventuell MAC-Adresse

3.4 Service PC

Der Service PC wird für die folgenden Aufgaben benutzt:

- Zugriff auf den OpenScape 4000 Assistant nach der Erstinstallation
- Zugriff auf die OpenScape 4000 mit Hilfe von OpenScape 4000 Expert Access (=Comwin) nach der Erstinstallation.
- Benutzung des vSphere Clients
- Erzeugen und Anpassen der Konfigurationsdateien
- Erstellen der Installations- Floppy (siehe [Section 3.12, "Floppy Image mit dem Inhalt der firstinst-netw-*.xml erzeugen"](#))
- Erstellen der Hotfix ISO-Datei (siehe [Section 3.13, "Hotfix Installation vorbereiten"](#))

3.5 Vorbereitung der VMware Umgebung

3.5.1 Vorbereitungen am ESXi Host

- Konfigurieren Sie die Portgruppen entsprechend den Kundenvorgaben in den virtuellen Switchen für die eth-Schnittstellen für Customer LAN, IPDA LAN, Atlantic LAN sowie Corosync LAN (nur bei Duplexbetrieb).

Wichtig: Es gibt zahlreiche Möglichkeiten, wie man die virtuellen Switches konfigurieren kann. Das hängt von den Kundenvorgaben ab. In unserem Beispiel haben wir für jede Portgruppe einen eigenen virtuellen Switch mit jeweils einem eigenen physikalischen Netzwerkinterface gewählt.

Wichtig: Im Staging Center sollte diese Konfiguration im virtuellen Switch ((**Standard Switch**)) ausreichen. Im Kundenumfeld ist jedoch häufig die Konfiguration im physikalischen Switch (**Distributed Switch**) erforderlich.

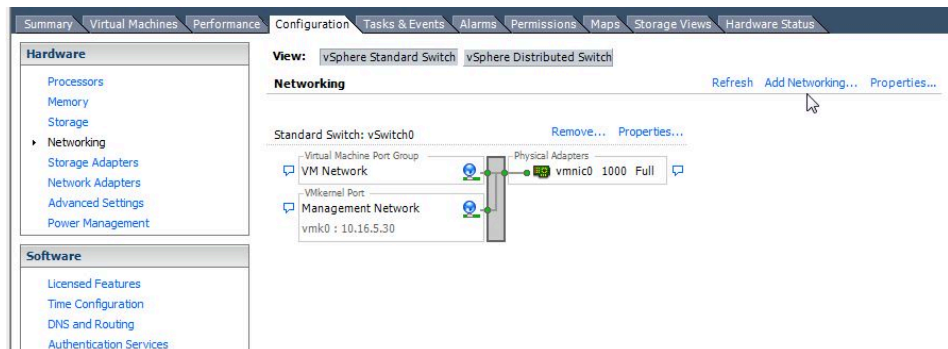


Abbildung 39: Default Konfiguration des virtuellen Switches nach ESXi Host-Installation

Um einen virtuellen Switch hinzuzufügen klicken Sie auf **Add Networking**.

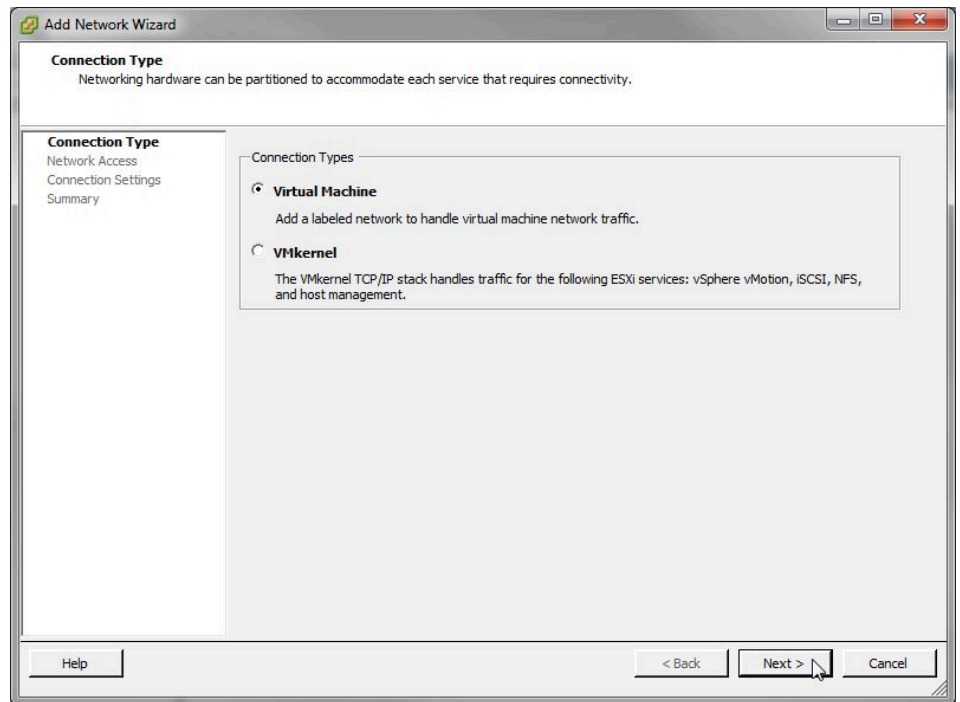


Abbildung 40: Virtuellen Switch hinzufügen

Wählen Sie **Virtual Machine** aus und bestätigen Sie mit **Next**.

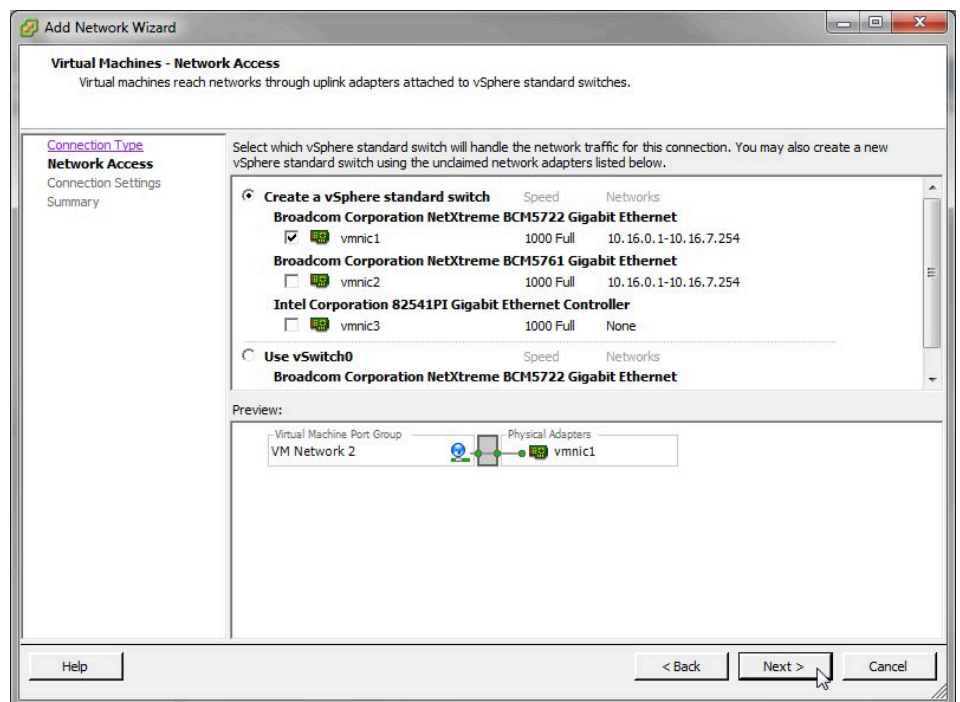


Abbildung 41: Physikalische Netzwerkschnittstelle für virtuellen Switch

Wählen Sie die physikalische Netzwerkschnittstelle aus, die zum virtuellen Switch hinzugefügt werden soll. Weiter mit **Next**.

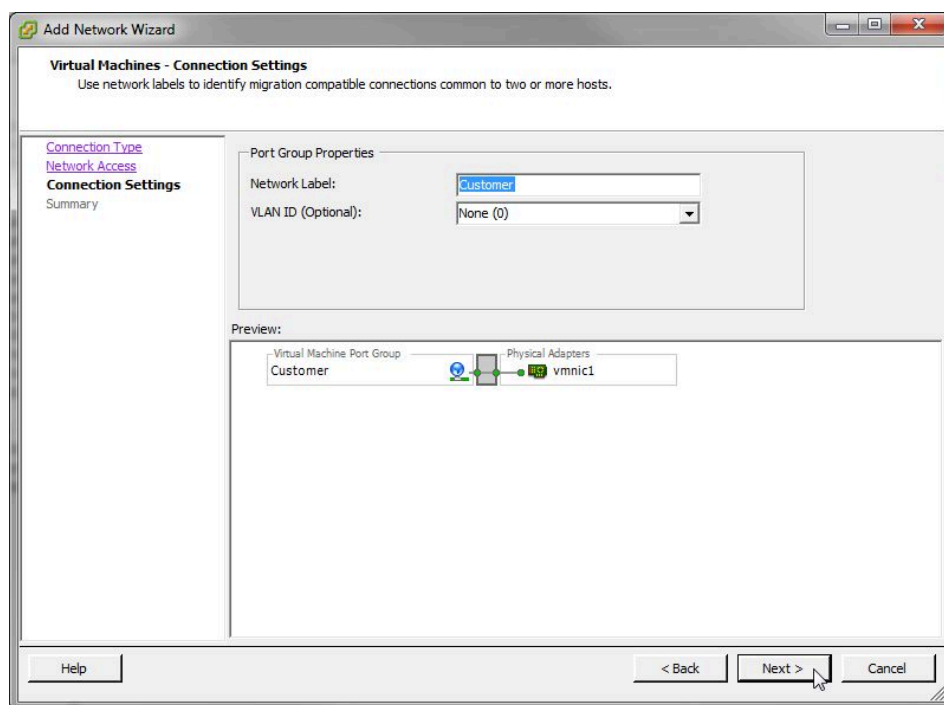


Abbildung 42: Name der Portgruppe

Legen Sie den Namen der Portgruppe (z.B. Customer) fest. Weiter mit **Next**.

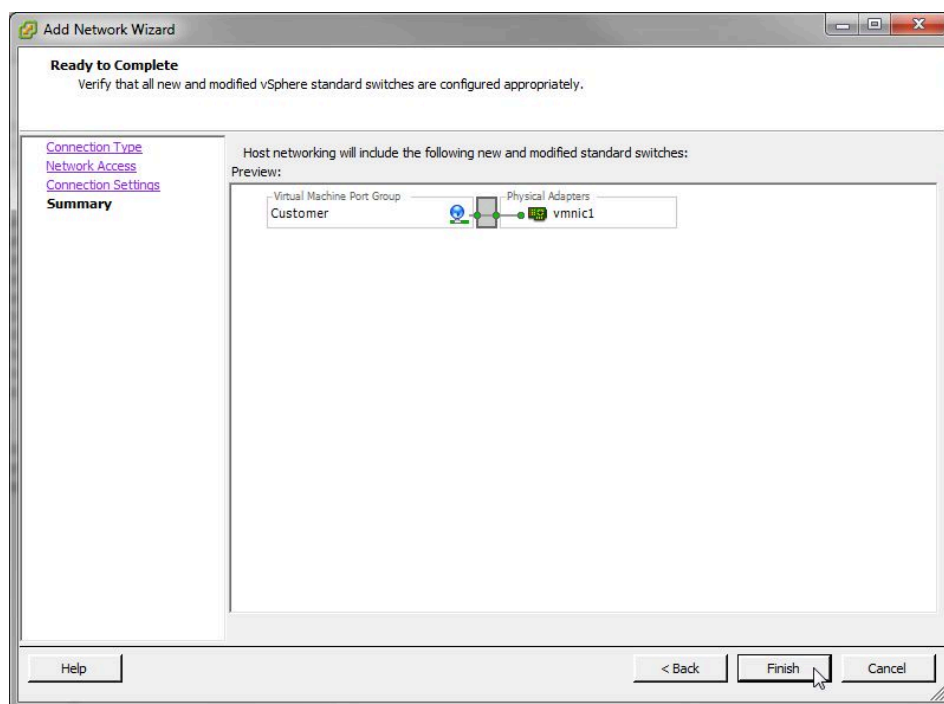


Abbildung 43: Zusammenfassung des zuvor konfigurierten virtuellen Switches

Bestätigen Sie mit **Finish**. Der neue virtuelle Switch mit der verbundenen Portgruppe "Customer" und dem physikalischen Netzwerkinterface "vmnic1" wird dem Netzwerk hinzugefügt und in der Netzwerkübersicht angezeigt.

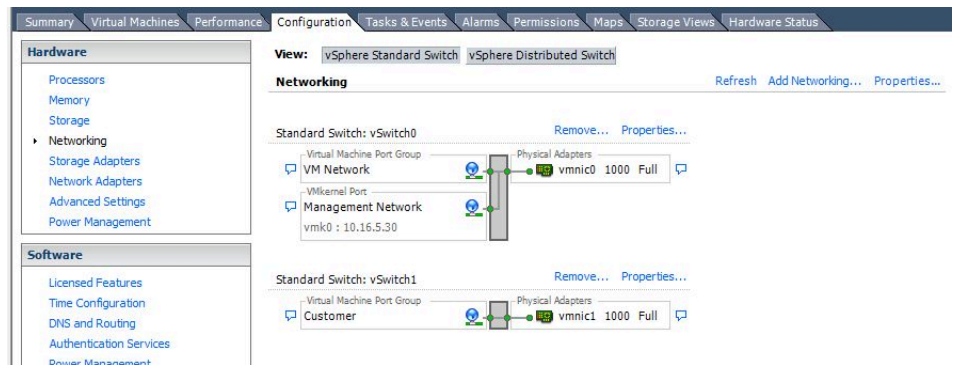


Abbildung 44: Netzwerkübersicht mit einem virtuellen Switch

Konfigurieren Sie auch IPDA LAN und Atlantic LAN. In unserem Beispiel haben diese jeweils eine eigene Portgruppe und eine eigne physikalische Netzwerkschnittstelle. Die Netzwerkübersicht sieht dann so aus.

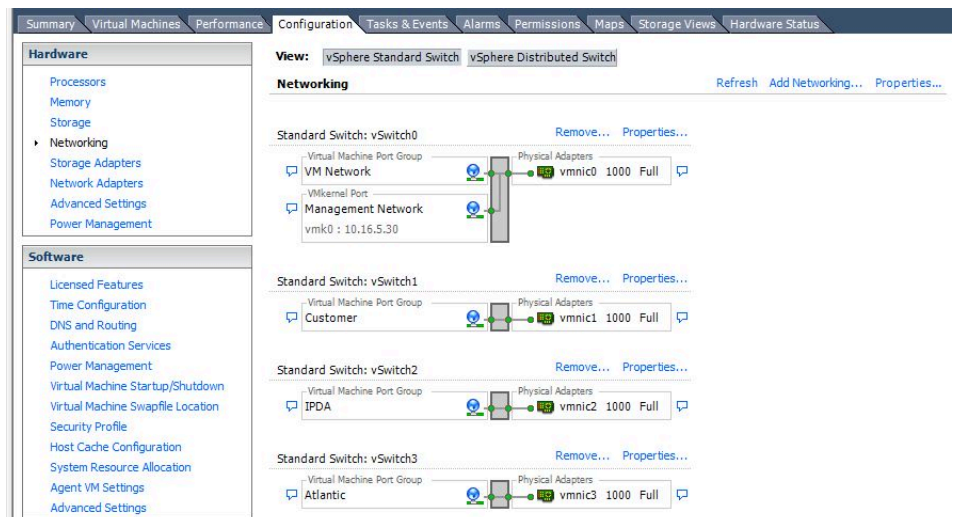


Abbildung 45: Netzwerkübersicht mit drei virtuellen Switchen

- Wenn das Atlantic LAN über OpenScape 4000 Expert Access erreicht werden soll, dann muss das Atlantic LAN nun auf **Promiscuous Mode** eingestellt werden. Diese Einstellung ist auch für Duplex Deployments zwingend notwendig.

Wichtig: Falls diese Einstellung nicht vorgenommen wird, ist das Atlantic LAN nicht erreichbar.

Anmerkung: Die Aktivierung des Promiscuous Mode am virtuellen Switch führt dazu, dass alle eintreffenden IP Pakete über alle Portgruppen und physikalischen Netzwerkkomponenten wie an einem Netzwerkhub gespiegelt werden. Daher sollte für das Atlantic LAN möglichst ein separater virtueller Switch konfiguriert werden.

Öffnen Sie **Home > Inventory > Host and Clusters**.

Wählen Sie aus der Liste der Hosts den entsprechenden Host aus und klicken dann auf das Register **Configuration**. In der Tabelle **Hardware** wählen Sie nun **Networking** aus.

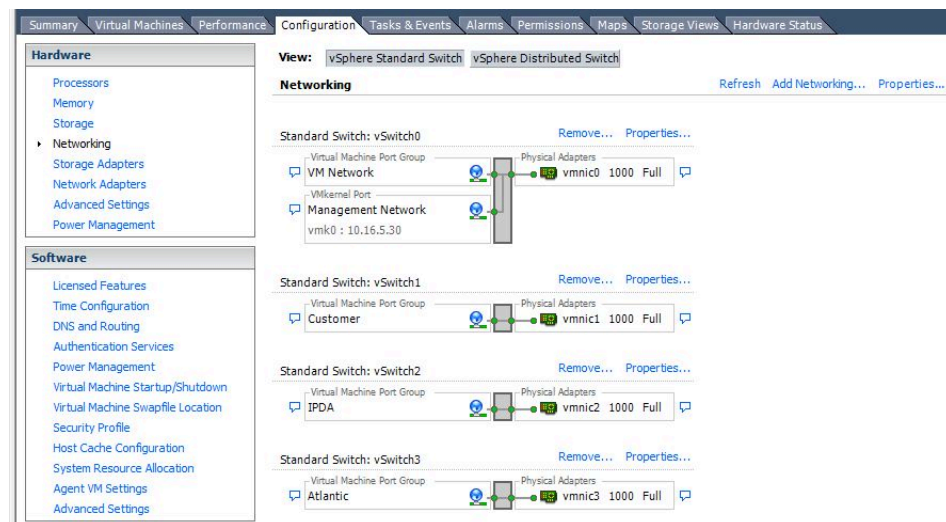


Abbildung 46: Netzwerkübersicht mit virtuellem Switch für Atlantic LAN

Klicken Sie auf die Eigenschaften (**Properties**) des virtuellen Switches, an dem die Portgruppe "Atlantic" konfiguriert ist. Die Properties-Seite für den virtuellen Switch wird geöffnet.

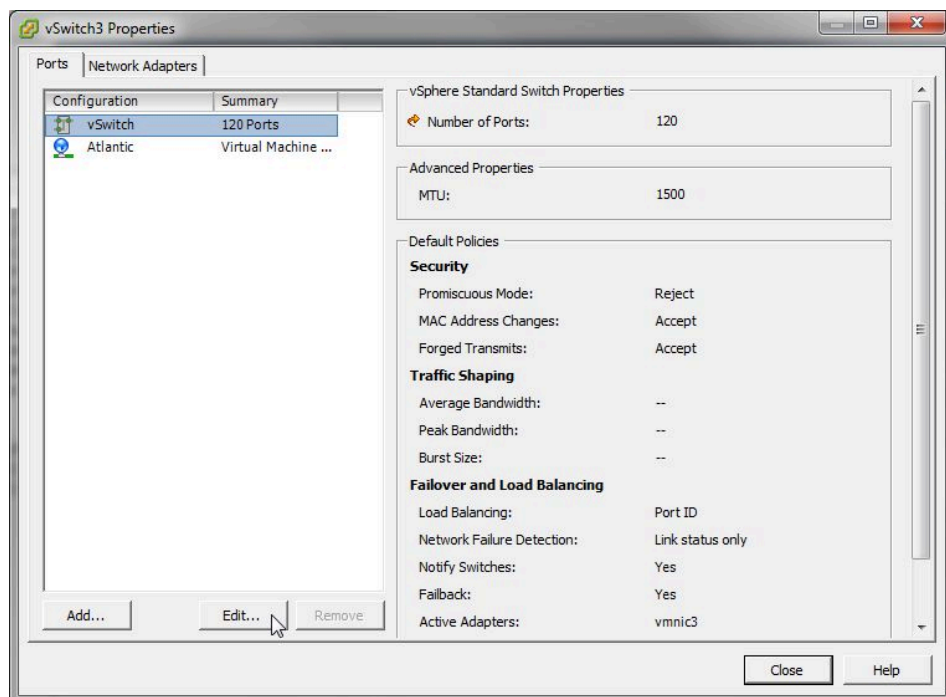


Abbildung 47: Eigenschaften des virtuellen Switches

Klicken Sie auf die Schaltfläche **Edit**.

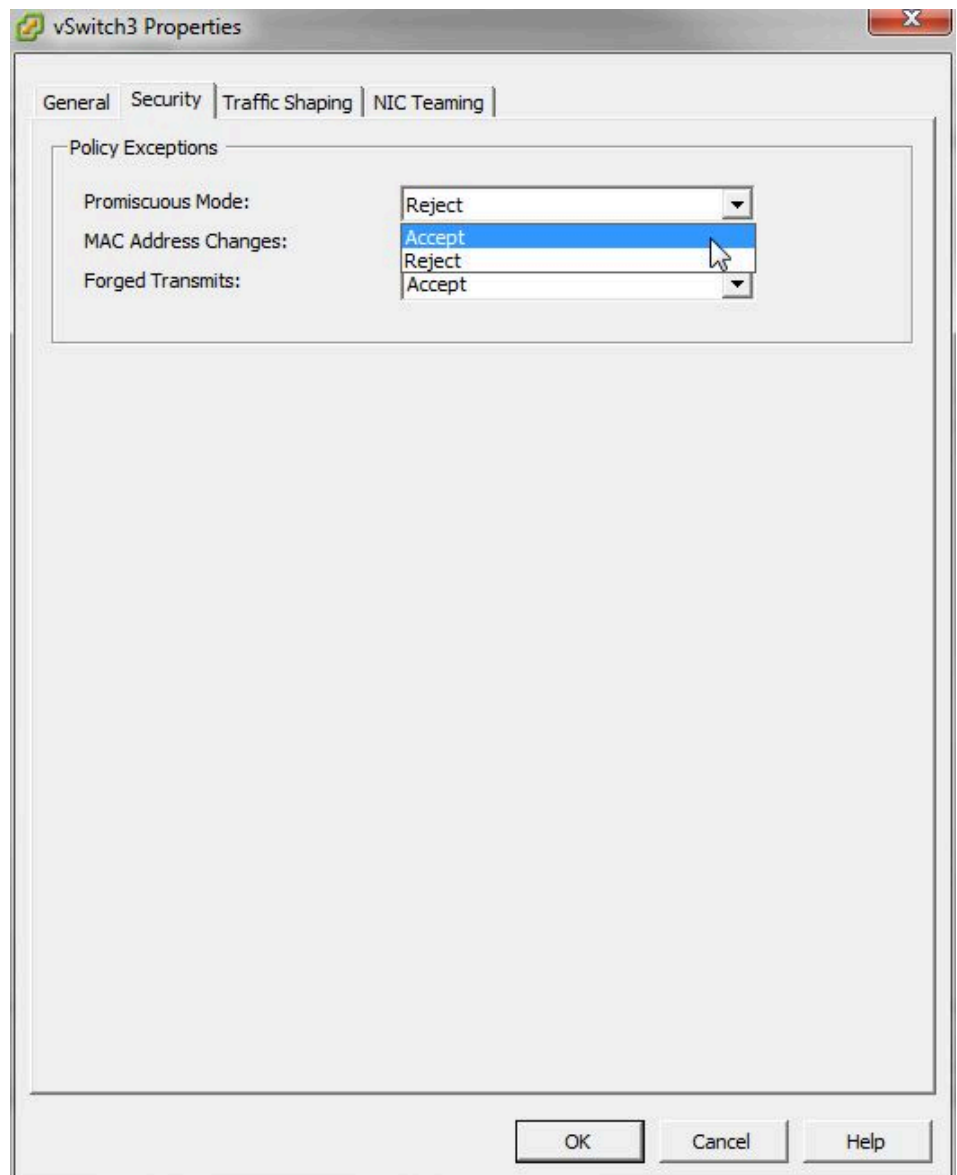


Abbildung 48: Promiscuous Mode für Atlantic LAN

Setzen Sie hier nun im Register **Security** den **Promiscuous Mode** auf **Accept** setzen und mit **OK** bestätigen.

In der Properties-Seite sieht man nun, dass der Promiscuous Mode aktiviert wurde (Abschnitt **Default Policies > Security > Promiscuous Mode**)

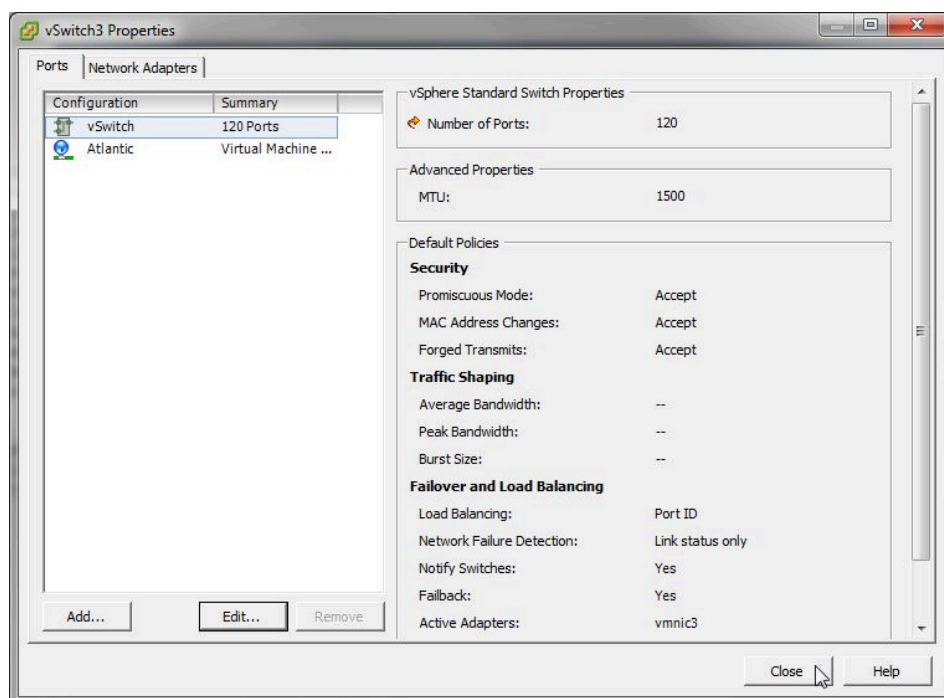


Abbildung 49: Properties-Seite mit aktiviertem Promiscuous Mode

- Stellen Sie sicher, dass **Forged Transmits** aktiviert ist - ohne diese Einstellung wird der RMX Standby-Prozessor nicht geladen.

Anmerkung: Standard ESXi-Switche verwenden als Default bereits **Accepted**, während ESXi Distributed Switches (VDS) verwenden als Default **Disabled**.

3.5.2 Vorbereitungen auf dem Service PC

- Tragen Sie eine freie Kunden IP-Adresse und Netzmaske auf der LAN-Karte des Service PC ein.

Console > Start > Control Panel > Network and Internet > Network Connection > LanAdapter > Rechte Maustaste Properties > TCP / IPv4 > Properties

Wählen Sie den Radio Button **Use the following IP address** und bestätigen Sie mit der Schaltfläche **OK**.

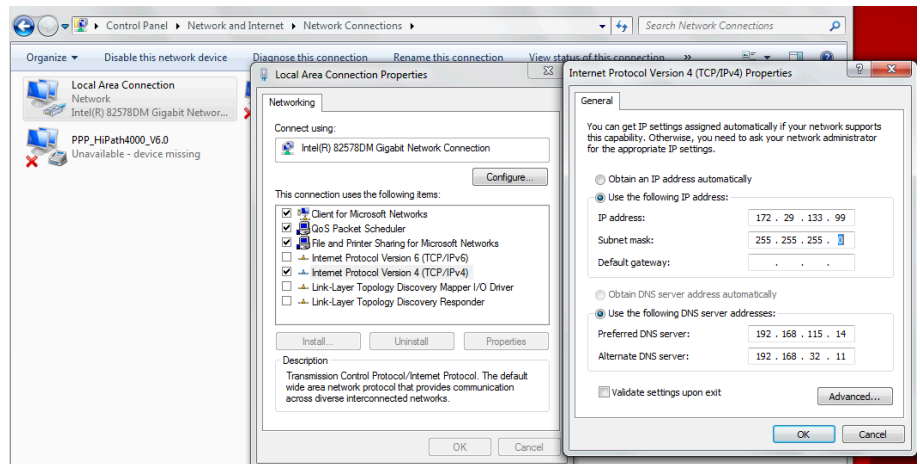


Abbildung 50: IP-Adresse und Netzmaske für den Service PC

- Erzeugen Sie auf dem PC einen Arbeitspfad für:
 - XML-Datei,
 - REGEN-Datei,
 - Floppy und Image Tools,
 - Floppy Image Datei,
 - Protokolldateien
 - Hotfixes
- Kopieren Sie die Installations-ISO-Datei an einen vom vSphere Client zugreifbaren Ort (z.B. Datastore).
- Extrahieren Sie das Verzeichnis VMware_ovf-Templates aus der Datei ...InstallImage.iso.

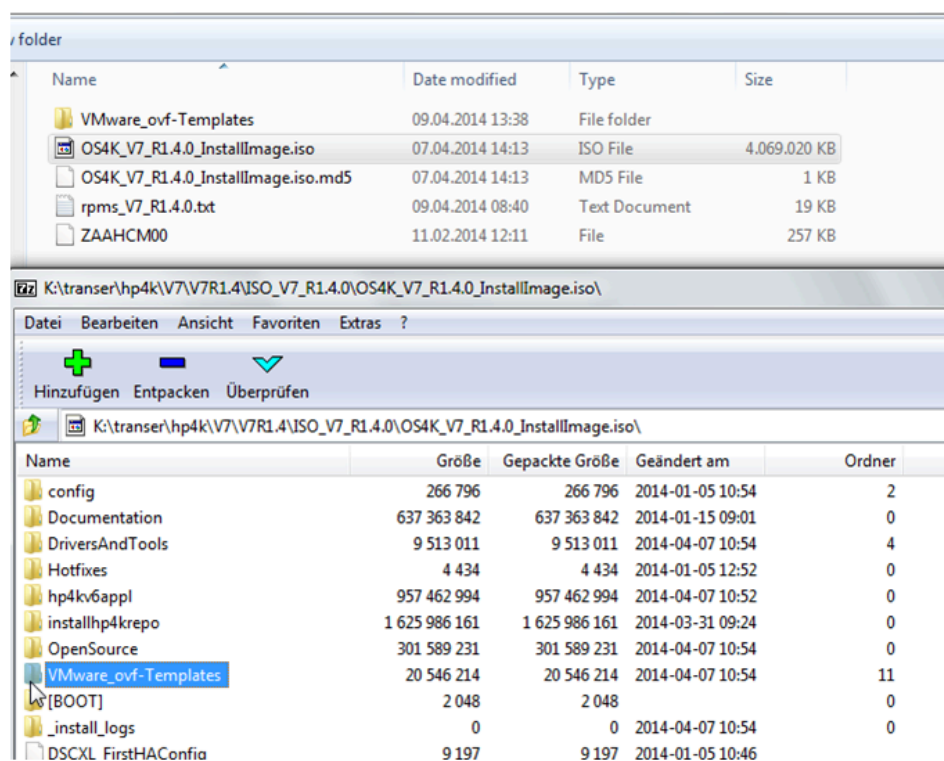


Abbildung 51: Verzeichnis "VMware_ovf-Templates" extrahieren

Diese OVF-Vorlagen müssen zusammen mit der ISO-Datei auf einem Datastore abgelegt werden.

Anmerkung: Der Inhalt dieser Dateien wird nicht verändert und kann als "readonly" definiert sein.

- Extrahieren Sie den Ordner `DriversandTools` \VMware_Installation_Resources in den zuvor erstellten Arbeitspfad des Service PCs. Dieser Ordner enthält die Floppy und Image Tools und eine leere Floppy Image Datei.

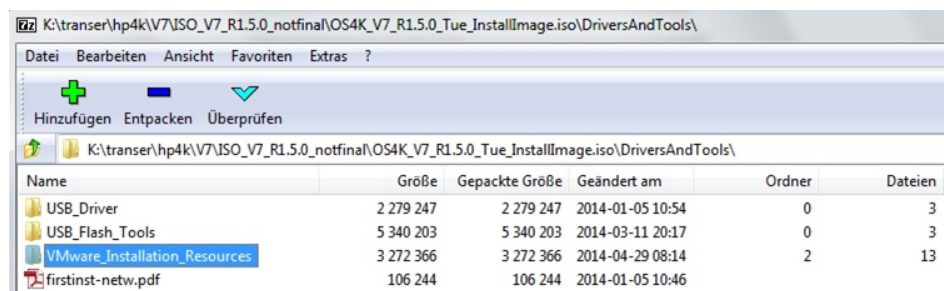


Abbildung 52: Verzeichnis "VMware_Installation_Resources" extrahieren

- Kopieren Sie die XML-Datei in den Arbeitspfad
Der Inhalt des Arbeitspfades sollte nun folgenden Inhalt haben:
- Verzeichnisse: `mkisofs` und `mtools`
- Dateien: `empty.flp`, `getdir.bat`, `getlogs.bat`, `mk-iso.bat` und `prepare.bat` und `firstinst-netw-*.xml`

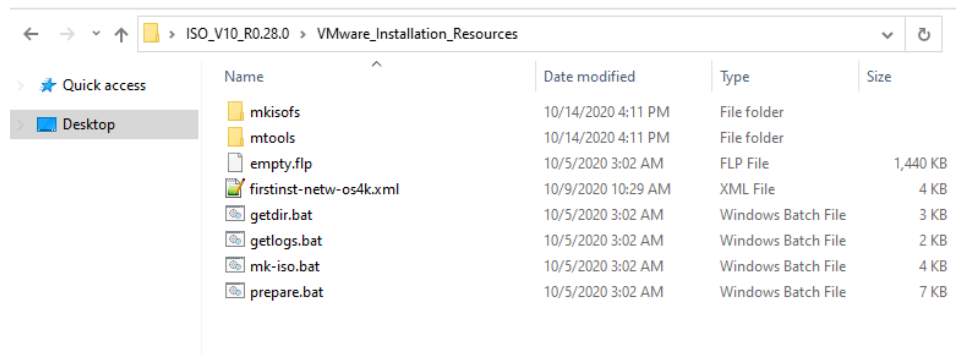


Abbildung 53: Inhalt des Arbeitspfades auf dem Service PC

3.6 Dimensionierung/Vorraussetzungen der virtuellen Maschine

Die Verwendung der OS4k OVF-Vorlagen ist obligatorisch.

3.6.1 Dimensionierung

Die OpenScape 4000 benötigt bestimmte Ressourcen, die beim Erzeugen der virtuellen Maschine (Import der OVF-Vorlage) festgelegt werden. Diese sind:

- Anzahl der CPUs
- benötigter Harddisk Speicher
- Größe des RAM Arbeitsspeichers
- Reservierungen für Arbeitstakt

Abhängig des zu installierenden OpenScape 4000 Deployments sind die Anforderungen an diese Ressourcen unterschiedlich. Genau Angaben zur Dimensionierung finden Sie in folgender Dokumentation:

OpenScape Solution Set V8, OpenScape Virtual Machine Resourcing and Configuration Guide > 5 Virtualization Dimensioning Details > 5.4 OpenScape 4000

Anzahl und Typ der LAN-Karten, DVD-Laufwerke und Floppy-Laufwerke können entsprechend der Kunden-Anforderungen konfiguriert werden.

3.6.2 Hardwarevirtualisierung

Wenn Sie eine OpenScape 4000 Host-Installation durchführen wollen, muss die Hardwarevirtualisierung auf dem ESXi Host möglich sein. Diese wird mit dem Import der OVF-Vorlage automatisch aktiviert.

3.7 Import einer OVF-Vorlage (Beispiel: Simplex)

Wichtig: Der OVF-Import muss für jeden Knoten durchgeführt werden, d.h. bei einem Separated-Duplex-System muss dieser OVF-Import und die nachfolgende Installation dreimal durchgeführt werden (Knoten 1, Knoten 2 und Quorum). Da es

sich um 3 getrennte virtuelle Maschinen handelt muss auch 3 fach installiert werden. Dasselbe gilt für jedes zu installierende OpenScape Softgate.

Im vSphere-Client:

1) File > Deploy OVF Template

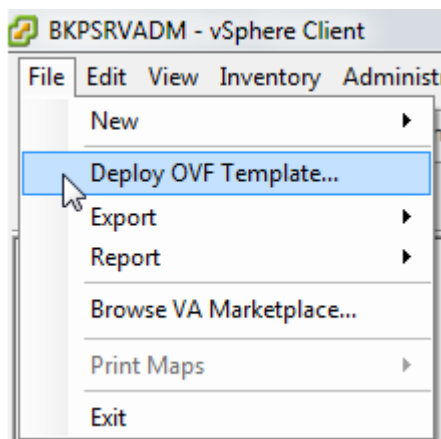


Abbildung 54: OVF importieren über vSphere Client

2) Wählen Sie das richtige Deployment (in diesem Fall: OS4K_Simplex.ovf im Verzeichnis OS4K_Simplex).

Anmerkung: Die Dateinamen der OVF-Vorlagen leiten sich von dem zu installierendem Deployment ab.

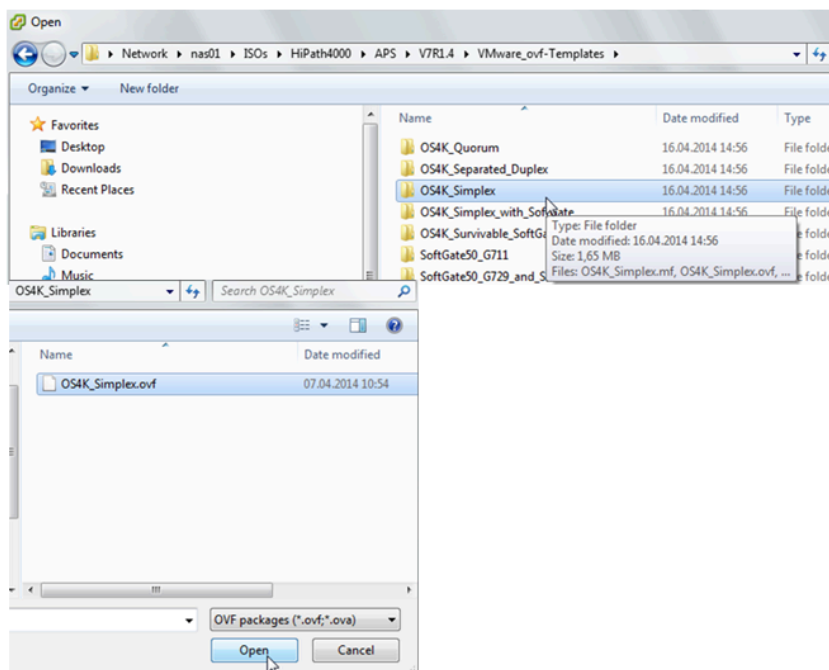


Abbildung 55: Deployment auswählen

Klicken Sie auf **Open**.

3) Quellverzeichnis auswählen.

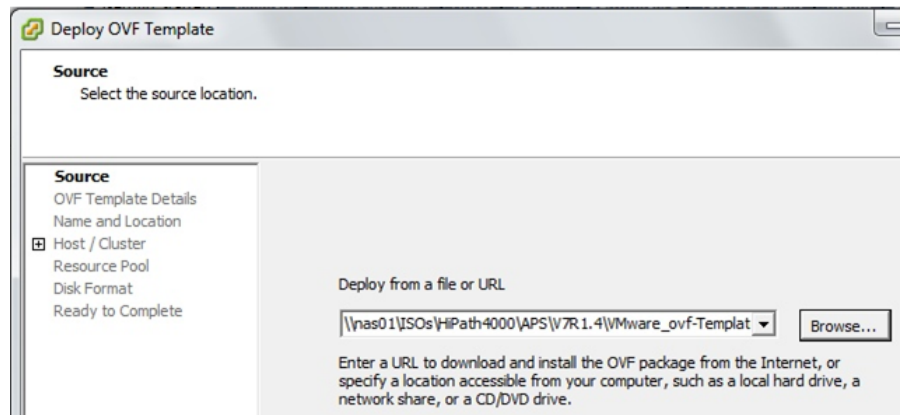


Abbildung 56: Quellverzeichnis auswählen (Source)

Klicken Sie auf **Next**.

4) Details der OVF-Vorlage verifizieren.

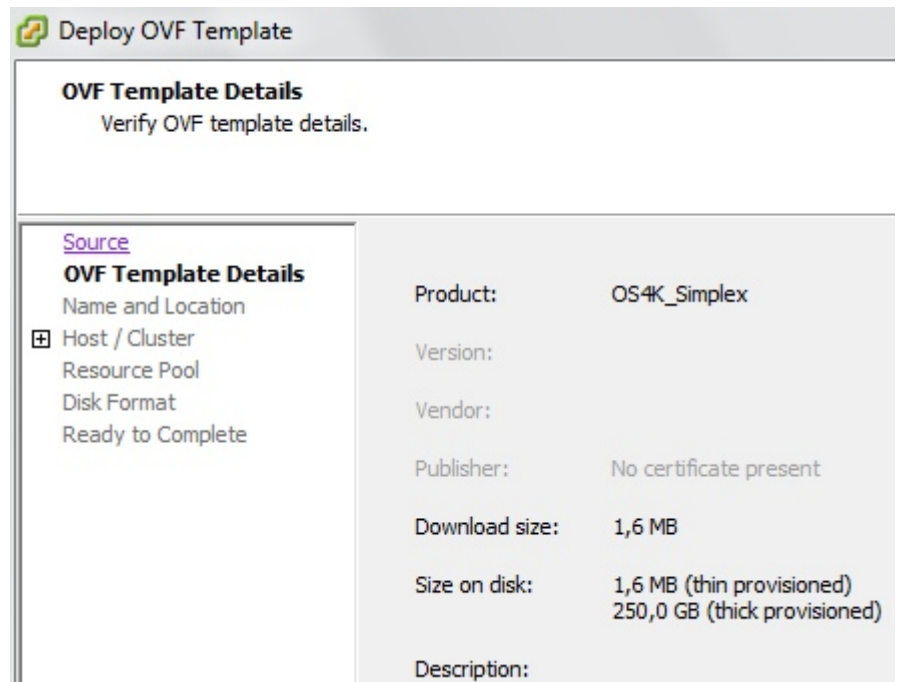


Abbildung 57: Details der OVF-Vorlage verifizieren (OVF Template Details)

Klicken Sie auf **Next**.

- 5) Ändern Sie den Namen, z.B. auf **OS4K-Simplex-Example**. Dieser Name wird dann in der Übersicht und im Datastore verwendet.

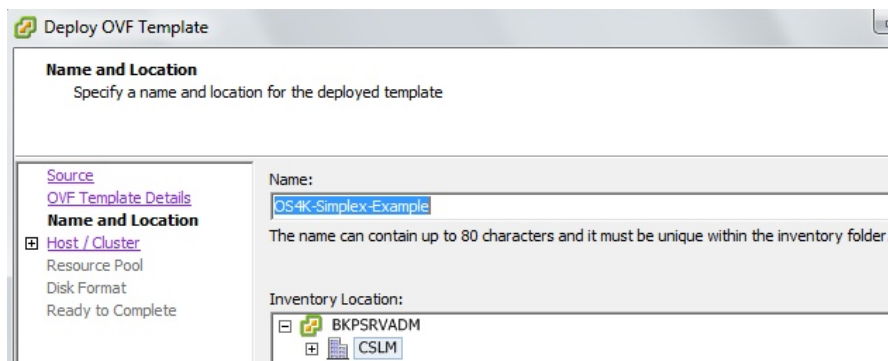


Abbildung 58: Name und Ort für die OVF-Vorlage festlegen (Name and Location)

Anmerkung: Bei der Installation einer Duplex ist es hilfreich im Namen Kennzeichnungen für die Knoten zu verwenden (NodeA, NodeB, QUORUM).

Klicken Sie auf **Next**.

- 6) Cluster und Host festlegen.

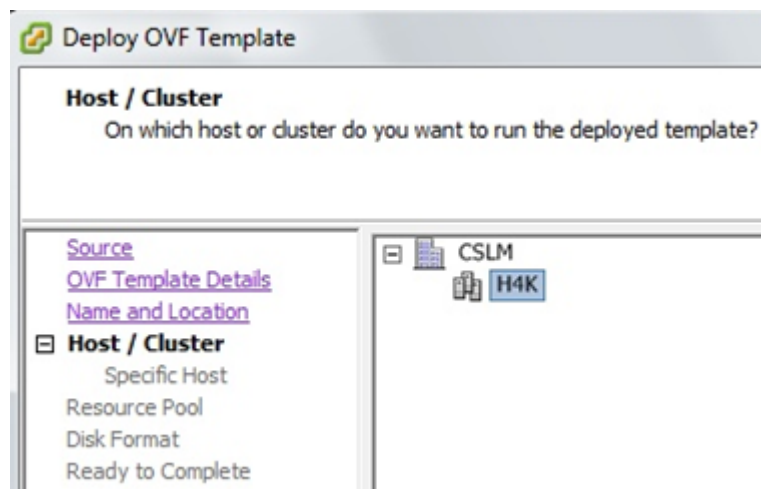


Abbildung 59: Cluster/Host festlegen (Host / Cluster)

Klicken Sie auf **Next**.

- 7) In diesem Fenster wird die Hardware angezeigt auf der die virtuelle Maschine installiert wird.

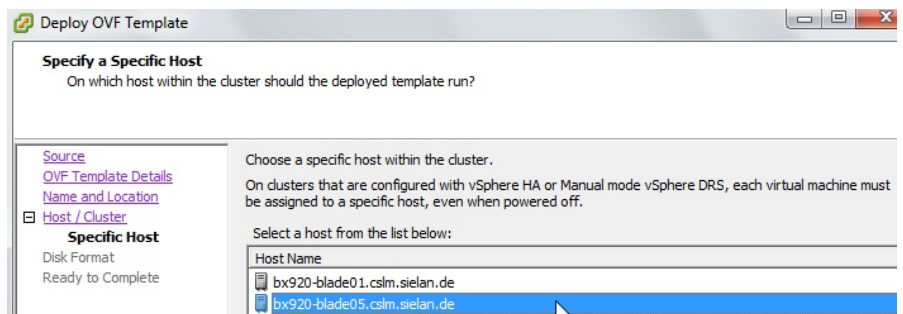


Abbildung 60: Hardware festlegen auf der die virtuelle Maschine installiert wird (Specific Host)

Klicken Sie auf **Next**.

- 8) Wählen Sie den Installationsort (**Storage**) aus.

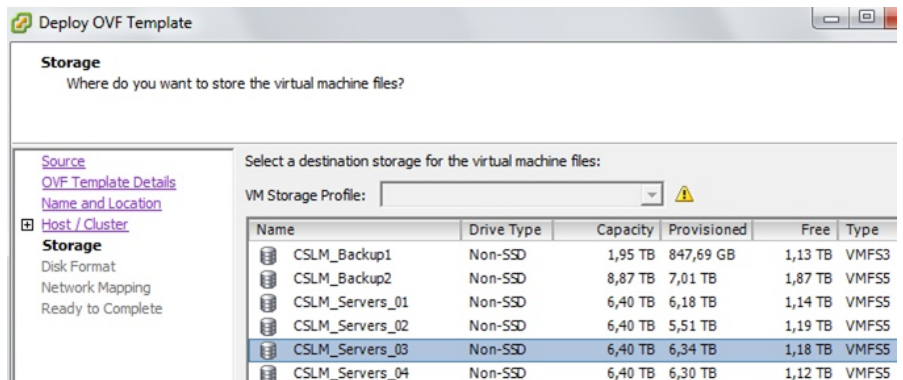


Abbildung 61: Installationsort für das OVF auswählen (Storage)

Klicken Sie auf **Next**.

- 9) Format auswählen.

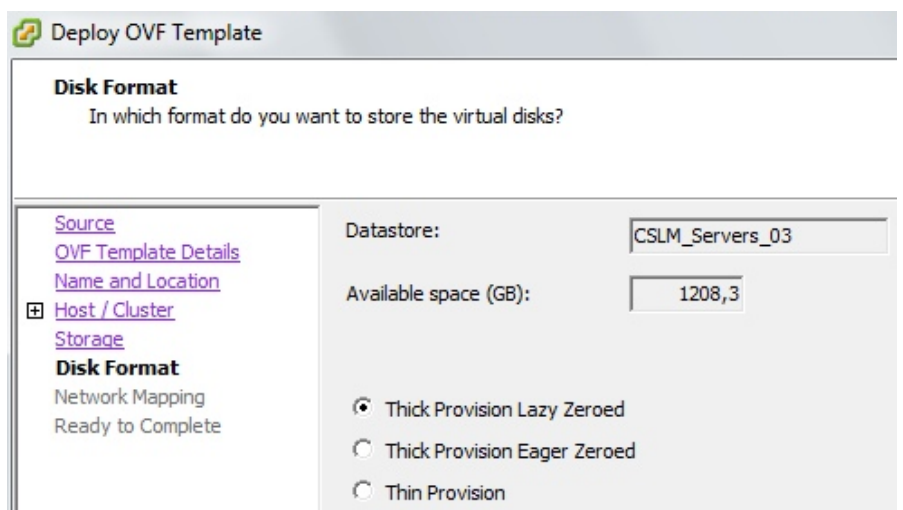


Abbildung 62: Format auswählen (Disk Format)

Klicken Sie auf **Next**.

10) Netzwerke auswählen.

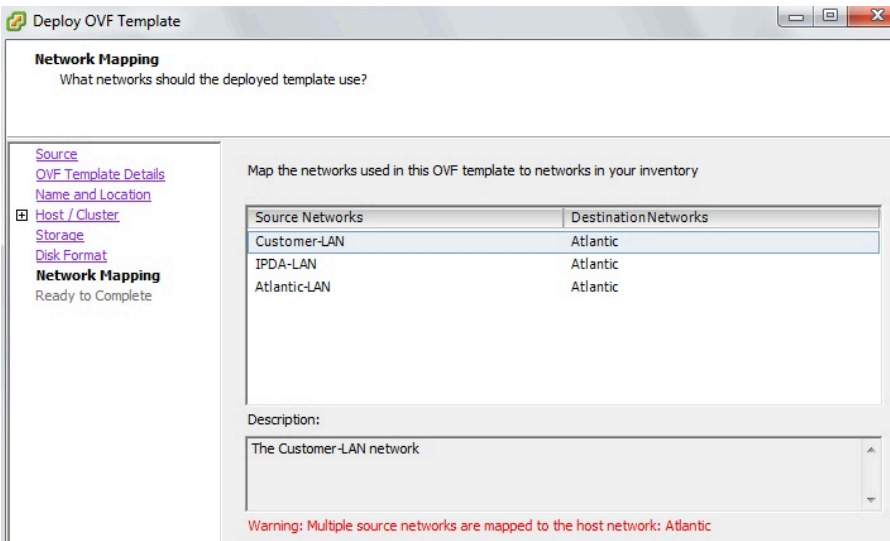


Abbildung 63: Netzwerke auswählen (Network Mapping)

Wichtig: Die angezeigte Warnung kann ignoriert werden, da erst nach der Installation die LAN-Zuordnung getroffen werden kann. vSphere trägt automatisch das erste gefundene Netzwerk ein.

Klicken Sie auf **Next**.

11) Es wird eine Zusammenfassung angezeigt.

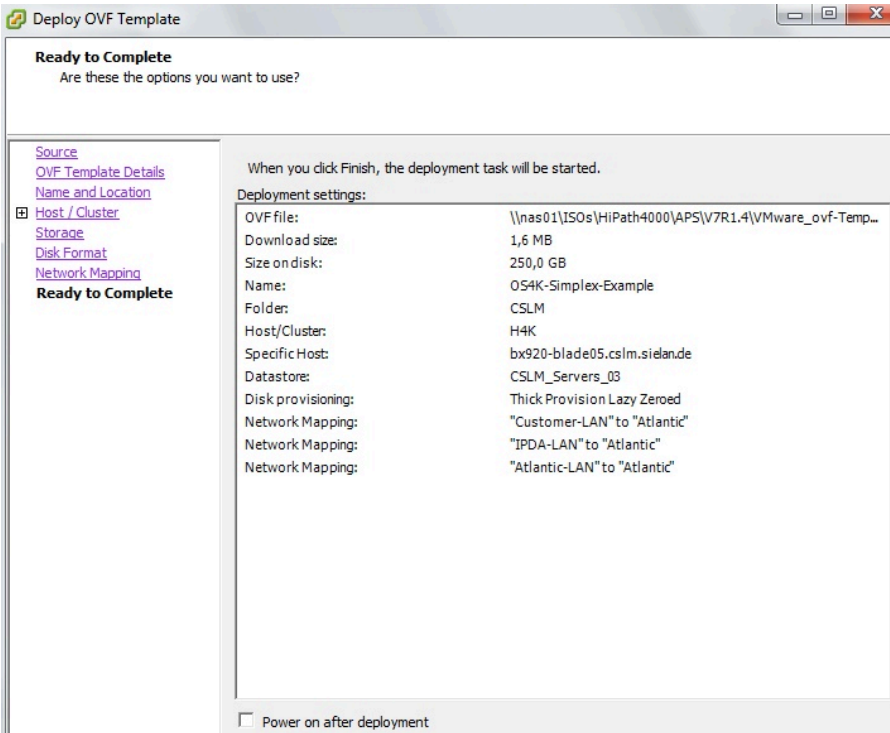


Abbildung 64: Zusammenfassung (Ready to Complete)

Klicken Sie auf **Fertigstellen**.

12) Import der OVF-Vorlage abschließen.

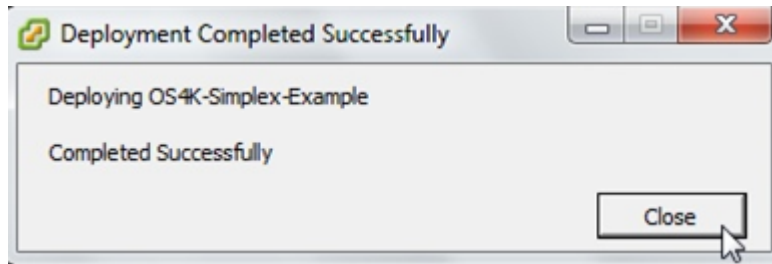


Abbildung 65: OVF-Import abschließen

Klicken Sie auf **Schließen**.

Die virtuelle Maschine ist nun installiert und weitere Einstellungen können mittels vSphere Client vorgenommen werden.

3.8 CPU Shares

Für die Bereitstellung von ausreichend CPU Ressourcen auf ESXi-basierten Systemen, wird für alle OpenScape 4000 Deployments empfohlen die CPU Shares der jeweiligen virtuellen Maschine nach dem OVF-Import auf "High" zu setzen. Das Setzen dieser Einstellung erfolgt z.B. per vSphere Client.

- 1) Wählen Sie die virtuelle Maschine aus und wählen Sie **Edit Settings**.

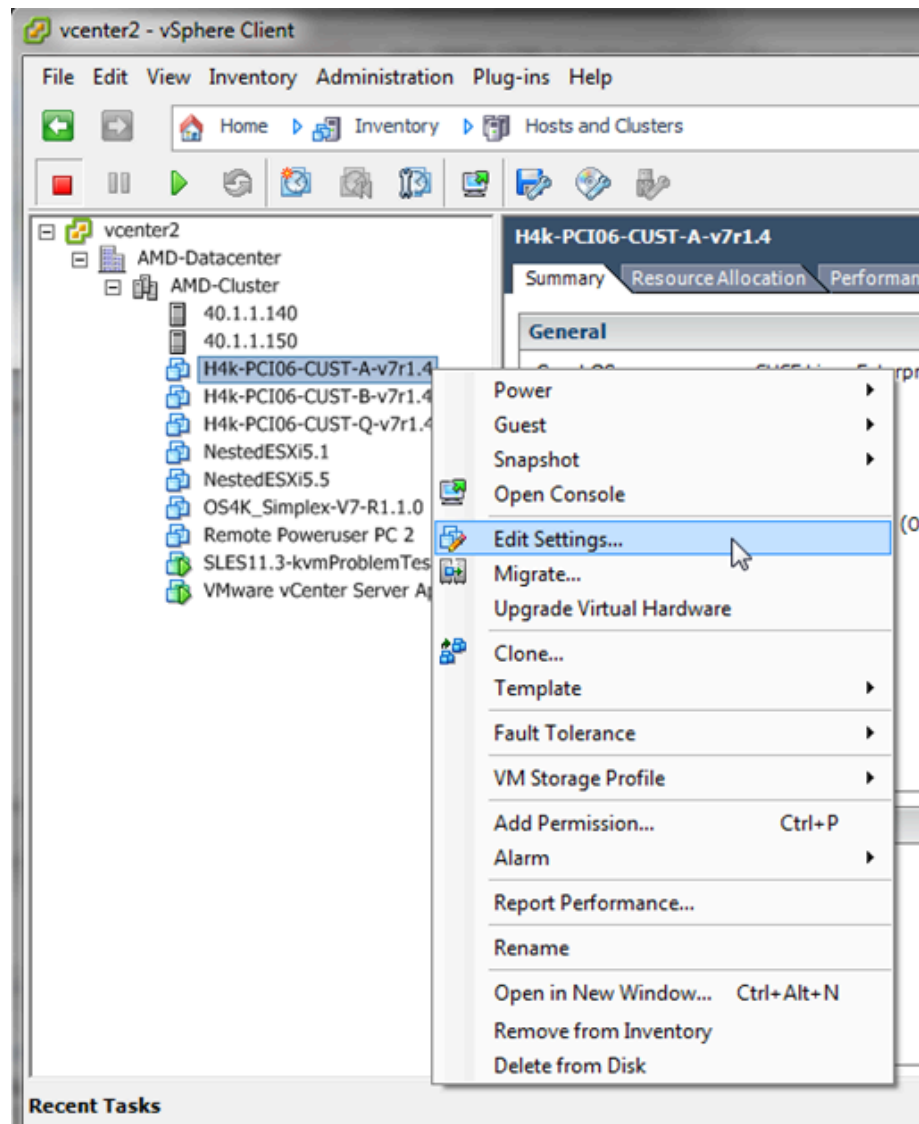


Abbildung 66: Virtuelle Maschine auswählen und Edit Settings Menü aufrufen

2) Änderung der Einstellungen der virtuellen Maschine im Register **Resources**.

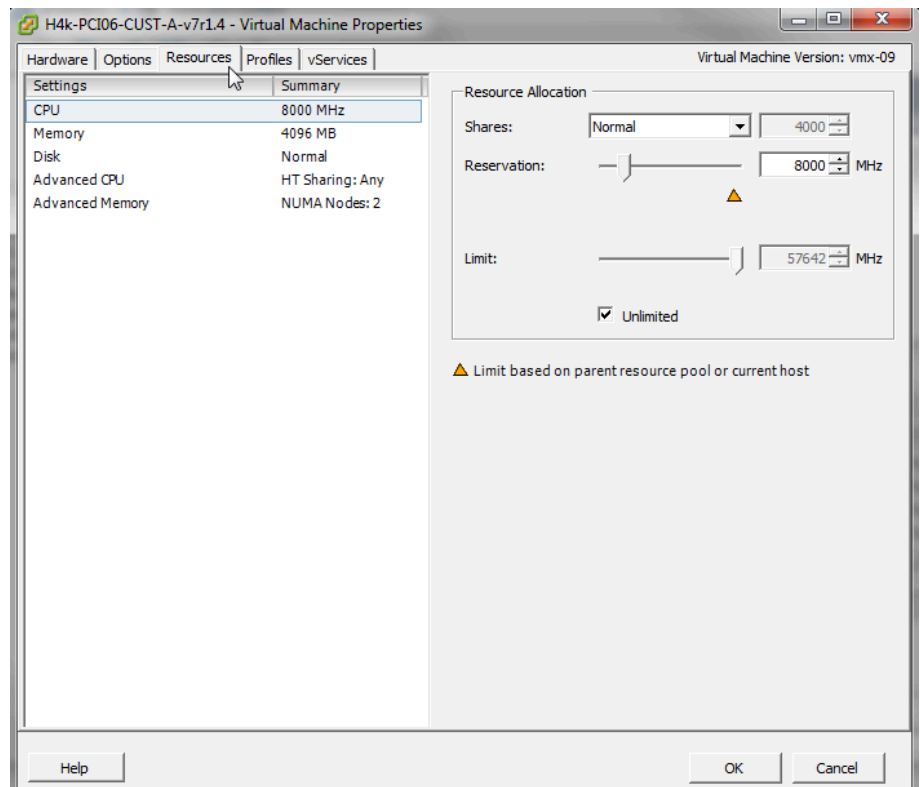


Abbildung 67: Register Resources

- 3) Im Bereich **Resource Allocation** wählen Sie aus der Klappliste **Shares** den Eintrag **High** aus.

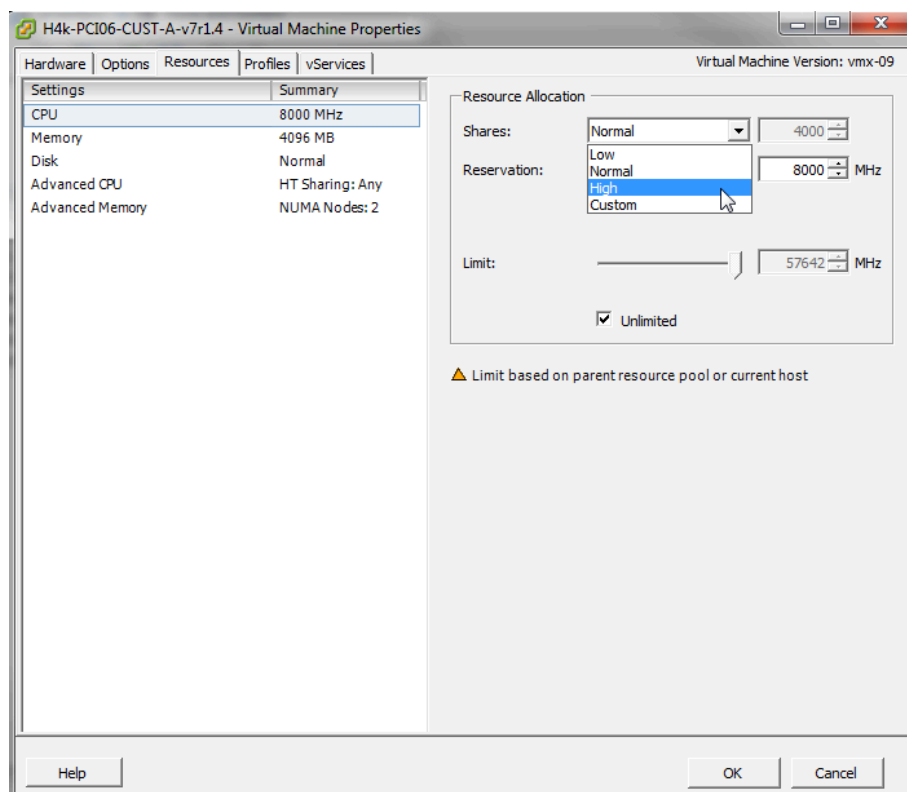


Abbildung 68: CPU Share auf High setzen

Wichtig: Der Default-Wert von 8000 Mhz bei **Reservation** darf nicht verändert werden.

Anmerkung: Bei Bereitstellung über OVF kann auch "Custom" (benutzerdefiniert) statt "High" (hoch) angezeigt werden. Es kann sowohl "Custom" als auch "High" verwendet werden. Der Wert der Reservierungen ist hier das Wichtige (dieser muss die unter OpenScape Virtual Machine Resourcing und im Configuration Guide genannten Anforderungen erfüllen).

- 4) Bestätigen Sie die Änderung mit **OK**.

3.9 Trennen nicht verwendeter Netzwerkadapter

Wichtig: Nach dem OVF-Import ist es zwingend notwendig alle nicht verwendeten Netzwerkadapter zu trennen.

Z.B. für ein Simplex-Deployment bei dem das Administration LAN und das IPDA LAN eth0 gemeinsam benutzen und es keine ATLAN Verbindung gibt, sollte bei den Netzwerkadaptern 2 und 3 die Checkbox **Connect...** deaktiviert werden.

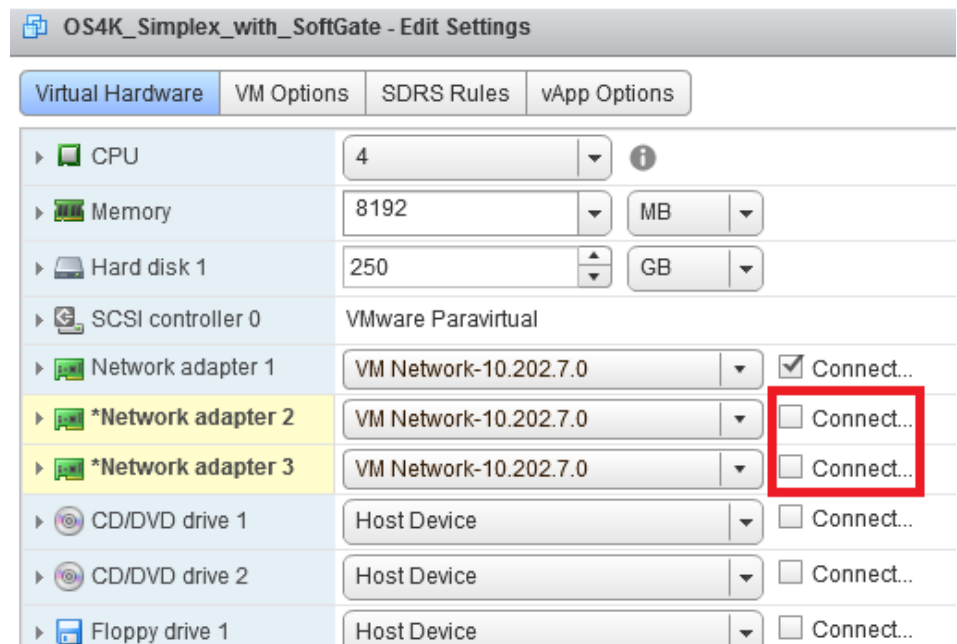


Abbildung 69: Netzwerkadapter trennen

3.10 Erst-Installations-XML-Datei erzeugen

Die `firstinst-netw*.xml` wird wie üblich erzeugt. Nun muss noch die MAC-Adresse (siehe [Section 3.11.1, "MAC-Adresse"](#)) und die IP-Adresse für den DNS-Server (siehe [Section 3.11.2, "DNS-Server"](#)) eingetragen werden.

3.10.1 MAC-Adresse

Die `firstinst-netw*.xml` wird wie üblich erzeugt und muss nun mit der MAC-Adresse versorgt werden.

Tragen Sie die MAC-Adresse der Netzwerk-Karte der virtuellen Maschine an die entsprechende Stelle der `firstinst-netw-*.xml`-Datei ein:

```
entry="mac-address">mac-adresse der netzwerkkarte der virtuellen maschine
```

3.10.1.1 Automatische generierte MAC-Adresse übernehmen (Regelfall)

Nach dem Import der OVF-Vorlage ist die MAC-Adresse in der Regel bereits sichtbar.

Anmerkung: In bestimmten Umgebungen, wird die MAC-Adresse erst generiert, nachdem die Maschine gestartet wurde. Um die MAC-Adresse zu erhalten, müssen Sie dann die virtuelle Maschine starten und gleich wieder stoppen.

Suchen Sie die automatisch erzeugte MAC-Adresse und tragen Sie diese dann in die `firstinst-netw-*.xml` ein.

Wählen Sie die virtuelle Maschine aus. Gehen Sie dann auf das Register **Getting Started** und klicken Sie in der Spalte **Hardware** auf **Network adapter 1**. Die MAC-Adresse finden Sie dann auf der rechten Seite im Bereich **MAC Address**.

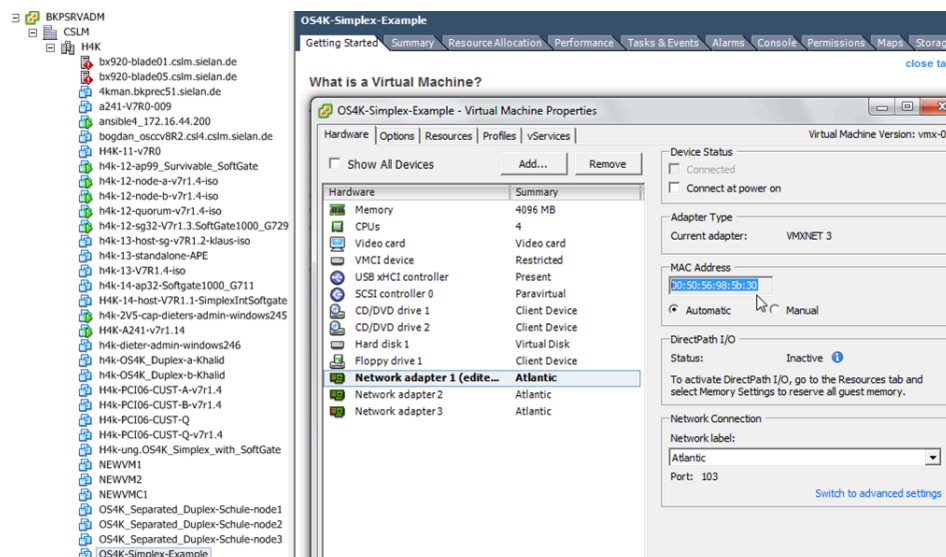


Abbildung 70: Automatische Vergabe der MAC-Adresse der virtuellen Maschine

3.10.1.2 Manuell generierte MAC-Adresse übernehmen (Staging Center)

Laut aktueller Anforderung des Service, soll die endgültige Lizenz des Kunden im Staging Center verwendet werden. Hierzu muss die vom Kunden abgefragte und gelieferte MAC-Adresse eingetragen werden.

Wichtig: Es kann nur eine beim Kunden manuell erzeugte MAC-Adresse eingetragen werden. Eine automatisch erzeugte MAC-Adresse kann nicht manuell eingetragen werden.

Wählen Sie die virtuelle Maschine aus. Gehen Sie dann auf das Register **Getting Started** und klicken Sie in der Spalte **Hardware** auf **Network adapter 1**. Die MAC-Adresse finden Sie dann auf der rechten Seite im Bereich **MAC Address**. Wählen Sie nun die Auswahl **Manual** und tragen Sie die MAC-Adresse ein.

OpenScape 4000 Installation auf VMware ESXi Floppy Image mit dem Inhalt der firstinst-netw-*.xml erzeugen

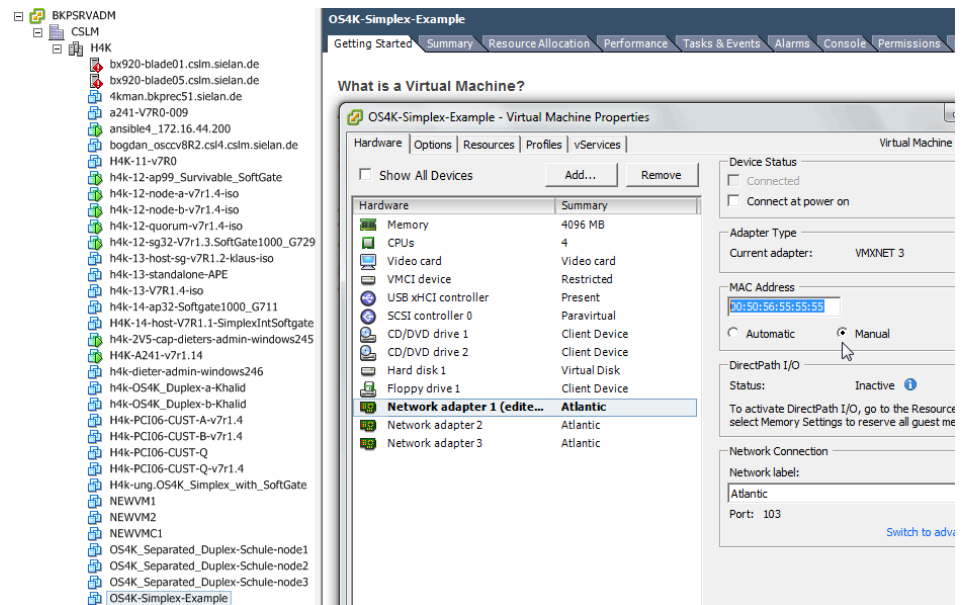


Abbildung 71: Manuelle Vergabe der MAC-Adresse der virtuellen Maschine

Tragen Sie nun noch die MAC-Adresse in die `firstinst-netw-*.xml` ein.

3.10.2 DNS-Server

Es muss ein gültiger und erreichbarer DNS-Server konfiguriert werden.

Der DNS-Server wird benötigt, damit der CLA-Daemon korrekt arbeitet. Ohne DNS-Server können Sie das System nicht mit einer gültigen Lizenz versorgen.

Es würden auch unerwünschte Zustände durch Timeouts beim Polling einer ungültigen/nicht erreichbaren DNS-IP-Adresse eintreten.

3.11 Floppy Image mit dem Inhalt der firstinst-netw-*.xml erzeugen

Auch bei der Installation mit einer ISO-Datei soll die Konfiguration der OpenScape 4000 schon während des Erstinstallationsvorganges durchgeführt werden.

Dazu wird wie bisher die Datei: `firstinst-netw-*.xml` verwendet.

Da die ISO-Datei (anders als der bisher verwendete USB-Stick) nicht beschrieben werden kann, wird als zusätzliches Medium eine Floppy Image Datei verwendet.

Eine leere Floppy Image Datei (`empty.flp`) ist Teil der Auslieferung.

Um auf dieses Floppy Image den Pfad `/config` erstellen zu können und darunter die `firstinst-netw-*.xml` abzulegen, werden Tools benötigt.

Im folgenden Beispiel werden die M-Tools verwendet, die ebenfalls mit der Installations-ISO-Datei zur Verfügung gestellt werden.

Mit Hilfe des Skripts `prepare.bat` wird in dem Installationsverzeichnis das Floppy Image `install.flp` mit dem Inhalt der `firstinst-netw-*.xml` erzeugt.

Wichtig: Bei einer Separated Duplex-Installation wird die Datei `install.flp` für jeden Knoten - also drei mal - benötigt (für Knoten 1, Knoten 2 und den Quorum). Dazu können Sie die Datei `install.flp` kopieren. Der neue Name sollte weiterhin auf `.flp` enden und ist ansonsten frei wählbar (z.B. `bpa.flp`, `bpb.flp`, `q.flp`).

Wichtig: Falls man ein und dieselbe Floppy Image Datei verwendet, können nicht alle Log-Dateien aufgezeichnet werden, da nur eine Installation hat Schreibrechte und kann Log-Dateien schreiben.

3.12 Hotfix Installation vorbereiten

Während der Erstinstallation können weiterhin Hotfixe für die Plattform und den OpenScape 4000 Assistant aktiviert werden. Hierfür muss eine eigene ISO-Datei, die nur die Hotfixe beinhaltet, erzeugt werden.

Anmerkung: Falls kein entsprechendes Tool zur Verfügung steht, kann auch das ebenfalls auf der Installations-ISO-Datei ausgelieferte Tool, wie wir es in diesem Beispiel benutzen, verwendet werden.

Kopieren Sie die gewünschten Installationsdateien in den Arbeitspfad des Service PC kopiert.

Anschließend führen Sie das Skript `mk-iso.bat` aus. Dadurch wird die ISO-Datei `hotfixes.iso` mit den Hotfixes (`*.tar`) erzeugt.

3.13 Hardware Virtualisierung auf dem ESXi Host aktivieren

3.13.1 Allgemeine Information

Damit die OpenScape 4000 (Host oder Survivable) installiert werden kann, muss auf der virtuellen Maschine der zentrale Schalter für die Hardwarevirtualisierung (Virtualized Hardware Virtualization (VHV)) aktiviert sein. Dieser Schalter ist in der OVF-Vorlage zwar schon gesetzt, geht aber verloren wenn mit dem "Windows vSphere Client" - wie in unserem Beispiel - installiert wird.

Wird mit dem "vSphere Web Client" installiert, dann geht diese Einstellung nicht verloren. Der vSphere Webclient ist aber nur im VMware vCenter enthalten.

Wichtige Hinweise

- Bei Änderungen an der virtuellen Maschine mit Hilfe des vSphere Clients kann diese Einstellung erneut verloren gehen und muss wieder gesetzt werden.

- Der vSphere Client deaktiviert diese Einstellung automatisch, falls ein LAN-Kabel im ausgeschalteten Zustand deaktiviert wird.

Wichtig: Diese Einstellung sollte deshalb nach der Installation, dem Herausnehmen der DVD und dem Zuordnen der LAN-Schnittstellen kontrolliert werden.

3.13.2 Hardwarevirtualisierung aktivieren mit vSphere Client

Voraussetzung: Die virtuelle Maschine ist nicht aktiv!

Maschine in hellblau zeigt den Zustand **power off** an.

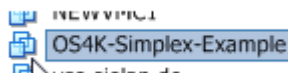


Abbildung 72: Virtuelle Maschine ist nicht aktiv.

Führe Sie nun die folgenden Schritte durch:

- Suchen Sie die virtuelle Maschine im Datastore und exportieren Sie die VMX Datei.
- Fügen Sie die Zeile `vhv.enable = "TRUE"` in die Datei ein.
- Importieren Sie diese korrigierte VMX Datei.

1) VM > Edit Setting

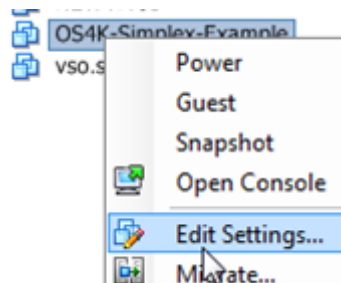


Abbildung 73: Einstellungen der virtuellen Maschine

- 2) Wählen Sie den Register **Options**.

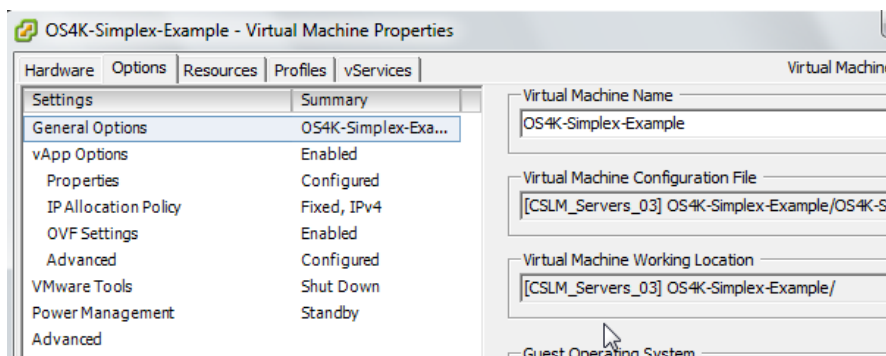


Abbildung 74: Konfigurationsdatei der virtuellen Maschine

Notieren Sie sich den Eintrag in der Zeile **Virtual Machine Configuration File** (in unserem Beispiel: [CSLM_Servers_03] OS4K-Simplex-Example/OS4K-Simplex-Example.vmx).

- 3) Die hier angezeigte Datei muss nun extrahiert werden. Schließen Sie hierfür das Edit-Fenster.
- 4) Wählen Sie den Register **Summary**.
- 5) Klicken Sie mit rechter Maustaste auf den Eintrag unter der Zeile **Storage**.
- 6) Wählen Sie **Browse Datastore**.

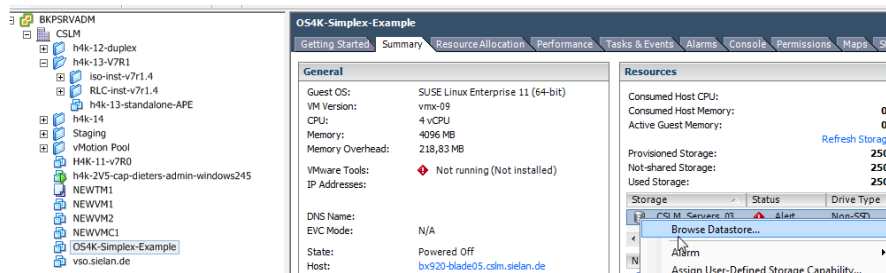


Abbildung 75: Datastore durchsuchen

- 7) Suchen Sie das Verzeichnis des zuvor notierten Eintrags (hier: OS4K-Simplex-Example).

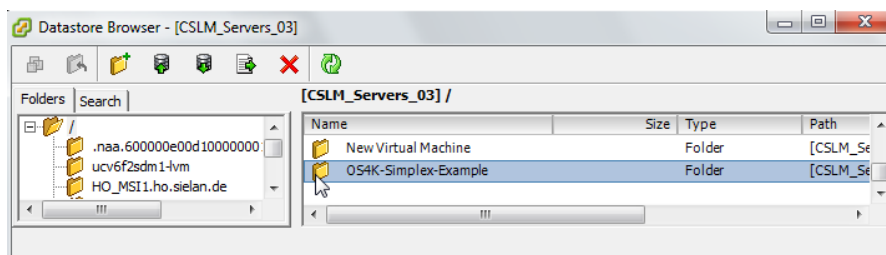


Abbildung 76: Verzeichnis der Konfigurationsdatei auswählen

- 8) Führen Sie einen Doppelklick auf die virtuelle Maschine aus.

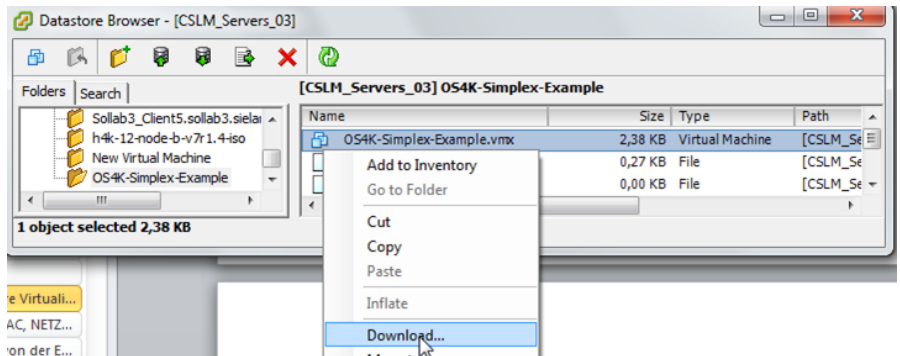


Abbildung 77: Konfigurationsdatei auswählen und exportieren

- 9) Selektieren Sie die VMX-Datei mit der rechten Maustaste. Wählen Sie **Download** und speichern Sie die Datei lokal auf Ihrem PC.
- 10) Öffne Sie die Datei in einem Text-Editor. Füge sie die Zeile `vhv.enable = "TRUE"` hinzu.

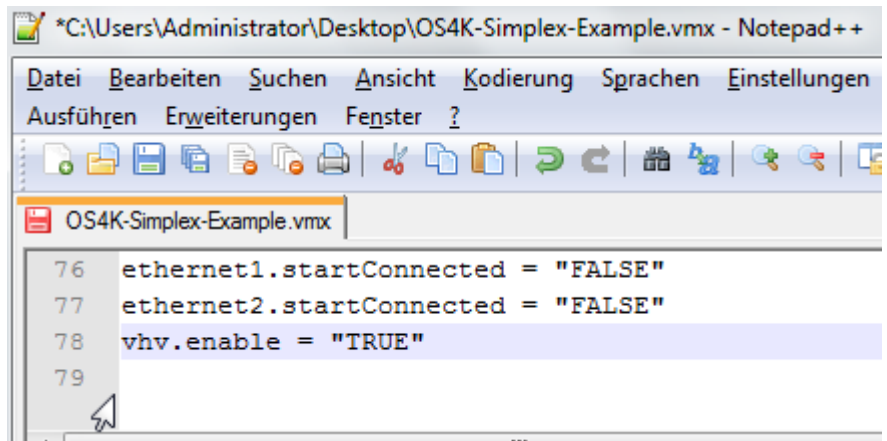


Abbildung 78: Konfigurationsdatei für Hardwarevirtualisierung bearbeiten

- 11) Speichern Sie die Datei und importieren Sie die Datei wieder - mit dem vSphere Client, um den Upload der VMX-Datei durchzuführen.

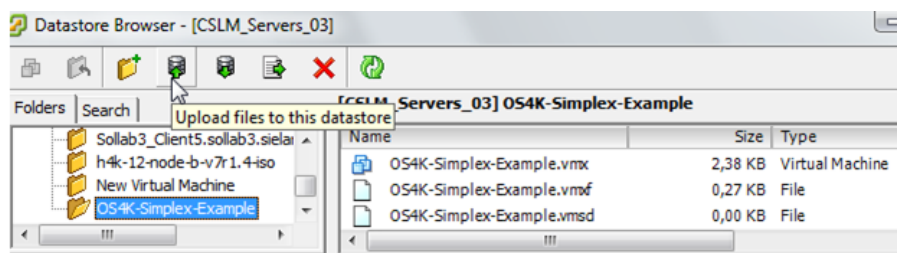


Abbildung 79: Konfigurationsdatei in Datastore importieren

3.13.3 Hardwarevirtualisierung aktivieren mit vSphere Web Client

Der Parameter muss unter **CPU > Hardware virtualization** aktiviert werden, indem man die Checkbox **Expose hardware assisted virtualization to the guest OS** aktiviert.

3.14 OpenScape 4000 Installation in der virtuellen Maschine

3.14.1 Vorbereitungen

Hardwarevirtualisierung

Stellen Sie sicher, dass die Hardwarevirtualisierung aktiviert ist (siehe auch [Section 3.7.2, "Hardwarevirtualisierung"](#)).

installimage.iso und Floppy Image mit dem ESXi Host verbinden

- 1) Starten Sie die virtuelle Maschine

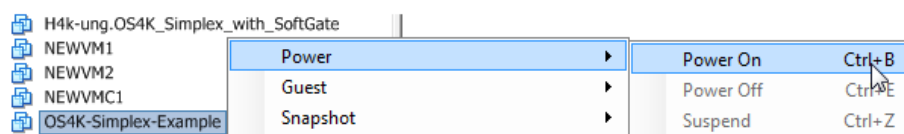


Abbildung 80: Virtuelle Maschine starten

- 2) Öffnen Sie die Konsole

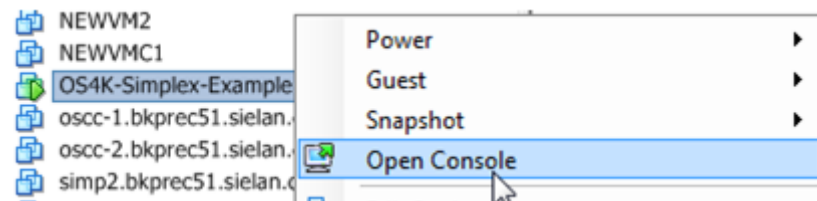


Abbildung 81: Konsole öffnen

3) Verbinden Sie die installimage.iso mit dem ESXi Host

Wählen Sie in der Konsole über DVD die installimage.iso aus.

Konsole > CD/DVD drive 1 > Connect to ISO image on a datastore

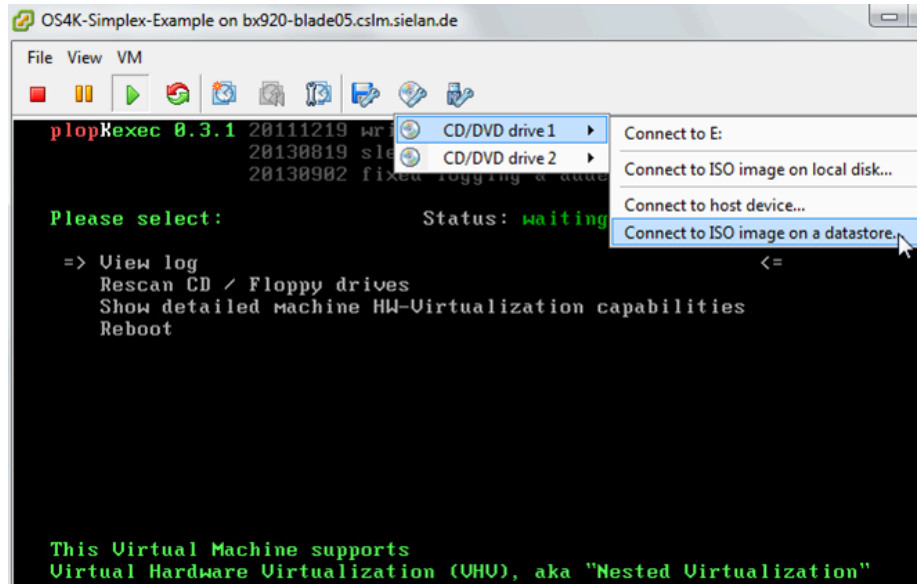


Abbildung 82: ISO-Image auf Datastore mit ESXi Host verbinden

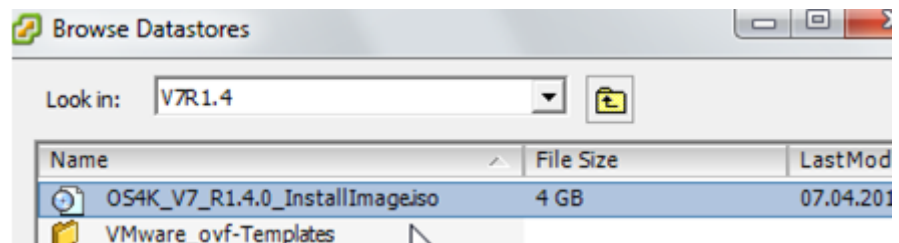


Abbildung 83: ISO-Image auswählen

Warten Sie, bis die Meldung => sr0: OpenScape 4000 version num... angezeigt wird.

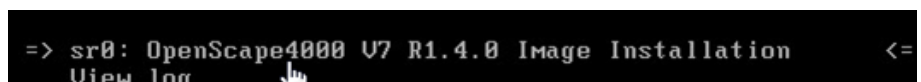


Abbildung 84: ISO-Image auf Datastore ist mit ESXi Host verbunden

4) Verbinden Sie das Floppy Image mit dem ESXi Host

Konsole > Floppy drive 1 > Connect to floppy image on local disk

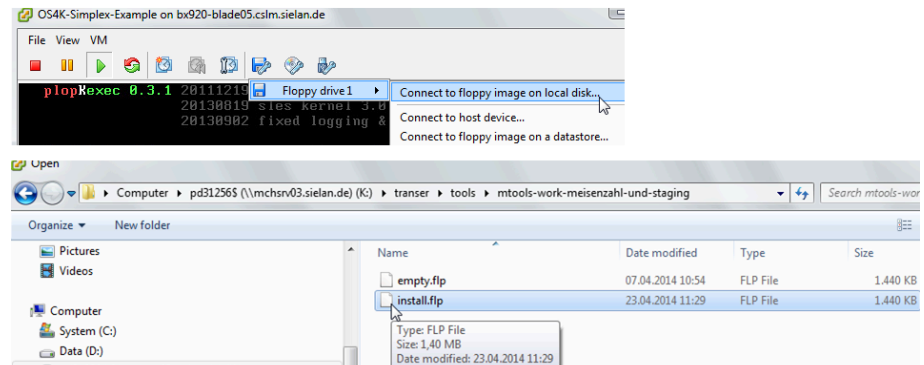


Abbildung 85: Floppy Image mit ESXi Host verbinden

Warten Sie, bis die Meldung `fd0: /config` angezeigt wird.

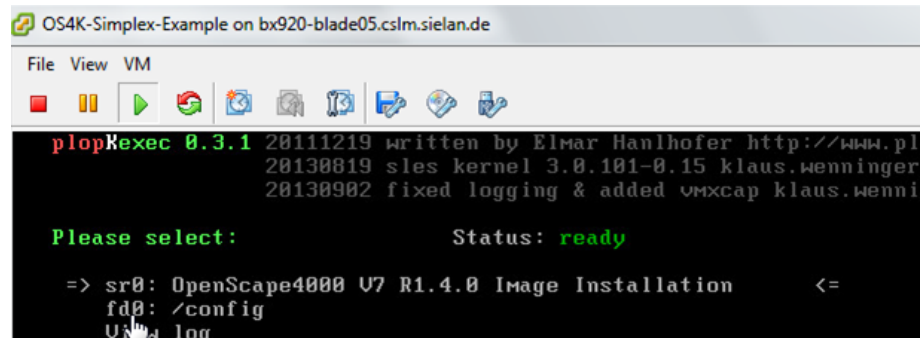


Abbildung 86: Floppy Image ist mit ESXi Host verbunden

5) Verbinden Sie die `hotfix.iso` mit dem ESXi Host

Anmerkung: Falls keine Hotfixe installiert werden sollen, überspringen Sie diesen Schritt.

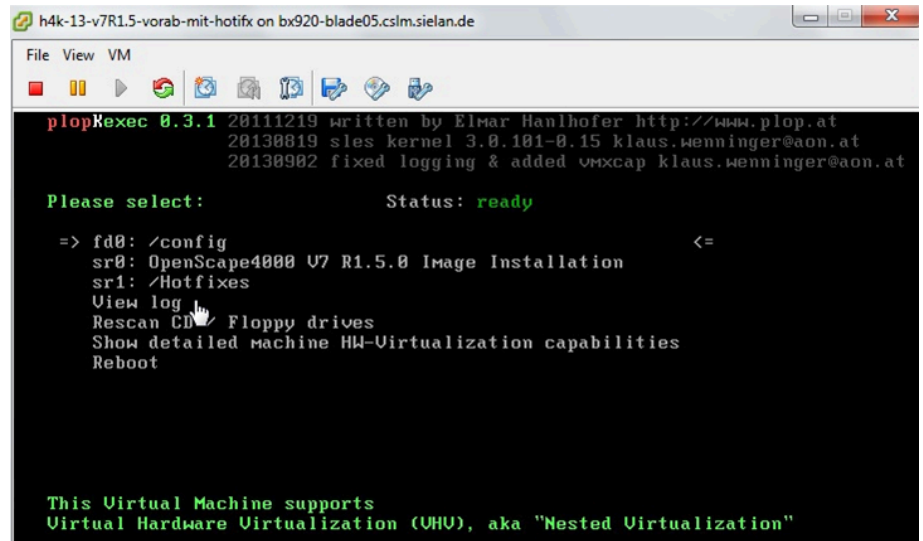


Abbildung 87: hotfix.iso mit ESXi Host verbinden

Wählen Sie mit den Cursortasten **sr0: OpenScape 4000 software version Image Installation** (hier **OpenScape 4000 V7 R1.5.0**) und drücken Sie die Eingabetaste.

3.14.2 Installation starten

- 1) Zum Starten der Installation klicken Sie ins Konsolenfenster und bestätigen Sie mit Return.
- 2) Akzeptieren Sie die Eula mit **Accept and install**.

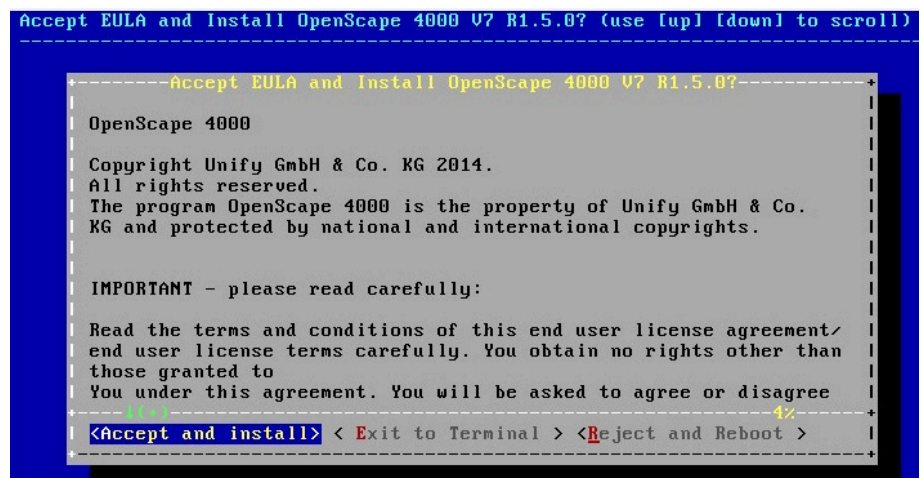


Abbildung 88: Eula akzeptieren

Die Installation wird durchgeführt.

OpenScape 4000 Installation auf VMware ESXi

Anpassungen nach der Installation

- 3) Nach ca. 25 Minuten sollte die Installation erfolgreich durchgeführt worden sein.
- 4) Entfernen Sie nun das Floppy Image und bestätigen Sie mit Ok. Das System wird neu gestartet.

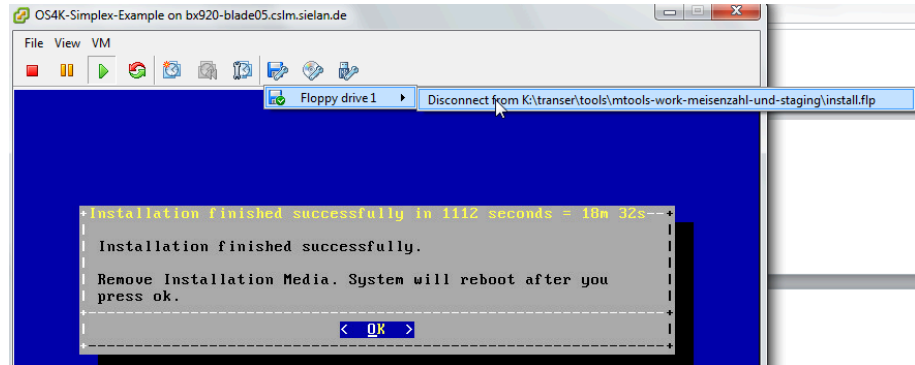


Abbildung 89: Installation erfolgreich

3.15 Anpassungen nach der Installation

3.15.1 Zuordnung der LAN-Schnittstellen zu den Netzwerkschnittstellen

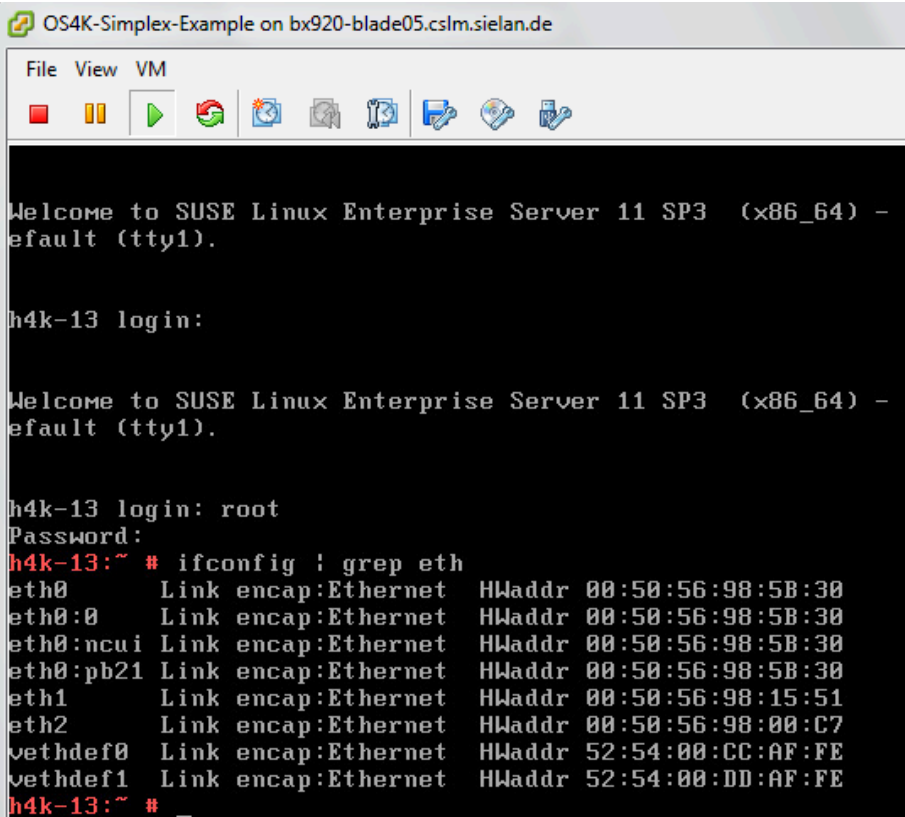
- 1) Fragen Sie die Zuordnung der Netzwerke zu den eth-Schnittstellen mit Hilfe der XML-Datei ab.

```

1  <?xml version="1.0" encoding="UTF-8"?>
2
3  <properties>
4    <comment>Mon Feb 24 12:58:14 CET 2014 Firstinstall Script Versi
5
6  <common>
7    <entry key="system-deployment">simplex</entry>
8    <entry key="customer-portal.ip">192.168.220.177/24</entry>
9    <entry key="customer-lan.assistant-ip-address">192.168.220.175/2
10   <entry key="customer-lan.csta-ip-address">192.168.220.176/24</en
11   <entry key="atlantic-interface.0">eth1</entry>
12   <entry key="ipda-interface">eth0</entry>
13   <entry key="ipda-lan.cca-ip-address">192.168.220.178/24</entry>
14   <entry key="ipda-lan.default-router-ipda">192.168.220.1</entry>
15   <entry key="internal-lan.network">192.168.187.0</entry>
16   <entry key="customer-def.gw">192.168.220.1</entry>
17   <entry key="integrated-softgate">1</entry>
18 </common>
19 <node1>
20   <entry key="system-root.password">$2y$10$e6tcBA.T4yUJcqP65AqVDeq
21   <entry key="mac-address">00:50:56:98:5b:30</entry>
22   <entry key="customer-interface">eth0</entry>
23   <entry key="eth0.ip.0">192.168.220.174/24</entry>
24   <entry key="eth0.hostname.0">h4k-13</entry>
25   <entry key="eth0.domainname.0">h4k.sielan.de</entry>
26   <entry key="eth1.ip.0">0.0.0.0/0</entry>
27   <entry key="customer-ntp.server.0">192.168.11.33</entry>
28   <entry key="customer-timezone">Europe/Berlin</entry>
29   <entry key="customer-keyboard-layout">german</entry>
30   <entry key="customer-def.gw.dev">eth0</entry>
31 </node1>
  
```

Abbildung 90: Zuordnung der Netzwerke zu den eth-Schnittstellen

- 2) Ermitteln Sie anhand der eth-Schnittstellen mit Hilfe des Konsolenbefehls `ifconfig | grep eth` die MAC-Adresse der Schnittstellenkarten.



```
OS4K-Simplex-Example on bx920-blade05.cslm.sielan.de
File View VM
Welcome to SUSE Linux Enterprise Server 11 SP3 (x86_64) -
default (tty1).
h4k-13 login:
Welcome to SUSE Linux Enterprise Server 11 SP3 (x86_64) -
default (tty1).
h4k-13 login: root
Password:
h4k-13:~ # ifconfig | grep eth
eth0      Link encap:Ethernet  HWaddr 00:50:56:98:5B:30
eth0:0    Link encap:Ethernet  HWaddr 00:50:56:98:5B:30
eth0:ncui Link encap:Ethernet  HWaddr 00:50:56:98:5B:30
eth0:pb21 Link encap:Ethernet  HWaddr 00:50:56:98:5B:30
eth1      Link encap:Ethernet  HWaddr 00:50:56:98:15:51
eth2      Link encap:Ethernet  HWaddr 00:50:56:98:00:C7
vethdef0  Link encap:Ethernet  HWaddr 52:54:00:CC:AF:FE
vethdef1  Link encap:Ethernet  HWaddr 52:54:00:DD:AF:FE
h4k-13:~ #
```

Abbildung 91: MAC-Adressen der eth-Schnittstellen abfragen

- 3) Anhand dieser MAC-Adressen können Sie dann in der virtuellen Maschine die LAN-Zuordnung festlegen.

Öffnen Sie den vSphere Client. Über die Drop-Down-Auswahl klappen Sie **Network Label** auf und wählen das der MAC-Adresse zugeordnete Netzwerk aus.

Im Bereich **Device Status** aktivieren Sie die Checkboxen für **Connected** und **Connected at power on**.

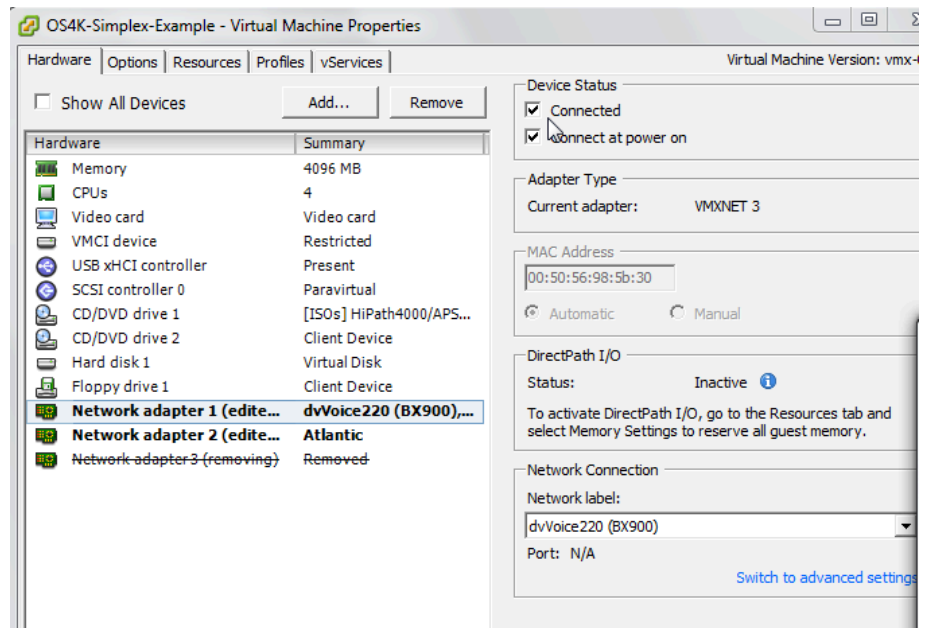


Abbildung 92: LAN-Zuordnung in der virtuellen Maschine

Wichtig: Löschen Sie nicht verwendete Schnittstellen!

3.15.2 Umstellen des DVD-Laufwerkes auf "lokales Gerät"

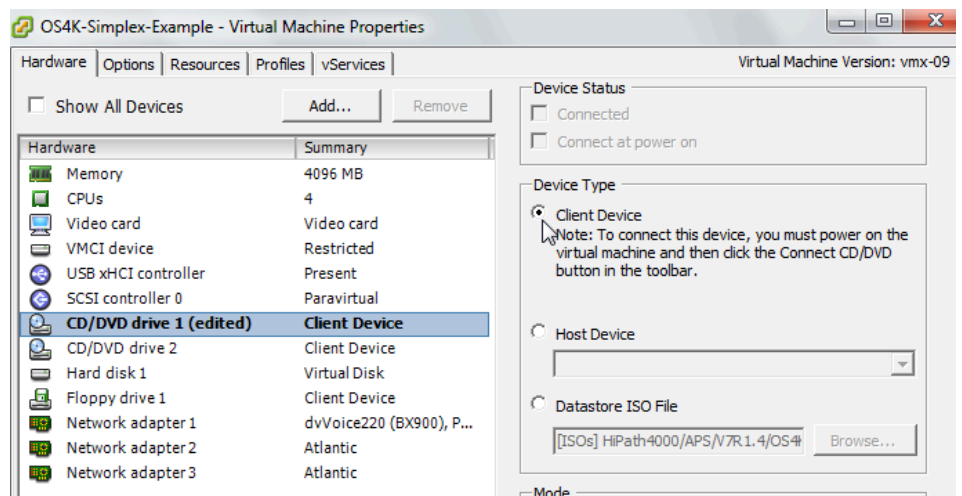


Abbildung 93: DVD-Laufwerk auf "lokales Gerät" umstellen

Ändern Sie den Gerätetyp für die DVD im Abschnitt **Device Type** auf **Client Device**.

Wichtig: Diese Einstellung ist wichtig, weil die virtuelle Maschine nach der Installation nicht mehr vom ISO-Image booten soll.

3.15.3 Auf die Fertigstellung der OpenScape 4000 Assistant Installation warten

Der Installationsstatus des OpenScape 4000 Assistant kann über die **OpenScape 4000 Plattform Administration (Portal)** abgefragt werden.

Status > Assistant Installation Status

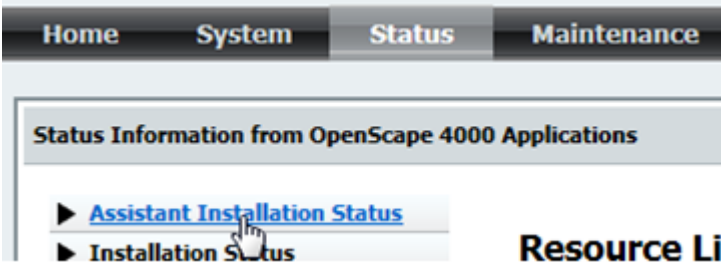


Abbildung 94: Installationsstatus OpenScape 4000 Assistant

3.15.4 Konfigurieren der Kundendaten

Führen Sie wie bisher die RMX und OpenScape 4000 Assistant Konfiguration durch.

3.15.5 Systemstatus überprüfen

Öffnen Sie die **OpenScape 4000 Plattform Administration (Portal)** und überprüfen Sie die Siebensegmentanzeige ob der Status "A" erreicht wurde.

System > Frontpanel.

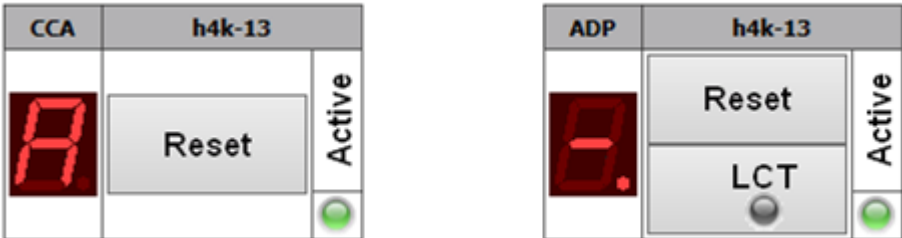


Abbildung 95: Status des Systems überprüfen

3.16 Staging Center Bereitstellung für den Endkunden

3.16.1 Export der virtuellen Maschine in eine OVF-Datei

Verwenden Sie für den Export eine USB-Festplatte, die am Service PC gesteckt ist.

- 1) Fahren Sie die virtuelle Maschine herunter.

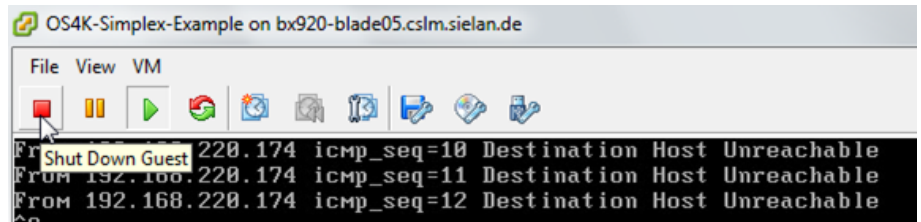


Abbildung 96: Virtuelle Maschine herunterfahren

- 2) Wählen Sie die virtuelle Maschine aus
- 3) Exportieren Sie die OVF-Vorlage

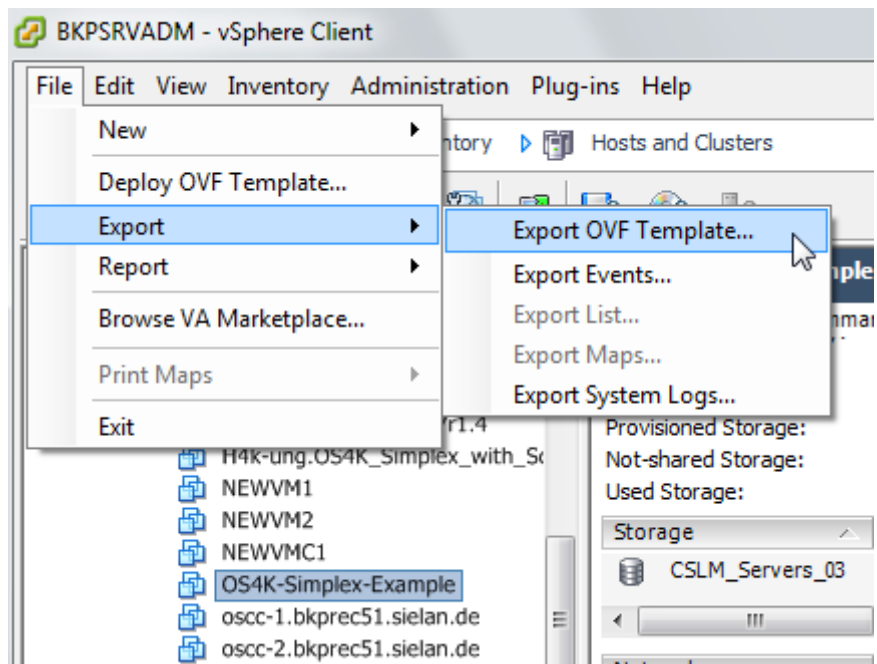


Abbildung 97: OVF-Vorlage exportieren

- 4) Wählen Sie den Speicherort aus und bestätigen Sie mit OK.

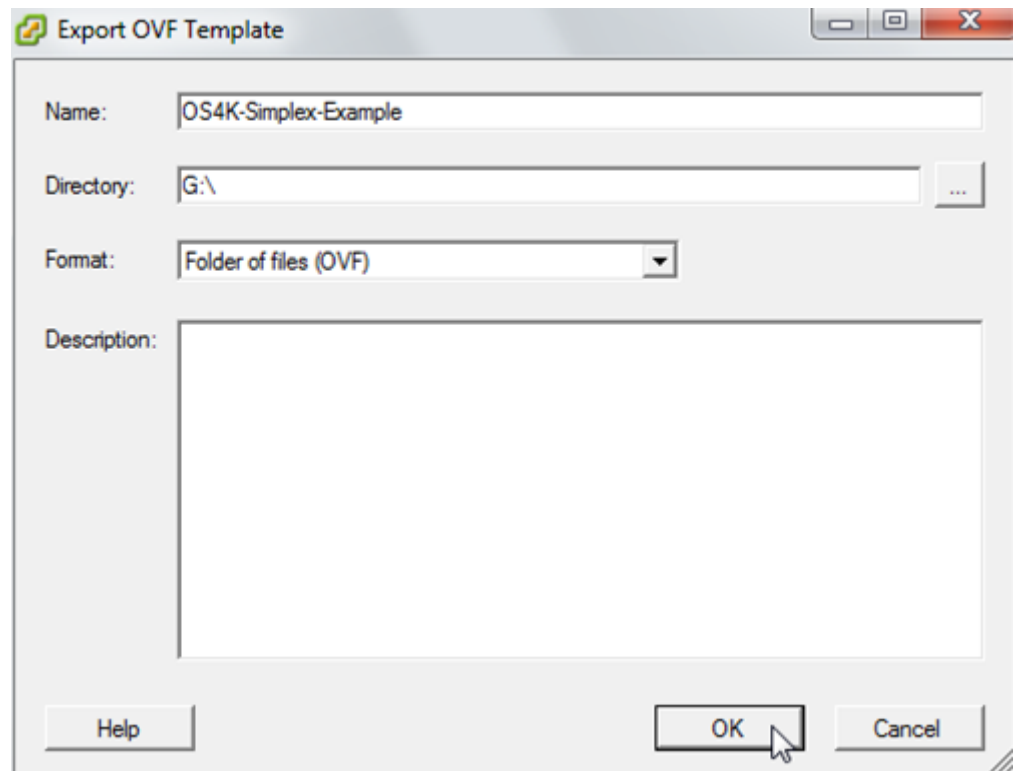


Abbildung 98: Speicherort für die exportierte OVF-Vorlage wählen

3.16.2 Installation beim Endkunden

Installation mit dem Windows vSphere Client

Deploy OVF Template von der USB Festplatte

Nach dem Import (Deploy OVF) geht der Schalter für Hardwarevirtualisierung verloren. Diese Einstellung muss wieder hergestellt werden. Die Vorgehensweise ist im [Section 3.14, "Hardware Virtualisierung auf dem ESXi Host aktivieren"](#) beschrieben.

Installation mit dem vSphere Web Client

Deploy OVF Template von der USB Festplatte

Nach dem Import (Deploy OVF) kann die Maschine direkt gestartet werden.

3.17 Hinweise und Mögliche Fehlerquellen

3.17.1 Log-Dateien während der Installation

Fehlerursachen bei der Installation können oft anhand der auf Floppy geschriebene Logdatei analysiert werden.

Um die Logdateien von der Floppy auf den PC zu kopieren wird das Skript `getlogs.bat` verwendet, dass Bestandteil der Installations-ISO-Datei ist.

3.17.2 Remote Major Update (RMU)

Mit dem Remote Major Update-Prozess kann ein zentrales Host-System, auf dem HiPath 4000 V7R2 ausgeführt wird, aus der Ferne auf OpenScape 4000 V10 aktualisiert werden.

Bei diesem Vorgang wird ein zweites System desselben Hardware-Typs wie das Remote-System verwendet, um ein Recovery ISO-Image vorzubereiten und zu erstellen, das die OpenScape 4000 V10R1 -Software sowie die komplette Systemkonfiguration enthält.

Dieses ISO-Image wird sodann an das Remote-Host-System übertragen und für den Remote Major Update-Prozess verwendet.

3.17.3 Hardwarevirtualisierung nicht aktiviert

Die Hardwarevirtualisierung muss wie im [Section 3.14, "Hardware Virtualisierung auf dem ESXi Host aktivieren"](#) beschrieben aktiviert werden.

Hardwarevirtualisierung bei Erstinstallation nicht aktiviert

Folgende Ausgabe erscheint auf der Konsole, wenn bei der Erstinstallation die Hardwarevirtualisierung nicht aktiviert ist:

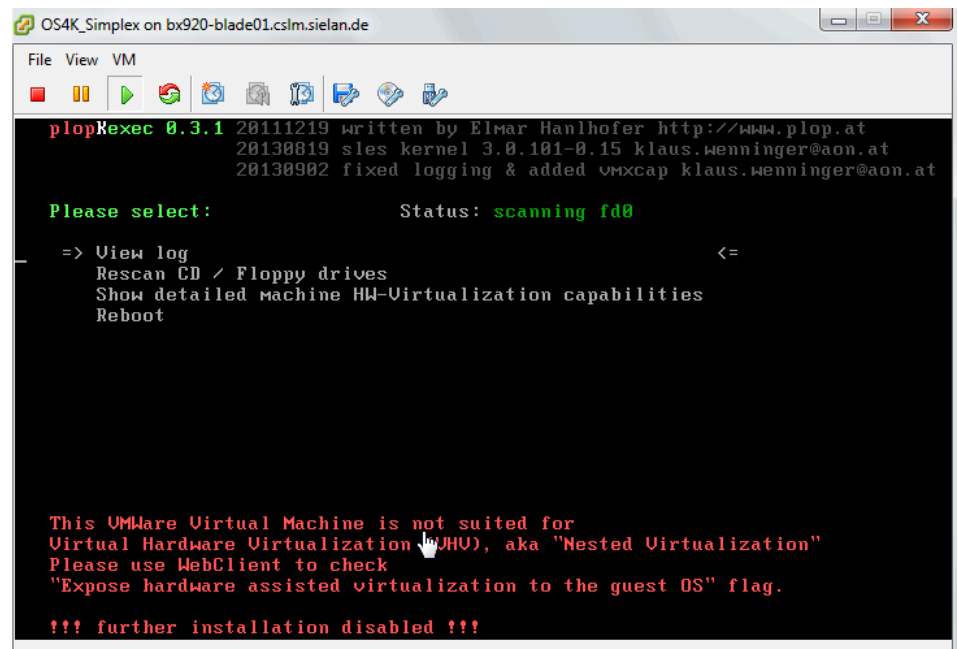


Abbildung 99: Hardwarevirtualisierung bei Erstinstallation nicht aktiviert

Hardwarevirtualisierung nach Änderungen deaktiviert

Folgende Ausgabe erscheint auf der Konsole, wenn nach der Installation eine Änderung mit Hilfe des vSphere Clients durchgeführt wurde, die zur Deaktivierung der Hardwarevirtualisierung geführt hat:

OpenScape 4000 Installation auf VMware ESXi

Re-Installation der OpenScape 4000 Software

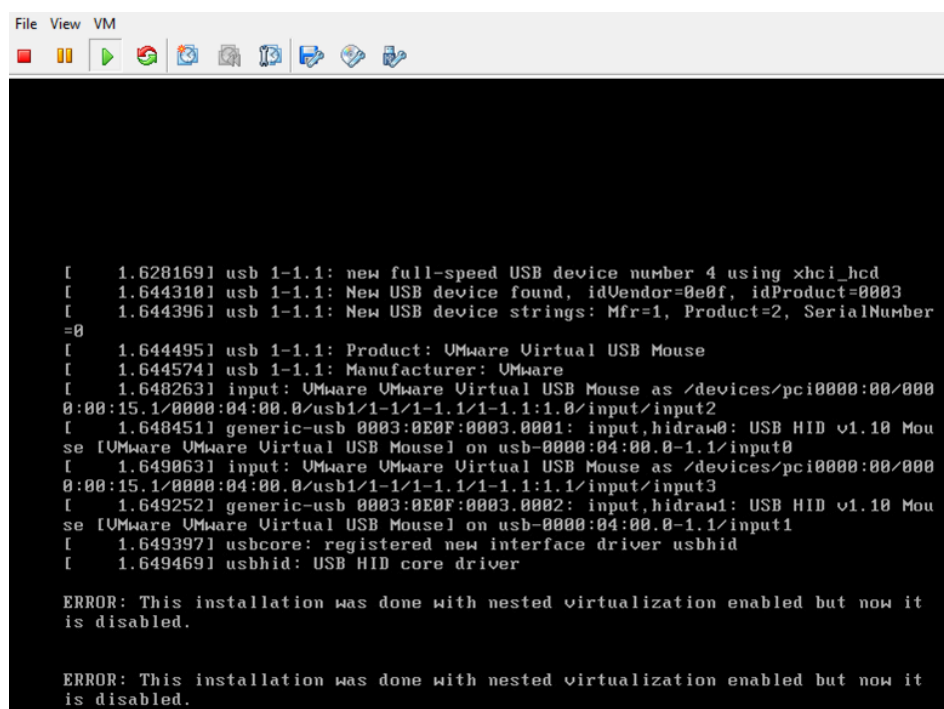


Abbildung 100: Hardwarevirtualisierung nach Änderungen deaktiviert

Aktivieren Sie in beiden Fällen die Hardwarevirtualisierung wie in [Section 3.14, "Hardware Virtualisierung auf dem ESXi Host aktivieren"](#) beschrieben.

3.18 Re-Installation der OpenScape 4000 Software

Vorraussetzung

Die virtuelle Maschine ist hochgefahren und läuft mit der alten Software.

Schritte für die Re-Installation

- 1) Öffnen Sie die Konsole

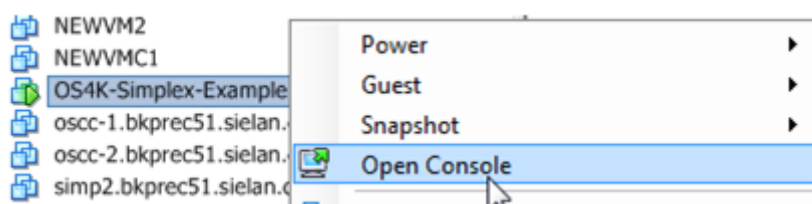


Abbildung 101: Konsole öffnen

1) Verbinden Sie die installimage.iso mit dem ESXi Host

Wählen Sie in der Konsole über DVD die installimage.iso aus.

Konsole > CD/DVD drive 1 > Connect to ISO image on a datastore

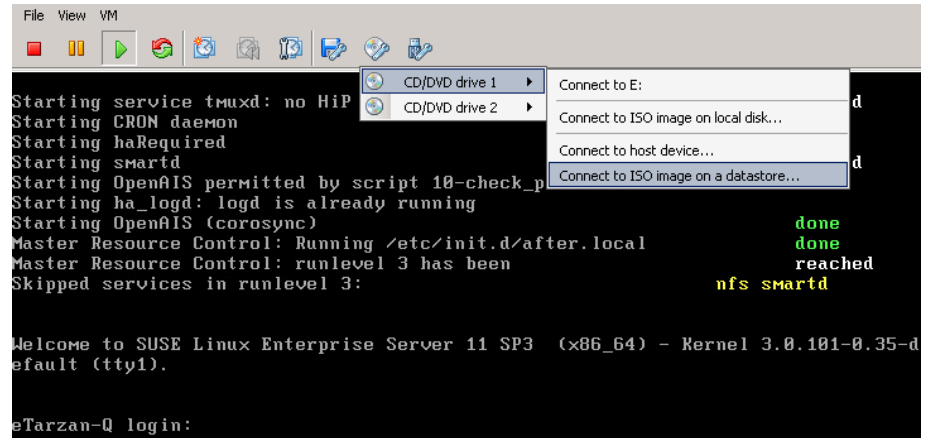


Abbildung 102: ISO-Image auf Datastore mit ESXi Host verbinden

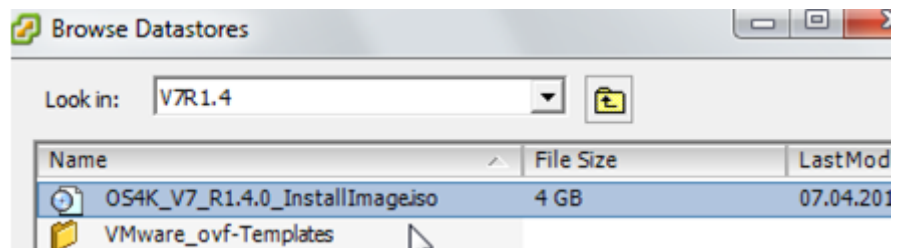
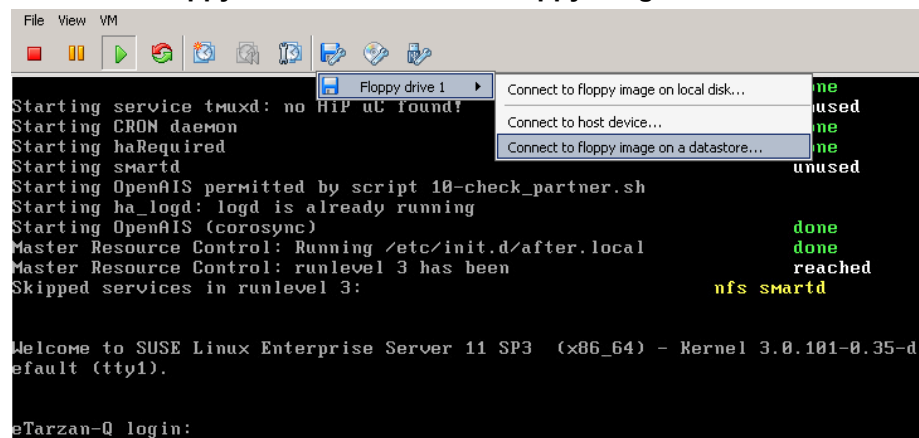


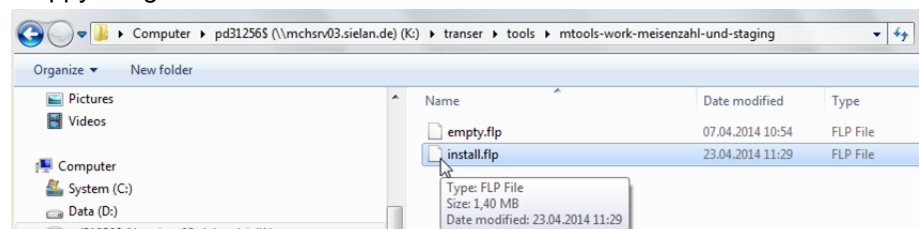
Abbildung 103: ISO-Image auswählen

2) Verbinden Sie das Floppy Image mit dem ESXi Host

Konsole > Floppy drive 1 > Connect to floppy image on a datastore



Floppy Image mit ESXi verbinden



Floppy Image auswählen

Wichtig: Für die Re-Installation müssen Sie ein neues, noch nicht für eine vorherige Installation benutztes Floppy Image (install.flp) mounten.

3) Melden Sie sich an der laufenden virtuellen Maschine an und geben Sie das Kommando `#reboot` ein.

- 4) Wenn die virtuelle Maschine hochfährt, wählen Sie die 3. Boot-Option **plopkexec -- use to reinstall**.

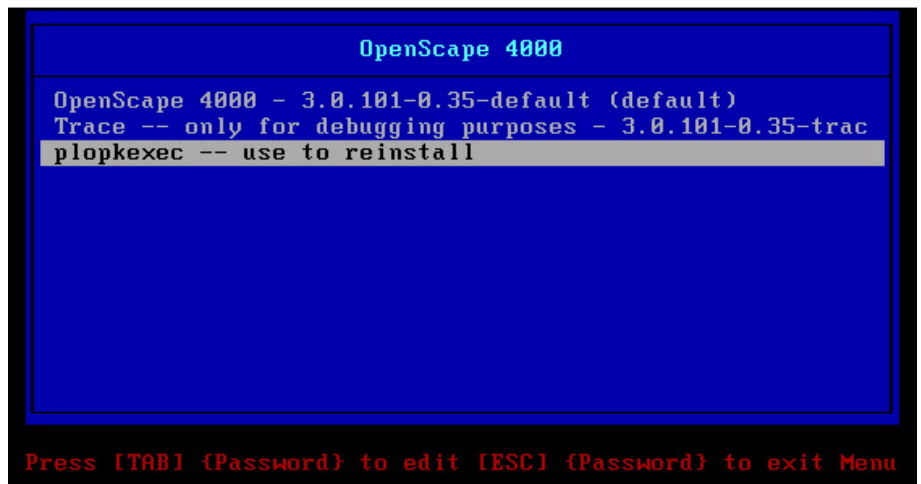


Abbildung 104: Boot-Option für Re-Installation

Warten Sie bis das zuvor verbundene ISO-Image und das Floppy-Image erkannt werden.

- 5) Wählen Sie mit den Cursortasten **sr0: OpenScape 4000 software version Image Installation** (hier **OpenScape 4000 V7 R1.28.0**) und drücken Sie die Eingabetaste.

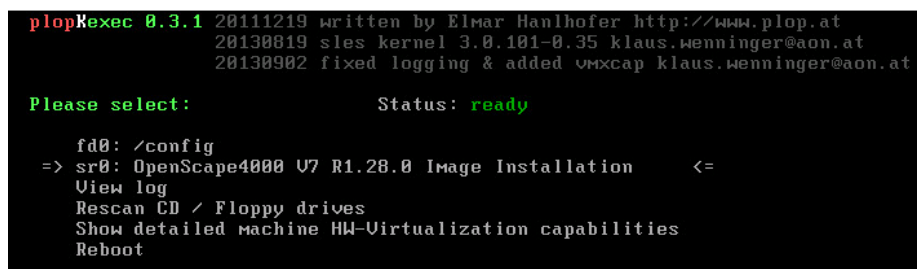


Abbildung 105: Re-Installation starten

4 Migration und Neuinstallation von älteren Systemen

4.1 Vorbereitung

Die Migration soll es dem Benutzer ermöglichen, problemlos von HiPath 4000 V6 und V7 auf OpenScape 4000 V10 hochzurüsten und in einigen wenigen Arbeitsschritten möglichst rasch ein neues System aufzusetzen.

Für den Migrationsvorgang werden folgende Hilfsmittel benötigt:

- USB-Stick
- Putty oder ein anderer SSH-Client
- ComWin

Optionale Hilfsmittel:

- WinSCP für die Übertragung der Dateien zwischen Ihrem lokalen Computer und dem System.
- Festplatte für die Wiederherstellung

Anmerkung: Es wird empfohlen, vor Beginn der Migration eine Wiederherstellungsfestplatte des HiPath 4000 V6 Systems zu erstellen.

Anmerkung: Nach einem Upgrade muss der OpenScape 4000 Assistant Browser-Client wieder auf allen Client-PCs eingerichtet und gegebenenfalls der Applet-Cache geleert werden.

Version/HW	HiPath4000 >= V6 R1.10	HiPath4000 >= V6 R2.x	OS4000 >= V7 R0.x	OS4000 >= V7 R1.x	OS4000 >= V7 R2.x	OS4000 V8 R.x	OS4000 V10 R0
VMware	✓ [1]	✓ [1]	✓ [1]	✓	✓	✓	✓
EcoServer	n/a	n/a	n/a	✓ [2]	✓	✓	✓
Branch	n/a	n/a	n/a	n/a	n/a	✓	✓
DSCXL2	✓	✓	✓	✓	✓	s	s
DSCXL2+	✓	✓	✓	✓	✓	s	s
OSA500	✓	✓	✓	✓	✓	s	s
Server ^[3]	✓	✓	✓	✓	✓	n/r	n/r

✓ = possible

s = supported but not offered generally anymore

n/a = not available

n/r = not released

1. Only Standalone SoftGate

2. Starting V7R1.39

3. The COTS (Commercial off-the-shelf) Server support will be discontinued with SW version V8.

NOTE: RG8350 is not offered anymore with SW version V8.

NOTE: for detailed HW & Deployment supported combination see [V10R0 Deployment Matrix](#)

Abbildung 106: Migration auf OpenScape 4000 V10 R0 - HW-Informationen

Anmerkung: RG8350 wird ab der SW-Version V8 nicht mehr angeboten.

4.2 Vor der Migration des HiPath 4000 V6 Host-Systems

RMX Regen und ein logischer Backup des OpenScape 4000 Assistant müssen durchgeführt werden und offline gespeichert werden.

4.2.1 Sichern der RMX-Datenbasis

Führen Sie einen REGEN durch um die Datenbasis des zu migrierenden Systems zu sichern. Danach konvertieren Sie den RXM Regen mit PC DACON auf die gewünschte neue Version (z.B. OpenScape 4000 V7 R0). Speichern Sie die RMX-Datenbasis offline.

4.2.2 Erstellen eines logischen Backups

Schritt 1: Das logische Backup des OpenScape 4000 Assistant ist am besten für die Migration geeignet und gewährleistet in diesem Fall die volle Funktionstüchtigkeit des Systems nach einer Wiederherstellung.

Anmerkung: Während des Backups der HG3550M (CGW/ NCUI Konfiguration Backup) müssen die Gateways noch mit dem alten System verbunden sein.

Voraussetzungen:

- 1) Um HG3550M korrekt zu sichern, dürfen die Gateways nicht im SECURITY Modus betrieben werden. Dies kann man erreichen, indem man alle Gateways mithilfe des Gateway Dashboards in den MAINTAIN-Modus schaltet, oder global, indem man das Leistungsmerkmal **Enable Gateway Secure Mode** in der Security Mode-Konfiguration deaktiviert.
- 2) Die Loadware aller Gateways muss vor dem Backup auf die neueste Version hochgerüstet werden.
- 3) Stellen Sie sicher, dass in der HG3550M Konfiguration alle Checkboxes aktiviert sind.

Backup & Restore > Administration > Configuration

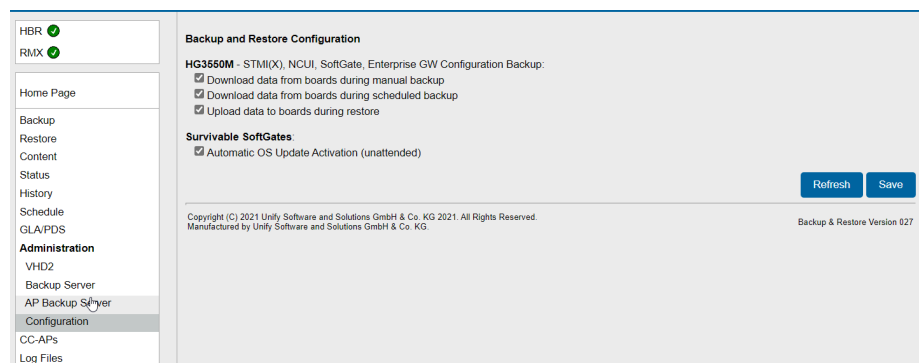


Abbildung 107: Konfiguration der HG 3550M

Führen Sie die folgenden Schritte für den logischen Backup aus:

- 4) Rufen Sie die OpenScape 4000 Assistant-Weboberfläche auf.

- 5) Navigieren Sie zu **Software Management > Backup & Restore (Sicherung und Wiederherstellung) > Backup (Sicherung)**.
- 6) Wählen Sie unter **Archive** (Archiv) die Option **Buffer** (Puffer). Wenn Sie über einen Server verfügen oder der Ansicht sind, dass in Ihrem Fall besser eine Festplatte verwendet werden sollte, können Sie auch diese Optionen verwenden. Im Allgemeinen wird jedoch empfohlen, den **Puffer** als Backup-Medium zu verwenden.
- 7) Wählen Sie unter **Type** (Typ) den Backup-Typ **Logical (export)** (Logisch (Export)) aus.
- 8) Aktivieren Sie im Bereich **Unix Configuration Data** (Unix-Konfigurationsdaten) alle Kontrollkästchen mit Ausnahme von **RMX** und **BEER**.
- 9) Nachdem Sie die oben genannten Einstellungen vorgenommen haben, klicken Sie auf **Start Backup** (Sicherung starten).

The screenshot shows the 'Backup' configuration page. On the left is a sidebar with a menu including 'Startseite', 'Backup', 'Restore', 'Inhalt', 'Status', 'Protokoll', 'Zeitplan', 'GLA/PDS', 'Administration', 'VHD2', 'Backup-Server', 'AP Backup-Server', 'Konfiguration', 'CC-APs', and 'Protokolldateien'. The 'Backup' option is selected. The main content area is titled 'Backup' and has three main sections: 'Archiv:', 'Typ:', and a list of checkboxes for 'Unix-Konfigurationsdaten'. Under 'Archiv:', the 'Festplatte' option is selected. Under 'Typ:', the 'Logisch (Export)' option is selected. The 'Unix-Konfigurationsdaten' section contains a list of checkboxes: RMX (unchecked), ABD (checked), Appctrl (checked), BEER (unchecked), BEER_CSTA (checked), CDB (checked), ComWin (checked), HBR (checked), HBR_MPCID (checked), HG3550M (checked), LAP2 (checked), LOGM (checked), ProclM (checked), SecM (checked), TRACE (checked), and webmin (checked). At the bottom of the page are three buttons: 'Aktualisieren', 'Alle auswählen', and 'Backup starten'.

Schritt 2: Sie werden in einer Meldung von der Webseite darauf hingewiesen, dass der Backup-Vorgang Störungen verursachen kann und einige Funktionen erst nach seinem Abschluss wieder verfügbar sein werden. Bestätigen Sie diese und die nächste eingblendete Meldung. Die zweite Meldung weist darauf hin, dass der Backup-Vorgang gestartet wurde. Klicken Sie in beiden Meldungsfenstern auf **OK**.

Schritt 3: Nachdem Sie auf **OK** geklickt haben, werden Sie auf die Seite **Status** weitergeleitet, auf der die zu sichernden Elemente, ihr Status (Successful, Running oder Waiting) und weitere Informationen angezeigt werden.

Warten Sie, bis alle Elemente den Status **Successful** (Erfolgreich) aufweisen und die Statusanzeige 100 % erreicht hat.

Schritt 4: Vergewissern Sie sich nach Abschluss des Backup-Vorgangs auf der Registerkarte **History** (Verlauf), dass während der Sicherung keine Fehler aufgetreten sind.

Überprüfen des Verlaufs des logischen Backups

Anschließend müssen Sie überprüfen, ob die Backup-Datei erstellt wurde.

Führen Sie folgende Schritte aus, um festzustellen, ob die Datei angelegt wurde:

Stellen Sie eine SSH-Verbindung zum Linux-Hostsystem her (bei Duplex- und Separated Duplex-Systemen muss die Verbindung auf dem [Aktiver/m Knoten](#) hergestellt werden).

Navigieren Sie zu `/var/opt/Assistant/data/BACKUP/IO_BUF_TRANS/OUTPUT/`.

Suchen Sie die Datei `backup_set.[date&time_code].Z`.

4.2.3 Speichern des logischen Backups

Jetzt wird das RMX-Image-Archiv zusammen mit dem mittels OpenScape 4000 Assistant erstellten logischen Backup auf einem USB-Stick gespeichert.

Wichtig: Sie müssen mit dem Mounten eines USB-Sticks unter Linux vertraut sein.

- 1) Verbinden Sie das USB-Speichermedium mit Ihrem System.
- 2) Stellen Sie eine SSH-Verbindung zum Linux-Hostsystem her (bei Duplex- und Separated Duplex-Systemen muss die Verbindung auf dem [Aktiver/m Knoten](#) hergestellt werden).
- 3) Erstellen Sie einen Bereitstellungspunkt.
- 4) Beispiel:

```
# mkdir /mnt/pen
```
- 5) Mounten Sie das USB-Speichergerät.
- 6) Beispiel:

```
# mount /dev/sdc1 /mnt/pen
```
- 7) Kopieren Sie das logische Backup von der Plattform auf den USB-Stick.
- 8) Beispiel:

```
# cp /var/opt/Assistant/data/BACKUP/IO_BUF_TRANS/OUTPUT/backup_set.[datum&zeitcode].Z /mnt/pen/
```

Wichtig: Achten Sie darauf, dass `[datum&zeitcode]` den Zeitpunkt des letzten Backups angibt.

- 9) Unmounten Sie den USB-Stick.
- 10) Beispiel:

```
# umount /dev/sdc1
```
- 11) Entfernen Sie den USB-Stick.

4.2.4 Abschließende Schritte vor dem Schließen des HiPath 4000 V6 Hosts

- Stellen Sie sicher, dass der zuletzt auf dem Host ausgeführte APE Backup auf allen CCAPs wiederhergestellt wurde.

- **OpenScape 4000 Assistant > Software Management > Backup & Restore > Administration > AP Backup Server**

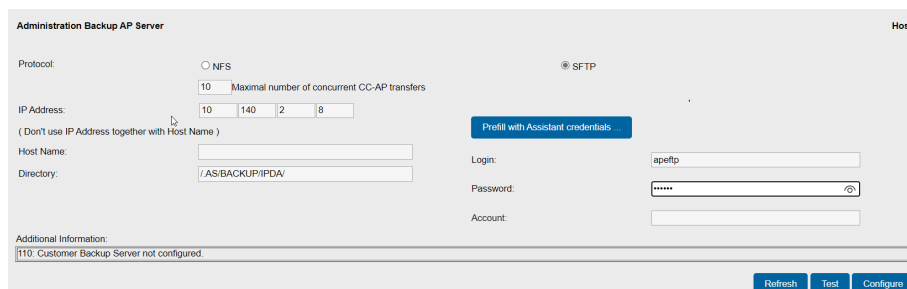


Abbildung 108: Automatische Wiederherstellung auf allen CC-APs deaktivieren

4.3 Migration des OpenScape 4000 Host-Systems

Nachdem Sie die Erstinstallation von OpenScape 4000 abgeschlossen, die OpenScape 4000 Plattform Administration (Portal) auf Ihrem System konfiguriert sowie RMX, OpenScape 4000 Assistant und OpenScape 4000 CSTA gestartet haben, können Sie mit dem Migrationsvorgang beginnen.

Für die Erstinstallation benötigen Sie eine XML-Datei mit den Konfigurationsdaten für Ihr System. Diese XML-Datei kann anhand Ihres "alten" Systems automatisch erstellt werden (siehe [Chapter 12, "Anhang D: Wie Sie eine XML-Datei automatisch erstellen"](#)).

Weitere Informationen zur Erstinstallation finden Sie in [Chapter 2, "Erstinstallation"](#).

4.3.1 Wiederherstellen der RXM-Datenbasis

Stellen Sie die Datenbasis mit Hilfe von GENDB wieder her. Hierfür benötigen Sie die zuvor mit PC DACON erstellte Datei (siehe [Section 4.2.1, "Sichern der RMX-Datenbasis"](#)).

Aktivieren Sie das System: `ACTIVATE-USSU:UNIT=LTG,LTG=1;`

Warten bis alle HG35xx Baugruppen geladen sind (READY in RMX).

`EXEC-UPDAT:MODUL=BP,SUSY=ALL;` ausführen.

4.3.2 Wiederherstellen von OpenScape 4000 Assistant anhand des logischen Backups

Anmerkung: Nach einem Upgrade muss, unabhängig von der alten Version, der OpenScape 4000 Assistant Browser-Client wieder auf allen Client-PCs eingerichtet und gegebenenfalls der Applet-Cache geleert werden.

Schritt 1: Klicken Sie unter **Software Management > Backup & Restore (Sicherung und Wiederherstellung) > Restore (Wiederherstellung)** auf die

Schaltfläche **Browse** (Durchsuchen) und navigieren Sie zum Speicherort Ihres Backup-Satzes. Wählen Sie Ihre Datei **backup_set.[datum&zeitcode].Z** aus und klicken Sie auf **Upload**. Warten Sie, bis der Upload abgeschlossen ist, und fahren Sie dann mit Schritt 2 fort.

Anmerkung: Zur korrekten Wiederherstellung der Komponente HG3550m müssen die Gateways bereits mit dem System in der neuen Version verbunden sein.

Restore

Zur Auflistung von Backup-Sets wählen Sie:

Archiv

☒ Festplatte
 ☐ Puffer
 ☐ Backup-Server
 ☐ Alle

Typ

☐ Daten
 ☐ Logisch
 ☒ Alle

Optionen

☐ Originalliste aus dem Archiv holen

Aktualisieren

Liste

Eine Datei zum Hochladen in den Puffer wählen

Datei auswählen

Keine ausgewählt

Hochladen

Abbildung 109: Wiederherstellen von OpenScape 4000 Assistant

Schritt 2: Warten Sie, bis die Seite geladen ist. Wählen Sie anschließend das Backup aus, das Sie wiederherstellen möchten, indem Sie die entsprechende Optionsschaltfläche aktivieren. Wenn Sie alle Elemente wiederherstellen möchten, aktivieren Sie alle Kontrollkästchen.

Wichtig: Wenn das logische Backup korrekt durchgeführt wurde, werden die Komponenten **RMX** und **BEER** nicht angezeigt (**BEER_CSTA** darf nicht mit **BEER** verwechselt werden). Falls die Komponenten RMX und BEER angezeigt werden, achten Sie darauf, die entsprechenden Kontrollkästchen NICHT zu aktivieren. RMX kann nicht mittels eines logischen Backup/Wiederherstellen-Vorgangs migriert werden, da die Versionen eine unterschiedliche REGEN-Syntax aufweisen.

Klicken Sie auf **Restore Set** (Satz wiederherstellen), um den Wiederherstellungsvorgang zu starten.

Restore

	Unit	Type	Archive	Date/time	System no.	Software	M/A/R/S (manual/automatic/fiso/swa)
<input type="radio"/>	<input type="checkbox"/> UNIX_CFDATA <input type="checkbox"/> BEER <input type="checkbox"/> BEER_CSTA <input type="checkbox"/> HG3550M <input type="checkbox"/> RMX	Data	Hard Disk	2022-03-05 16:36	L31988Q0585X00000	HiPath4000V10 SA01 RL27	A
<input type="radio"/>	<input type="checkbox"/> UNIX_CFDATA <input type="checkbox"/> BEER <input type="checkbox"/> BEER_CSTA <input type="checkbox"/> HG3550M <input type="checkbox"/> RMX	Data	Hard Disk	2022-02-26 16:36	L31988Q0585X00000	HiPath4000V10 SA01 RL27	A

Refresh

Restore Set

Abbildung 110: Auswählen der Backup-Datei und Festlegen der Wiederherstellungsoptionen

Schritt 3: Warten Sie, bis die Wiederherstellung abgeschlossen ist, und starten Sie dann OpenScape 4000 Assistant auf dem neuen System. Navigieren Sie zu diesem Zweck zu **OpenScape 4000 Assistant > Base Administration (Basisadministration) > Webmin** und klicken Sie auf der linken Seite auf den Link **Reboot/Shutdown** (Neustarten/Herunterfahren).

Schritt 4: Starten Sie einen "Alle hochladen"-Vorgang auf dem neuen System. Navigieren Sie zu diesem Zweck zu **OpenScape 4000 Assistant > Configuration Management (Konfigurationsverwaltung) > Network (Netzwerk) > System** und klicken Sie auf **Search** (Suchen). Wenn Sie das System gefunden haben, wählen Sie den Menüpunkt **Action (Aktion) > Upload (Hochladen)**.

Schritt 5: Das neue System läuft nun mit einer Übergangslizenz. Importieren Sie die offiziellen Lizenzdateien für OpenScope 4000 über das Lizenzmanagement des OpenScope 4000 Assistant.

1) Lizenzverwaltung > Browse... > Lizenzdatei auswählen > Senden

Wichtig: In Mehrknoten-Bereitstellungen sollten die Lizenzen sowohl für den aktiven als auch für den Standby-Knoten importiert werden!

OpenScope 4000 System		SLES-Upgrade-Schutz		
Lizenz-Version	V10 (ID:13494248)	Lizenziert	Verwendeter Wert	Gültigkeit
Advanced Locking ID(sys7)	+NWDNQY43UDM4.V:*RVFNFL	20	2	bis 31.12.2022
Verwendete Netzwerk-Management-Ports 14		Lizenzdetails zum SLES-Upgrade-Schutz		
		OpenScope 4000 Host system		1
		CC-AP für AP Emergency (nur IPDA)		0
		Softgate (einschließlich OpenScope Access)		1
		STMIX Baugruppen		0
		OpenScope Enterprise Gateway		0

OpenScope 4000 RMX		Lizenziert	Verwendeter Wert	Gültigkeit
Anlagennummer		L31988Q0695X	L31988Q0695X00000	
Support-Vertrag				199 Tage
Flex	4000		11 (counted at : Wed Jun 15 05:30:23 2022)	199 Tage
TDM (Analog, Up0E, ISDN, Cordless, PSM, PSE anlagen)	4000		3 (counted at : Wed Jun 15 05:30:23 2022)	199 Tage
OpenScope Mobile	10		0	199 Tage
Unify_Phone	10		0	199 Tage
Duplex	Ja		Ja	199 Tage

Abbildung 111: OpenScape 4000 Assistant - Installation der Lizenzdatei über das Lizenzmanagement

Nach ca. 15 bis 20 Minuten wird eine automatische CODEW-Generierung gestartet. Anschließend können Sie die Gültigkeit wie zuvor beschrieben überprüfen.

Schritt 6: Falls in der vorherigen Version Web-Zertifikate für OpenScape 4000 Assistant installiert waren, werden diese in der neuen Version wiederhergestellt. Das entsprechende Zertifikat muss jedoch wieder manuell aktiviert werden. Diese Zertifikate können nicht automatisch aktiviert werden, weil für den Eintrag des Passworts in das Zertifikat Angaben des Technikers erforderlich sind.

4.3.3 Konfiguration des OpenScape 4000 SoftGate bei aktivierter Signalisierungs- und Payload-Verschlüsselung

Wenn in HiPath 4000 V6/V7 die Signalisierungs- und Payload-Verschlüsselung aktiviert war und das OpenScape 4000 SoftGate vom OpenScape 4000 Installationsmedium neu installiert wurde, muss der Master Encryption Key (MEK) in der OpenScape 4000 Plattform Administration (Portal) manuell hinzugefügt werden:

System > LAN Configuration (LAN-Konfiguration) > SoftGate > unter SoftGate Master Encryption Key (MEK) Management > Master Encryption Key (MEK)

Anmerkung: Wenn bei einem Standalone OpenScape 4000 SoftGate die IP-Adresse der OpenScape 4000 Plattform Administration (Portal) in der XML-Datei nicht konfiguriert ist, ist die OpenScape 4000 Plattform Administration (Portal) unter der NCUI IP-Adresse und Port 8443 erreichbar (z. B. https://NCUI_IP:8443).

Anmerkung: Allgemeine Informationen zur Konfiguration des OpenScape 4000 SoftGate finden Sie in [Section 2.3, "Manuelle Konfiguration des OpenScape 4000 SoftGate"](#).

Anmerkung: Nach der Migration sollte die Security Checkliste angewendet werden.

4.4 Reinstallation/Aktualisierung der Remote-Appliance (RAR)

4.4.1 Wichtige Hinweise

- RAR unterstützt Appliance-Versionen ab HiPath 4000 V6 R1.10.0.
- Die Voraussetzung für RAR ist, dass der zentrale Host bereits auf die Zielversion bzw. das Zielrelease aufgerüstet wurde.
- RAR darf nicht vom APE, Quorum, Standalone oder Survivable OpenScape 4000 SoftGate gestartet werden.
- Mit der RAR-Funktion können folgende Remote-Appliances über den Host aktualisiert werden:
 - APE DSCXL2-Baugruppe in CC-AP
 - Standalone OpenScape 4000 SoftGate, OpenScape Access 500 oder OpenScape 4000 Branch
 - Survivable OpenScape 4000 SoftGate, OpenScape Access 500 oder OpenScape 4000 Branch
 - Enterprise Gateway
 - Survivable Enterprise Gateway
 - Für Geräte, die als Standalone OpenScape 4000 SoftGate konfiguriert sind, überträgt und installiert RAR dieselbe Softwareversion wie auf

dem Host (einschließlich des letzten Plattform-HotFix). For appliances configured as APE or Survivable OpenScape 4000 SoftGate the upgrade to the last Platform HotFix applied the Host should be done over the APE Backup and Restore Feature after RAR has completed.

- Das Hostsystem muss mit der Zielversion der Software betrieben werden (z. B. V7R1.39).
- RAR verwendet das SSH- und das SFTP-Protokoll. RAR funktioniert nur, wenn das Host-System (Client) auf den TCP-Port 22 der Remote-Appliance (Server) zugreifen kann.
- Das Terminal oder die Service PC - Host System Verbindung kann geschlossen werden. Der RAR Prozess läuft trotzdem im Hintergrund weiter.
- Zwischen dem Host und der Remote-Appliance werden etwa 3 GB übertragen. Bei Deployment "Stand Alone OpenScape 4000 SoftGate" werden nur 1,5 GB übertragen.
- LINUX Root-Passwörter der Remote-Appliances sind erforderlich.
- Alle Remote-Appliances (Plattform & RMX) müssen die gleiche Software-Version haben wie das Host-System. Wenn die Remote Appliances eine andere Software-Version als das Host-System haben, dann müssen sie mit RAR reinstalliert werden oder (anders gesagt) wenn die Software-Versionen vor dem nächsten RLC-Upgrade synchronisiert werden, dann vermeidet man spätere Upgrade-Probleme.
- Ab OpenScape 4000 V7 R1.39 ist es möglich, den Zeitpunkt des Neustarts bei der Aktivierung zu planen (z. B. Samstag 03:00) und die von RAR für die Transferaktivitäten verwendete Bandbreite zu begrenzen.
- Auf dem Host-System eingerichtete Plattform HotFix-Upgrades werden von RAR nicht an Ziele übertragen, die als AP Emergency- oder Survivable SoftGate-Bereitstellung konfiguriert sind. Zum Aktivieren des letzten Plattform HotFix auf solchen RAR-Zielen muss nach Abschluss des RAR-Vorgangs APE Restore verwendet werden.
- Bei Versionen vor OpenScape 4000 V7 R2 muss, wenn das Host-System von einem ISO/USB-Stick installiert wurde, auf dem ein Plattform HotFix enthalten war, dieses HotFix ein weiteres Mal per Assistant Software Transfer aufgerüstet und anschließend ein APE-Backup durchgeführt werden, sodass das HotFix über APE Restore auf RAR-Zielen repliziert werden kann, die als AP Emergency- oder Survivable SoftGate-Bereitstellungen konfiguriert sind.

Wichtig: In diesem Dokument wird die Aktualisierung von HiPath 4000 V6 R2.15 auf OpenScape 4000 V7 R1 beschrieben. Diese Beschreibung gilt jedoch ebenso für das Upgrade von HiPath 4000 V6 R1.12 auf OpenScape 4000 V7 R1.

4.4.2 Reinstallieren/Aktualisieren der Remote-Appliance (RAR)

Die Reinstallation/Aktualisierung der Remote-Appliance (RAR) geschieht in 4 Arbeitsschritten:

- [Teil 1: Vorbereitung der Remote Appliance.](#)

Zur Vorbereitung der Remote-Appliance muss beispielsweise APE deaktiviert und das Passwort geprüft werden. Dieser Schritt kann vor

der Aufrüstung/Reinstallation/Installation des zentralen Hosts ausgeführt werden.

- [Teil 2: Vorbereitung des zentralen Hosts](#)

Zur Vorbereitung des zentralen Hosts muss HBR konfiguriert werden. Dieser Schritt kann nur **nach** der Aufrüstung/Reinstallation/Installation des zentralen Hosts ausgeführt werden.

- [Teil 3: Start des eigentlichen RAR-Vorgangs per Skript im Terminalfenster](#)
- [Teil 4: Manuelle Überprüfung der reinstallierten Appliance über RAR](#) (nach erfolgreicher Ausführung auf dem Host).

4.4.2.1 Teil 1: Vorbereitung der Remote Appliance.

Vor Beginn der Aktualisierung auf dem zentralen Host sollte die automatische Wiederherstellung auf allen CC-APs deaktiviert werden:

OpenScape 4000 Assistant > Software Management > Backup & Restore > Administration > AP Backup Server

The screenshot shows the 'Administration Backup AP Server' configuration window. It includes fields for Protocol (NFS or SFTP), IP Address (with a sub-field for 'Maximal number of concurrent CC-AP transfers' set to 10), Host Name, Directory (set to /AS/BACKUP/), Login (set to apeftp), Password (masked with asterisks), and Account. A button 'Profile with Assistant credentials...' is visible. At the bottom, a message box displays '[110: Customer Backup Server not configured.]' and there are 'Refresh', 'Test', and 'Configure' buttons.

Abbildung 112: Automatische Wiederherstellung auf allen CC-APs deaktivieren

Passwortprüfung über SSH:

Da RAR das Root-Passwort auf der Remote-Appliance nicht ändern kann, sollte manuell geprüft werden, ob das Passwort in den einzelnen Remote-Appliances geändert wurde (bei der ersten Anmeldung als Root-Benutzer müssen Sie das Passwort ändern).

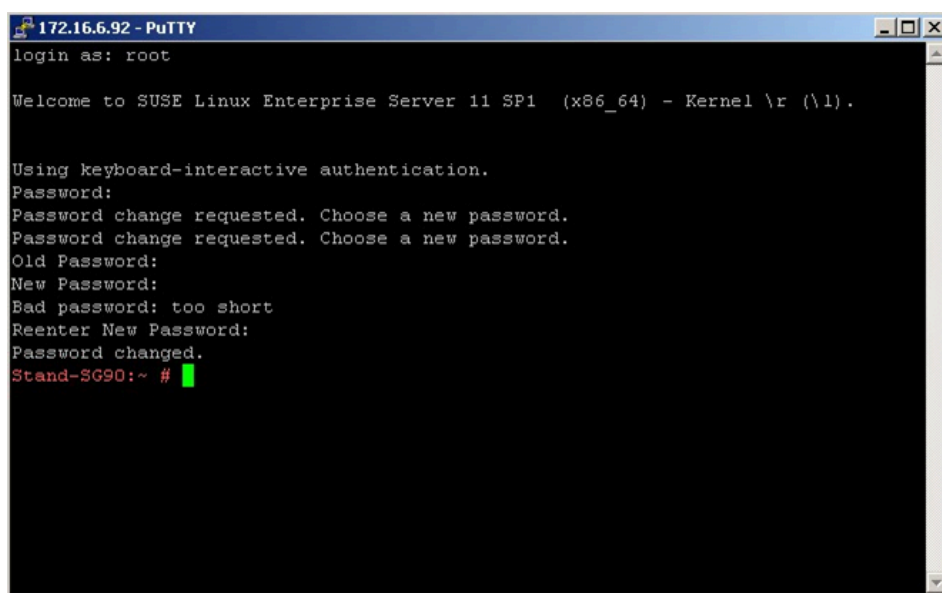


Abbildung 113: Passwortprüfung über SSH

4.4.2.2 Teil 2: Vorbereitung des zentralen Hosts

Das Host-Installation/-Upgrade-Verfahren wird hier nicht beschrieben.

Nach Abschluss der Installation auf dem Host sollte der AP Backup Server konfiguriert oder mittels eines logischen HBR-Restore wiederhergestellt werden.

OpenScape 4000 Assistant > Software Management > Backup & Restore > Administration > AP Backup Server

A screenshot of the 'Administration Backup AP Server' configuration window. The window has a title bar 'Administration Backup AP Server' and a 'Host' button in the top right. It contains several fields: 'Protocol' with radio buttons for 'NFS' and 'SFTP' (selected); 'Maximal number of concurrent CC-AP transfers' with a value of '10'; 'IP Address' with four input boxes containing '172', '16', '6', and '12'; a note '(Don't use IP Address together with Host Name)'; 'Host Name' with an empty text box; 'Directory' with the value '/AS/BACKUP/IPDA'; 'Login' with the value 'engr'; 'Password' with a masked field '*****'; and 'Account' with an empty text box. At the bottom, there is an 'Additional Information' section with a text area and three buttons: 'Refresh', 'Test', and 'Configure'. A large red arrow points down towards the 'Configure' button.

Abbildung 114: AP Backup Server konfigurieren/wiederherstellen

Starten Sie AP Backup auf dem Host, um sicherzustellen, dass auf dem AP Backup Server ein frischer APE Backup-Satz vorhanden ist.

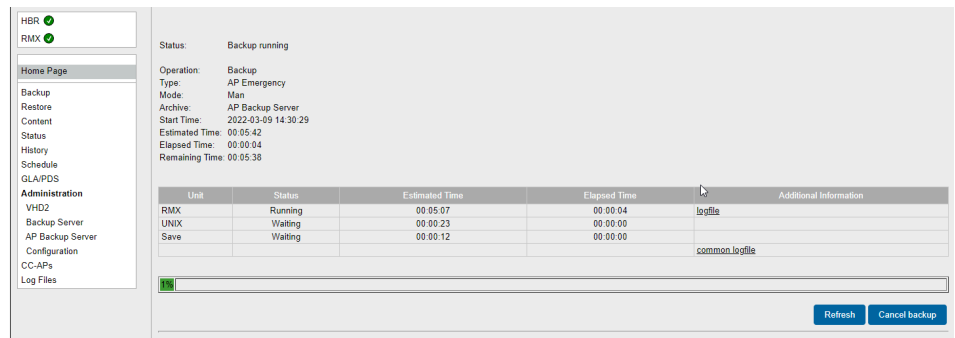


Abbildung 115: APE Backup-Satz erstellen

4.4.2.3 Teil 3: Start des eigentlichen RAR-Vorgangs per Skript im Terminalfenster

Bei einer Duplex-Bereitstellung wird dringend empfohlen, RAR auf dem Standby-Knoten zu starten.

Das RAR-Skript wird mit den folgenden Parametern gestartet:

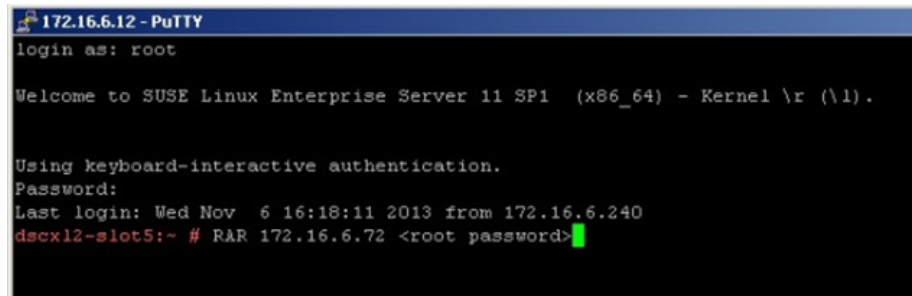
- physikalische IP-Adresse (YAST) der Remote-Appliance (Survivable OpenScape 4000 SoftGate, Standalone OpenScape 4000 SoftGate, APE)
- Root-Passwort der Remote-Appliance
- Geplanter Aktivierungszeitpunkt
- Verwenden Sie den optionalen Parameter **no_version_check**, um RAR zu zwingen, die Installation auf Appliances, die bereits dieselbe Fix-Release-Softwareversion wie der Host verwenden, zu überschreiben. Verwenden Sie diese Vorgehensweise bei Appliances, die als Standalone OpenScape 4000 SoftGate konfiguriert sind, um den aktuellen Plattform-Hotfix zu übertragen und auf ihnen zu installieren.
- Standardmäßig installiert RAR auf den SoftGate-Zielen (Standalone oder Survivable) die LW von der RMX-Festplatte des Hosts, von der aus RAR gestartet wurde (:A1H1E:APSP/LTG/LGA0/PZKSGW50).
- Der optionale Parameter **keep_sg_version** dient dazu, RAR zu zwingen, die bereits auf dem Ziel laufende SoftGate-Version beizubehalten. Dies ist jedoch nur möglich, wenn das SoftGate mindestens einmal mit einer offiziellen oder privaten SG LW aktualisiert wurde. Wenn noch keine solche Aktualisierung stattgefunden hat, ist diese Option wirkungslos und die RMX HDD-Version wird installiert.

Anmerkung: Rufen Sie den RAR-Befehl ohne Parameter auf, um alle möglichen Parameter-Befehle und -Optionen anzuzeigen. Informationen zu allen Optionen finden Sie in der Onlinehilfe zu RAR oder im [Section 4.4.3, "RAR Hilfe"](#).

Schritte zum Starten von RAR vom Host aus:

- Melden Sie sich als Root bei einer SSH-Sitzung auf dem Host an.

- RAR 172.16.6.72 Root-Passwort scheduled=Datum_und_Zeit



```
172.16.6.12 - PuTTY
login as: root

Welcome to SUSE Linux Enterprise Server 11 SP1 (x86_64) - Kernel \r (\l).

Using keyboard-interactive authentication.
Password:
Last login: Wed Nov  6 16:18:11 2013 from 172.16.6.240
dscx12-slot5:~ # RAR 172.16.6.72 <root password>
```

Abbildung 116: RAR auf dem Host starten

Hinweise zum Passwort

- Wenn das Passwort Sonderzeichen (alles außer Buchstaben und Ziffern) enthält, dann muss das Passwort zwischen einfachen Hochkomma stehen.
RAR 172.16.6.72 'abc\$efg' scheduled=2015.02.18-02:00
- Wenn das Passwort der Appliance das Zeichen ' (einfaches Anführungszeichen) enthält, muss es vor dem Starten von RAR geändert werden. RAR funktioniert nicht, wenn das Appliance-Passwort das Zeichen ' (einfaches Anführungszeichen) enthält.

Notes regarding scheduled activation

The RAR process consists of the following phases:

- transfer,
- background installation,
- waiting for scheduled activation,
- activation

These phases correspond to the RAR statuses as displayed by the RAR status command described further below: [TRANSFER-RUNNING], [REINSTALL-RUNNING], [SCHEDULED-ACTIVATION-PENDING], [ACTIVATION-STARTED]

During the transfer phase, the OpenScape 4000 software is being transferred from the host to the appliance over SFTP. This can take a variable amount of time depending on the bandwidth available between the two machines.

All other phases are running then on the remote appliance independently and the amount of time needed depends on the hardware performance of the appliance machine.

The activation of the new software on the remote appliance machine can take place only once the background installation phase has completed.

In order to control the activation time which implies a reboot and thus telephony services downtime, the parameter scheduled activation time should be used. The remote appliance will wait for the scheduled activation time and only then do the activation.

If for some reason the scheduled activation time is reached and the necessary prerequisites are not fulfilled, then RAR will stop with corresponding error message and the RAR process needs to be started again.

If an unexpected reboot or power failure occurs during the waiting for scheduled activation, then the activation of the new software will happen immediately after the appliance is again started. This will spare an extra downtime later since a

recent downtime has already occurred. However, if for some reason this is not wanted, then the option "no_activation_on_reboot" can be used to prevent this behavior. For e.g.:

```
RAR 172.16.6.72 'abc$efg' scheduled=2015.02.18-02:00
no_activation_on_reboot
```

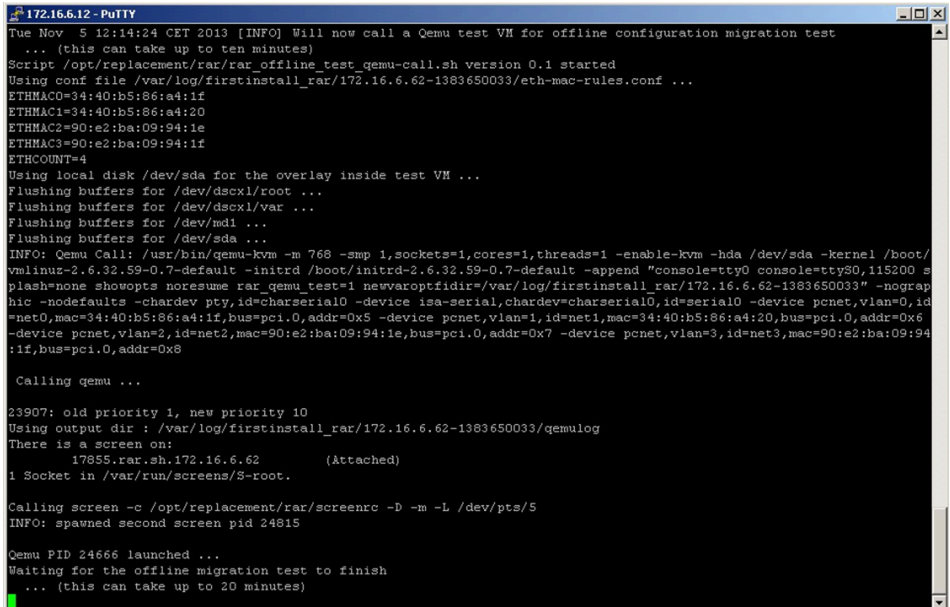
In the case that the "no_activation_on_reboot" option is specified and an unexpected reboot occurs, then the RAR process will resume waiting for the scheduled activation time and will carry on with the steps as described above.

Anmerkung: If option "no_activation_on_reboot" is not specified and RAR has already reached the waiting for scheduled activation phase, the activation can be triggered by the user at any time before the scheduled activation time by just issuing a Linux reboot on the appliance.

The scheduled activation time is expressed in the time zone of the Host. If different time zones are configured for the host and for the appliance, the user must calculate the corresponding time difference in order to plan the scheduled activation time correctly.

E.g. host is on GMT+1 and appliance is on GMT+2. Then in order to plan the scheduled activation on the appliance to be done on 24 February 2014 at 2:00 AM local time on the appliance, the scheduled activation time to be passed to the RAR command must be 2015.02.24-01:00.

Während der Skriptausführung werden im Terminalfenster die Ausgaben angezeigt.



```
172.16.6.12 - PuTTY
Tue Nov  5 12:14:24 CET 2013 [INFO] Will now call a Qemu test VM for offline configuration migration test
... (this can take up to ten minutes)
Script /opt/replacement/rar/rar_offline_test qemu-call.sh version 0.1 started
Using conf file /var/log/firstinstall_rar/172.16.6.62-1383650033/eth-mac-rules.conf ...
ETHMAC0=34:40:b5:86:a4:1f
ETHMAC1=34:40:b5:86:a4:20
ETHMAC2=90:e2:ba:09:94:1e
ETHMAC3=90:e2:ba:09:94:1f
ETHCOUNT=4
Using local disk /dev/sda for the overlay inside test VM ...
Flushing buffers for /dev/dscxl/root ...
Flushing buffers for /dev/dscxl/var ...
Flushing buffers for /dev/nd1 ...
Flushing buffers for /dev/sda ...
INFO: Qemu Call: /usr/bin/qemu-kvm -m 768 -smp 1,sockets=1,cores=1,threads=1 -enable-kvm -hda /dev/sda -kernel /boot/
vmlinuz-2.6.32.59-0.7-default -initrd /boot/initrd-2.6.32.59-0.7-default -append "console=tty0 console=ttyS0,115200 s
plash=none showopts noresume rar qemu_test=1 newvaroptfidir=/var/log/firstinstall_rar/172.16.6.62-1383650033" -nograph
hic -nodefaults -chardev pty,id=charserial0 -device isa-serial,chardev=charserial0,id=serial0 -device pcnet,vlan=0,id
=net0,mac=34:40:b5:86:a4:1f,bus=pci.0,addr=0x5 -device pcnet,vlan=1,id=net1,mac=34:40:b5:86:a4:20,bus=pci.0,addr=0x6
-device pcnet,vlan=2,id=net2,mac=90:e2:ba:09:94:1e,bus=pci.0,addr=0x7 -device pcnet,vlan=3,id=net3,mac=90:e2:ba:09:94
:1f,bus=pci.0,addr=0x8
Calling qemu ...
23907: old priority 1, new priority 10
Using output dir : /var/log/firstinstall_rar/172.16.6.62-1383650033/qemulog
There is a screen on:
17855.rar.sh.172.16.6.62 (Attached)
1 Socket in /var/run/screens/S-root.
Calling screen -c /opt/replacement/rar/screenrc -D -m -L /dev/pts/5
INFO: spawned second screen pid 24815
Qemu PID 24666 launched ...
Waiting for the offline migration test to finish
... (this can take up to 20 minutes)
```

Abbildung 117: Ausgaben während des RAR-Vorgangs

The RAR script on the Host will stop after the transfer to the appliance has completed and the background installation activities are initiated. To continue getting live information from the appliance the monitor command can be used:

RAR monitor 172.16.6.72

It is possible to start RAR activities with scheduled activation time for multiple RAR appliances at the same time. In order not to use too many resources on the Host, a maximum number of 5 RAR sessions are allowed to perform transfer activities at the same time. Any RAR session started when this number has already been reached will wait until one of the other running RAR instances finishes the transfer. The RAR appliance status for this case is [WAITING-TO-TRANSFER].

For narrow bandwidth connections between host and appliance the parameter "bandwidth" can be used when starting RAR. For e.g.:

```
RAR 172.16.6.72 'abc'\efg' scheduled=2015.02.18-02:00 bandwidth=1000
```

The bandwidth parameter is expressed in Kilobits per second and must be an integer number.

Cancelling RAR process

If for some reason the user decides to interrupt the RAR process for an appliance then this can be done with the cancel command:

```
RAR cancel 172.16.6.72
```

This will initiate the cancellation and the RAR process will be stopped in a nice and safe way during the next minutes. More details can be checked live with the monitor command.

A RAR process cannot be cancelled if the activation has already begun on the remote appliance.

Mögliche RAR Statussequenzen

Mögliche RAR-Statussequenzen bei Survivable OpenScape 4000 SoftGate und CC-AP:

```
172.16.6.72 active [STARTING] @ Tue Nov 5 14:54:06 CET 2013
```

```
172.16.6.72 active [DATA-COLLECT-PENDING] @ Tue Nov 5 14:54:08 CET 2013
```

```
172.16.6.72 active [DATA-COLLECT] @ Tue Nov 5 14:57:06 CET 2013
```

```
172.16.6.72 active [WAITING-TO-TRANSFER] @ Tue Nov 5 14:58:00 CET 2013
```

```
172.16.6.72 active [TRANSFER-RUNNING] @ Tue Nov 5 14:58:06 CET 2013
```

```
172.16.6.72 active [STARTING-REINSTALL] @ Tue Nov 5 15:03:05 CET 2013
```

```
172.16.6.72 active [REINSTALL-RUNNING] @ Tue Nov 5 15:07:58 CET 2013
```

```
172.16.6.72 active [SCHEDULED-ACTIVATION-PENDING] @ Tue Nov 5 15:29:41 CET 2013
```

```
172.16.6.72 active [ACTIVATION-STARTED] @ Tue Nov 5 15:32:33 CET 2013
```

```
172.16.6.72 active [HEALTH-CHECK] @ Tue Nov 5 15:48:10 CET 2013
```

```
172.16.6.72 active [VERSION-CHECK] @ Tue Nov 5 15:49:11 CET 2013
```

```
172.16.6.72 active [ASSISTANT-INSTALLATION] @ Tue Nov 5 15:49:16 CET 2013
```

```
172.16.6.72 active [APE-HBR-CONFIG-RESTORE] @ Tue Nov 5 16:10:37 CET 2013
```

172.16.6.72 active [APE-RESTORE-RUNNING] @ Tue Nov 5 16:12:12 CET 2013

172.16.6.72 done [SUCCESS] @ Tue Nov 5 16:12:13 CET 2013

oder im Falle von fehlgeschlagenem RAR:

13. 172.16.6.72 done [ERROR] @ Tue Nov 5 16:12:13 CET 2013

Mögliche RAR-Statussequenzen bei Standalone OpenScape 4000 SoftGate:

172.16.6.82 active [STARTING] @ Tue Nov 5 14:40:28 CET 2013

172.16.6.82 active [DATA-COLLECT-PENDING] @ Tue Nov 5 14:40:30 CET 2013

172.16.6.82 active [DATA-COLLECT] @ Tue Nov 5 14:46:43 CET 2013

172.16.6.82 active [WAITING-TO-TRANSFER] @ Tue Nov 5 14:47:40 CET 2013

172.16.6.82 active [TRANSFER-RUNNING] @ Tue Nov 5 14:47:43 CET 2013

172.16.6.82 active [STARTING-REINSTALL] @ Tue Nov 5 14:52:05 CET 2013

172.16.6.82 active [REINSTALL-RUNNING] @ Tue Nov 5 14:52:37 CET 2013

172.16.6.72 active [SCHEDULED-ACTIVATION-PENDING] @ Tue Nov 5 14:58:40 CET 2013

172.16.6.82 active [ACTIVATION-STARTED] @ Tue Nov 5 15:00:52 CET 2013

172.16.6.82 active [HEALTH-CHECK] @ Tue Nov 5 15:06:42 CET 2013

172.16.6.82 active [VERSION-CHECK] @ Tue Nov 5 15:07:14 CET 2013

172.16.6.82 done [SUCCESS] @ Tue Nov 5 15:07:22 CET 2013

oder im Falle von fehlgeschlagenem RAR:

10. 172.16.6.82 done [ERROR] @ Tue Nov 5 15:07:22 CET 2013

Der RAR-Status kann in einer anderen SSH-Sitzung bzw. in einem anderen SSH-Fenster mit dem Kommando `RAR status` überprüft werden.

```

172.16.6.12 - PuTTY
dscx12-slot5:~ # RAR status
Remote Appliance Reinstall
-----
172.16.6.21 .... done [SUCCESS] @Tue Nov 5 16:29:21 CET 2013
172.16.6.62 .... done [SUCCESS] @Tue Nov 5 17:27:49 CET 2013
172.16.6.72 .... done [SUCCESS] @Tue Nov 5 16:12:13 CET 2013
172.16.6.72 active [REINSTALL-RUNNING] @Wed Nov 6 18:11:31 CET 2013
172.16.6.82 .... done [SUCCESS] @Tue Nov 5 15:04:11 CET 2013
172.16.6.82 .... done [SUCCESS] @Wed Nov 6 18:10:37 CET 2013
172.16.6.92 .... done [SUCCESS] @Tue Nov 5 15:07:22 CET 2013
172.16.6.92 .... done [SUCCESS] @Wed Nov 6 18:13:53 CET 2013
dscx12-slot5:~ #

```

Abbildung 118: RAR-Status

Die erfolgreiche Ausführung eines RAR-Skripts endet mit:

Tue Nov 5 16:12:13 CET 2013 [PASSED] **Remote Appliance Reinstallation finished OK.**

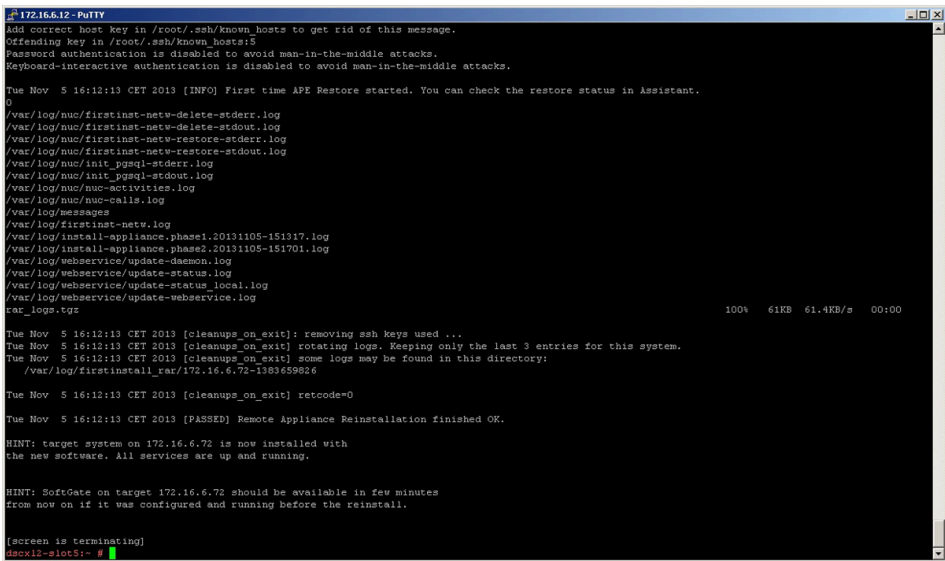


Abbildung 119: RAR erfolgreich abgeschlossen

4.4.2.4 Teil 4: Manuelle Überprüfung der reinstallierten Appliance über RAR

- auf der reinstallierten Appliance **OpenScope 4000 Plattform Administration (Portal)**

Status	LAN	Software	Hardware
Hostname	eTarzan-A	eTarzan-B	eTarzan-Q
BIOS			
Vendor	American Megatrends Inc.	American Megatrends Inc.	American Megatrends Inc.
Version	2.2.000	2.2.000	2.2.000
Date	01/20/2015	01/20/2015	10/07/202006
Linux			
Distribution	SUSE Linux Enterprise Server 15 SP3	SUSE Linux Enterprise Server 15 SP3	SUSE Linux Enterprise Server 15 SP3
Kernel Version	5.3.18-150300.59-48-default	5.3.18-150300.59-48-default	5.3.18-150300.59-48-default
Platform			
Current Version	V10_R1.27.0	V10_R1.27.0	V10_R1.27.0
Linux Update			
Update Status	-	-	-
RTMX			
FPDIA Firmware	HICCOv.R.0133.190522.1301	HICCOv.R.0133.190522.1301	N/A
Loadware	ccertm0.os.a0.048 (SVN 2824)	ccertm0.os.a0.048 (SVN 2824)	N/A

Abbildung 120: Software-Version in Plattform Administration (Portal) prüfen

- Survivable OpenScope 4000 SoftGate (auf OpenScope Access 500) oder APE DSCXL2-Baugruppe/APE EcoServer
- Wenn es sich bei der reinstallierten Appliance um ein Survivable OpenScope 4000 SoftGate (auf OpenScope Access 500) oder um eine APE DSCXL2-Baugruppe handelt, wird der erste APE Restore-Vorgang ungeachtet der Einstellung des Deaktivierungs-Flags auf der Konfigurationswebseite des AP Backup Servers automatisch ausgeführt. Der Restore-Status kann im OpenScope 4000 Assistant von APE wie gewohnt überprüft werden:
- Die CC-AP (oder Survivable OpenScope 4000 SoftGate)-Appliance ist jetzt reinstalliert und betriebsbereit. Um weitere automatische APE-Wiederherstellungen zu ermöglichen, achten Sie darauf, dass das Kontrollkästchen **Automatic restore disabled** (Automatische

Wiederherstellung deaktiviert) in der Konfiguration des AP Backup Servers nicht aktiviert ist.

OpenScape 4000 Assistant > Software Management > Backup & Restore > Administration AP Backup Server

Administration Backup AP Server Host

Protocol: ☐ NFS ☒ SFTP

10 Maximal number of concurrent CC-AP transfers

IP Address: 172 16 6 12

(Don't use IP Address together with Host Name)

Host Name:

Directory: /AS/BACKUP/IPDA

Login: engr

Password:

Account:

Additional Information:

Refresh Test Configure

Abbildung 121: Automatische APE-Wiederherstellung zulassen

- Standalone OpenScape 4000 SoftGate (auf OpenScape Access 500)

Wenn es sich bei der reinstallierten Appliance um ein Standalone OpenScape 4000 SoftGate (auf OpenScape Access 500) handelt, wird

der OpenScape 4000 Assistant nicht installiert und AP Restore wird nicht gestartet.

```
172.16.6.12 - PuTTY
Tue Nov 5 15:03:04 CET 2013 [INFO] No answer from remote side
Tue Nov 5 15:04:06 CET 2013 [INFO] New Software is active and running on remote side
Tue Nov 5 15:04:06 CET 2013 [INFO] Checkydata on remote side is now :
V7_R0.11.0
Component hp4k-assistant-image is not installed
Component hp4k-base-image is not installed
Component hp4k-cdp_inside-image is not installed
Version Check OK
0
/var/log/nuc/firstinst-netw-delete-stderr.log
/var/log/nuc/firstinst-netw-delete-stdout.log
/var/log/nuc/firstinst-netw-restore-stderr.log
/var/log/nuc/firstinst-netw-restore-stdout.log
/var/log/nuc/nuc-activities.log
/var/log/nuc/nuc-calls.log
/var/log/messages
/var/log/firstinst-netw.log
/var/log/install-appliance:phase1.20131105-145259.log
/var/log/install-appliance:phase2.20131105-145259.log
/var/log/webservice/update-daemon.log
/var/log/webservice/update-status_local.log
/var/log/webservice/update-webservice.log
rst_logs.tmp 100% 13KB 13.1KB/s 00:00
Tue Nov 5 15:04:11 CET 2013 [cleanup_on_exit]: removing ssh keys used ...
Tue Nov 5 15:04:11 CET 2013 [cleanup_on_exit]: rotating logs. Keeping only the last 3 entries for this system.
/var/log/firstinstall_rar/172.16.6.82-1303658803
Tue Nov 5 15:04:11 CET 2013 [cleanup_on_exit] retcode=0
Tue Nov 5 15:04:11 CET 2013 [PASSED] Remote Appliance Reinstallation finished OK.
HINT: SoftGate on target 172.16.6.82 should be available in few minutes
from now on if it was configured and running before the reinstall.
[screen is terminating]
dscxl2-slot5:- #
```

Abbildung 122: RAR auf einem Standalone OpenScape 4000 SoftGate erfolgreich abgeschlossen

Der Status des OpenScape 4000 SoftGate kann in der SSH-Sitzung auf dem OpenScape 4000 SoftGate Linux-Rechner manuell geprüft werden:

```
172.16.6.82 - PuTTY
login as: root
Welcome to SUSE Linux Enterprise Server 11 SP1 (x86_64) - Kernel \r (\l).
Using keyboard-interactive authentication.
Password:
Hpa500-SASG80:~ # date ; service socod status
Tue Nov 5 15:07:21 CET 2013
2013-11-05 15:07:21 Checking for service SOCO
Hpa500-SASG80:~ # running
```

Abbildung 123: Status des OpenScape 4000 SoftGate prüfen

Der Plattform-Status kann im OpenScape 4000 SoftGate mit dem Linux-Befehl `checkydata` geprüft werden. Hierbei sollte eine ähnliche Version wie die des Hosts angezeigt werden.

Ausnahme: Wenn der Host über RLC aktualisiert und anschließend RAR ausgeführt wird, wird die Appliance mit der Basisversion des Hosts installiert.

Beispiel: Der Host wurde mit OpenScape 4000 V7 R0.12.0 installiert und das Standalone OpenScape 4000 SoftGate unter HiPath 4000 V6 wurde vergessen oder ist nicht erreichbar.

Anschließend wurde der Host auf OpenScape 4000 V7 R0.13.0 aktualisiert. Wenn das HiPath 4000 V6 Standalone HiPath 4000 SoftGate nun wieder erreichbar wird, kann es mit RAR reinstalliert werden, allerdings nur mit der Basisversion OpenScape 4000 V7 R0.12.0.

4.4.3 RAR Hilfe

```
dscxl2-slot5:~ # RAR
```

```
Remote Appliance Reinstall 6.1
```

```
-----
```

Usage:

RAR IP_Address root_password [option1 option2 ...]

- start RAR on given target system including automatic APE restore launching at the end of RAR. Please read carefully the RAR documentation in case the password contains special characters like \$
- possible options are (space separated) :

no_version_check - forces RAR to perform the reinstall without checking target SW version

no_ape_restore - start RAR on given target system WITHOUT automatic APE restore launching at the end of RAR. User must do restore manually.

keep_sg_version - use current SoftGate LW version in the newly installed Linux platform.

To be used in case the latest LW HotFix or a private LW was applied prior to starting the RAR process. If there was no previous LW update, then the LW from RMX Harddisk will be installed on the SG appliance.

scheduled=date_and_time - do all reinstall actions except for the activation reboot which will happen at the moment given by date_and_time. The format is : YYYY.MM.DD-HH:mm where :

JJJJ ist das Jahr

MM is the month

DD is the day

HH is the 24-hours format hour

mm is the minute

Note: the time is considered in the timezone of the Host system from which RAR is started.

no_activation_on_reboot - do not activate new software in case an unexpected reboot occurs during waiting for scheduled activation moment to come

bandwidth=bandwidth_in_Kbits - limit used bandwidth to the given amount expressed in Kbits.

RAR status [IP_Address|--active|--long]

- print overall status of RAR activities. If IP address is given then show detailed information for given target system

Migration und Neuinstallation von älteren Systemen

Remote Major Update (RMU)

- the "--active" option displays just active running instances

- the "--long" option displays the complete history

RAR cancel [IP_Address]

- interrupt and abort the execution of given RAR instance

RAR attach IP_Address

- re-attach to the terminal of an active running RAR

To dettach just close the terminal window or press CTRL-ad

!! Do NOT use CTRL-c to dettach since this will interrupt RAR !!

RAR monitor IP_Address

- monitor execution of remote RAR after it has started reinstall

RAR clear IP_Address|alle,

- clear run history for given target system or for all

4.5 Remote Major Update (RMU)

Mit dem Remote Major Update-Prozess kann ein zentrales Host-System, auf dem HiPath 4000 V7R2 ausgeführt wird, aus der Ferne auf OpenScape 4000 V10 aktualisiert werden.

Bei diesem Vorgang wird ein zweites System desselben Hardware-Typs wie das Remote-System verwendet, um ein Recovery ISO-Image vorzubereiten und zu erstellen, das die OpenScape 4000 V10R1 -Software sowie die komplette Systemkonfiguration enthält.

Dieses ISO-Image wird sodann an das Remote-Host-System übertragen und für den Remote Major Update-Prozess verwendet.

4.5.1 Wichtige Hinweise

- RMU unterstützt Appliance-Versionen ab HiPath 4000 V6 R1.10.0.
- Voraussetzung für RMU ist ein zweites System desselben Hardware-Typs wie das Remote-System.
- Folgender Zugriff auf das Remote-System wird benötigt:
 - Zugriff auf das Kopieren des logischen Backups vom Remote-System.
 - SFTP/SSH-Zugriff auf die Linux-Plattform des Remote-Systems.
 - Root-Passwort für die Linux-Plattform des Remote-Systems.
- RMU wird nur für zentrale Host-Systeme unterstützt. Informationen zu allen anderen Bereitstellungen (APEs, Standalone SoftGates und Survivable SoftGates) finden Sie im Abschnitt [Section 4.4, "Reinstallation/Aktualisierung der Remote-Appliance \(RAR\)"](#).
- RMU wird für alle Hardware-Typen unterstützt.
- Die Terminalverbindung zum Remote-Host-System kann nach dem Starten des RMU-Prozesses geschlossen werden. Der RMU-Prozess läuft im Hintergrund weiter.
- Es müssen ungefähr 4 GB an das zentrale Remote-Host-System übertragen werden. Bei Duplex-Bereitstellungen müssen diese Daten nur an den jeweils

aktiven Knoten des Remote-Systems (dem Knoten, auf dem der Assistant ausgeführt wird) übertragen werden.

- Es ist möglich, den Zeitpunkt des Neustarts bei der Aktivierung zu planen (z. B. 2015.08.11-03:00).
- Falls nach dem Aktivieren der OpenScape 4000 V10 Software Probleme auftreten, kann RMU die Original Hipath 4000/OpenScape 4000 Software automatisch wiederherstellen. Dies ist innerhalb von maximal zwei Stunden nach dem Neustart möglich, mit dem die neue Software aktiviert wurde.

4.5.2 Ablauf des Remote Major Update (RMU)

4.5.2.1 Teil 1: Vorbereiten des zweiten Systems

Installieren und konfigurieren Sie das zweite Host-System wie in [Chapter 4, "Migration und Neuinstallation von älteren Systemen"](#) beschrieben mit denselben Konfigurationsdaten wie denen des Remote-Systems.

4.5.2.2 Teil 2: Erstellen des Recovery ISO-Backups

Verwenden Sie das in der Dokumentation "OpenScape 4000 Assistant/ Manager, Backup und Restore, Administratordokumentation, Ausgabe" beschriebene Recovery ISO-Verfahren, um ein Recovery ISO-Backup auf dem zweiten System zu erstellen.

Übertragen Sie dann das erstellte Recovery ISO-Image in das Verzeichnis "/" tmp" im Dateisystem der Linux-Plattform des Remote-Host-Systems.

Wichtig: Im Falle von Duplex und Geo Separated Duplex ist es möglich, mit dem gleichen Image für Knoten A und B bzw. A, B und Q im Falle von Geo Separated Duplex wiederherzustellen. Um dies zu erreichen, wird das Recovery ISO-Image auf einen Stick (bootfähiger Stick) übertragen. In diesem Fall erstellen wir ein Backup-RISO-Image auf einem beliebigen Knoten A oder B, und die Wiederherstellung kann auf einem beliebigen Knoten (A, B oder Q) mit demselben auf dem Stick erstellten Image erfolgen.

Hinweis:

Wenn Sie über die IP-Adresse des Assistant Remote-Zugriff auf das System haben, können Sie per SFTP unter der IP-Adresse des Assistant und der Anschlussnummer 922 auf die Linux-Plattform des Remote-Systems zugreifen. Bei Duplex-Bereitstellungen erfolgt der Zugriff auf die Linux-Plattform des aktiven Knotens.

4.5.2.3 Teil 3: Starten des RMU-Prozesses

Öffnen Sie ein SSH-Terminal mit Root-Zugriff auf die Linux-Plattform des Remote-Host-Systems. Bei Duplex-Bereitstellungen öffnen Sie ein SSH-Terminal nur zum aktiven Knoten.

Hinweis:

Auf einigen Plattform-Versionen ist dies auch im Plattform Administration-Portal unter System -> Shell to host (System -> Shell zum Host) möglich. Hierdurch wird im Browser ein Terminal zum aktiven Knoten geöffnet.

Mounten Sie entweder die OS4K-Installation oder ein Recovery ISO-Image. Rufen Sie hierzu im Terminal das folgende Kommando auf (Dateinamen des ISO-Image entsprechend anpassen):

```
mount -o loop /tmp/recoveryISO_V10_R0.6.0.iso /media/
```

Starten Sie dann den RMU-Prozess, indem Sie mit dem folgenden Kommando das RMU-Skript aufrufen:

```
bash /media/RMU.sh
```

Der RMU-Prozess wird eingeleitet und die Fortschrittsanzeige eingeblendet.

Falls ein geplantes Update erforderlich ist, starten Sie den RMU-Prozess, indem Sie mit dem folgenden Kommando das RMU-Skript aufrufen:

```
bash /media/RMU.sh scheduled=datum_und_uhrzeit
```

Die Syntax für datum_und_uhrzeit lautet JJJJ.MM.TT-HH:mm. Hierbei gilt:

- JJJJ ist das Jahr
- MM ist der Monat
- TT ist der Tag
- HH ist die Stunde im 24-Stunden-Format
- mm ist die Minute

Beispiel für den RMU-Aufruf:

```
bash /media/RMU.sh scheduled=2015.08.27-02:00
```

Der RMU-Prozess installiert die neue Software im Hintergrund und wartet anschließend den mit dem scheduled-Parameter für die Aktivierung festgelegten Zeitpunkt ab. Sobald der Zeitpunkt gekommen ist, führt das Remote-Host-System einen Linux-Neustart durch und aktiviert die neue OpenScape 4000 V10-Software.

Anmerkung: Bei einer Duplex-Bereitstellung überträgt RMU das ISO-Image automatisch vom aktiven Knoten auf den/die anderen Knoten des Remote-Host-Systems.

Einmal gestartet, läuft der RMU-Prozess im Hintergrund ab, sodass das Terminal geschlossen werden kann, ohne den RMU-Prozess zu unterbrechen. RMU kann jedoch manuell durch Drücken von STRG-C im Terminal oder Eingeben des folgenden Kommandos unterbrochen werden:

```
bash /media/RMU.sh cancel
```

4.5.2.4 Teil 4: Manuelle Überprüfung nach RMU

Etwa 2 Stunden nach Beginn des RMU-Prozesses sollte sich das Remote-Host-System in folgendem Zustand befinden:

- Die OS4K V10-Software wird ausgeführt.
- Die Telefonie-Services sind betriebsbereit.
- Die CSTA- und Telefonie-Anwendungen sind betriebsbereit.
- Der Assistant wurde frisch installiert und eine logische Wiederherstellung ausgeführt (überprüfen auf der Seite "Backup & Restore" [Sichern & Wiederherstellen]).

4.6 Reinstallation vom Recovery ISO-Image

Die Recovery ISO-Funktion und der Reinstallationsvorgang sind in der "OpenScape 4000 Assistant, Appliance-Management, Administratordokumentation" im Kapitel "Reinstallation einer Appliance vom Recovery ISO-Image" beschrieben.

5 Update-/Upgrade-Prozess für OpenScape 4000

Dieses Leistungsmerkmal ist ab OpenScape 4000 V7 R1 freigegeben.

Ab OpenScape 4000 V7 R1 können die zentralen Systemkomponenten (Hostsystem einschließlich OpenScape 4000 Assistant, OpenScape 4000 CSTA usw.) und die peripheren Systemkomponenten (Zugangspunkte, Access-Points einschließlich APE) beim Aktualisieren von einem auf ein anderes Minor Release in einem Arbeitsgang aktualisiert werden.

Informationen zur Migration auf OpenScape V10 R0, siehe [Chapter 4, "Migration und Neuinstallation von älteren Systemen"](#).

Wichtig: Der gesamte Update-Prozess kann per Remote-Zugriff erfolgen. Unterstützung vor Ort ist nicht erforderlich.

Die Aktualisierung wird in zwei Phasen durchgeführt:

Vorbereitungsphase

- 1) Die Vorbereitung beginnt automatisch nach der Übertragung des RLC-Pakets auf die Festplatte. Während der Vorbereitungsphase wird die Software in das Verzeichnis `var/newdisk` kopiert und die Loadware der IP-Baugruppen verteilt.

Während der Vorbereitungsphase ist nicht mit Ausfällen der Telefonfunktionen zu rechnen.

Aktivierungsphase

In der Aktivierungsphase wird die neue Loadware geladen, ein Backup sämtlicher Daten angelegt, die Installation durchgeführt und anschließend das Backup wieder vollständig eingespielt.

Für den Update-Prozess werden lediglich die OpenScape 4000 Assistant-Anwendungen Software Transfer und Software Activation benötigt.

Die Knoten werden in der folgenden Reihenfolge aktualisiert:

- 2) Quorum (falls vorhanden)
- 3) Standby-Knoten (falls vorhanden)
- 4) Aktiver Knoten

Während der Aktualisierung werden verschiedene Timer installiert, um den Prozess zu "überwachen". Im Falle einer Zeitüberschreitung eines dieser Timer wird ein Rollback zur Wiederherstellung der vorherigen Systemversion eingeleitet. Für einen aktualisierten Knoten beträgt die Vorgabezeit 20 Minuten.

Die gesamte Aktualisierung (Vorbereitung und Aktivierung) eines Separated Duplex-Systems dauert etwa 2 bis 3 Stunden (Ausfallzeit des Telefonsystems ungefähr 1 Stunde). Die Zeiten können je nach Konfiguration des Kunden und Systemauslastung während der Aktualisierung variieren.

Die Protokolldateien für den Update-Prozess befinden sich im Verzeichnis `var/log/nuc` und sind in der OpenScape 4000 Administration Platform (Portal) einsehbar. Alle NUC Upgrade-Protokolle können nach einer erfolgreichen ebenso wie nach einer fehlgeschlagenen Aktualisierung in der **OpenScape 4000 Administration Platform (Portal)** abgerufen werden. Aktivieren Sie zu diesem Zweck die Kontrollkästchen "Update", "Messages", "Webservice" und "Firstinstall".

5.1 Aktualisieren von einem Minor Release auf ein anderes Minor Release

Das HotFix-Paket wird mittels SWT (Software-Transfer) auf das System übertragen und anschließend mittels SWA (Software-Aktivierung) aktiviert. Im nächsten Schritt wird RLC V10R0 über SWT hochgeladen und mittels SWA aktiviert. Bitte befolgen Sie den Prozess, der in [Chapter 5, "Major-Release-Upgrade"](#) beschrieben wird,

nachdem Sie den HotFix erfolgreich angewendet und RLC hochgeladen haben.

5.1.1 Voraussetzungen

- Die folgenden Versionen müssen auf dem zu aktualisierenden System installiert sein:

Bei OpenScape 4000 V7 R1

- mindestens OpenScape 4000 Platform Version V7 R1.39.2
- mindestens OpenScape 4000 Assistant Version V7 R1.7.11

Bei OpenScape 4000 V7 R2

- mindestens OpenScape 4000 Platform Version V7 R2.23.2
- mindestens OpenScape 4000 Assistant Version V7 R2.20.4

Wichtig: Übertragen Sie den OpenScape 4000 Assistant Hotfix nicht zusammen mit dem neuen OpenScape 4000 V10 R0 RLC-Paket, weil die Vorbereitungsphase nach der Übertragung des RLC-Pakets auf das System automatisch gestartet wird.

- Parameter **NOIPBLWL** in AMO ZANDE

Um die Ausfallzeiten des Telefonsystems zu minimieren, muss in AMO ZANDE der Parameter **NOIPBLWL (No IP Board Loadware Load)** auf **YES** gesetzt werden. Wenn dieser Parameter auf **YES** gesetzt ist, wird die neue Loadware einer IP-Baugruppe bei einem Neustart/Reboot nicht geladen.

CHANGE-ZANDE:TYPE=ALLDATA2,NOIPBLWL=YES;

EXEC-UPDAT:UNIT=BP,SUSY=DELTA;

Wichtig: Führen Sie ein APE-Backup aus, um sicherzugehen, dass die Access Points ebenfalls korrekt eingestellt sind.

Wenn der empfohlene Parameter **NOIPBLWL** nicht verwendet wird, sieht der Ablauf wie folgt aus:

Während des Updates bekommen die NCUIs/CGWs und OpenScape 4000 SoftGates die OpenScape 4000 V10 R0 Loadware über das Leistungsmerkmal "Reduce down time" über https (Default).

Dann wird das System heruntergefahren und NCUIs/CGWs und OpenScape 4000 SoftGates werden auf den APE umgeschaltet (wenn konfiguriert).

Da der APE mit der OpenScape 4000 V7 R1 Loadware oder höher läuft, wird die OpenScape 4000 V10 R0 Loadware, die im ersten Schritt

heruntergeladen wurde, überschrieben und die Umschaltung zum APE wird extrem langsam, weil die Loadware über FTP zu den NCUIs und STMIs übertragen wird.

Wenn das RLC beendet ist, werden die NCUIs/CGWs und OpenScape 4000 SoftGates vom APE wieder zum Host zurückgeschaltet und NCUIs/ STMIs laden die OpenScape 4000 V10 R0 Loadware über FTP (was wieder langsam ist).

Wenn der empfohlene Parameter **NOIPBLWL** verwendet wird (auf **JA** gesetzt), dann umgeht man die FTP-Downloads in den Schritten 3 und 4, was die Umschaltung zum APE und vom APE zurück zum Host (nach dem NCUI Startup) extrem schnell macht.

Anmerkungen:

- Wenn kein APE verwendet wird, dann ist das Setzen des Parameters **NOIPBLWL** nicht nötig.
- Wenn die OpenScape 4000 V10 R0 Loadware vor dem RLC auf dem Host und APE manuell aktualisiert wurde, ist das Setzen des Parameters **NOIPBLWL** nicht nötig.
- Öffnen Sie Sysinfo auf dem **active node**

Mit Sysinfo können Sie den Update-Prozess auf allen Knoten überwachen.

http://portal_ip_address/sysinfo

OpenScape 4000			
System Information			
Status	Settings	Software	Hardware
Hostname	Katrina-A	Katrina-B	Katrina-Q
Info			
Vendor	American Megatrends Inc.	American Megatrends Inc.	Phoenix Technologies LTD
Version	080015	080015	6.00
Date	12/12/2011	12/12/2011	06/22/2012
Linux			
Distribution	SUSE Linux Enterprise Server 11 x86_64 SP3	SUSE Linux Enterprise Server 11 x86_64 SP3	SUSE Linux Enterprise Server 11 x86_64 SP3
Version	3.0.101-0.40-default	3.0.101-0.40-default	3.0.101-0.40-default
Kernel Version			
Update Info			
Current Version	V7.81.39.2	V7.81.39.2	V7.81.39.2
Last Update	V7.81.39.0	V7.81.39.0	V7.81.39.0
From Version	V7.81.39.2	V7.81.39.2	V7.81.39.2
to Version	2016-06-18 11:23:45	2016-06-18 11:23:45	2016-06-18 11:23:45
started at	2016-06-18 11:01:00	2016-06-18 11:01:00	2016-06-18 11:01:00
ended at	successful	successful	successful
Update Status			

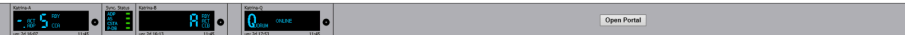


Abbildung 124: sysinfo

- Alle Knoten des Systems müssen betriebsbereit sein.

Dies kann in Sysinfo (siehe Bild oben) oder im Frontpanel der OpenScape 4000 Platform Administration (Portal) überprüft werden.

OpenScape 4000 Platform Administration (Portal) > System Frontpanel

- Vor Beginn des Update-Prozesses müssen alle OpenScope 4000 CCAPs/ Survivable Softgate synchronisiert sein.

Der Status des Hostsystems und aller CC APs/Survivable OpenScope 4000 SoftGates kann im OpenScope 4000 Assistant unter "Backup & Restore" (Sichern & Wiederherstellen) überprüft werden.

Backup & Restore									
HBR									
RMX									
Home Page									
Backup									
Restore									
Content									
Status									
History									
Schedule									
GLA/PDS									
Administration									
VMD2									
Backup Server									
AP Backup Server									
Configuration									
CC-APs									
Log Files									

Status of the Host and all CC-APs:									
Name	IP Address	Transfer	Status		Backup/Restore		RMX Status	Log	Delete
			Status	Date/Time	Status	Date/Time			
Host	192.168.127.1 (LAP2)	OK	2016-08-08	05:13:05	OK	2016-08-08 05:13:12		-	Delete
CC-AP(18)	192.168.127.113 (LAP2)	OK	2016-08-08	12:01:58	OK	2016-08-08 05:09 DAP L31985Q0071X00000 HPPath4000V70 SA01 RL39 001 RMX UNIX		-	Delete
CC-AP(20)	192.168.127.123 (LAP2)	OK	2016-08-08	11:55:51	OK	2016-08-08 05:09 DAP L31985Q0071X00000 HPPath4000V70 SA01 RL39 001 RMX UNIX		-	Delete
CC-AP(30)	192.168.127.133 (LAP2)	OK	2016-08-08	11:56:46	OK	2016-08-08 05:09 DAP L31985Q0071X00000 HPPath4000V70 SA01 RL39 001 RMX UNIX		-	Delete
CC-AP(98)	192.168.127.193 (LAP2)	OK	2016-08-08	11:59:30	OK	2016-08-08 05:09 DAP L31985Q0071X00000 HPPath4000V70 SA01 RL39 001 RMX UNIX		-	Delete

Abbildung 125: Status des Hostsystems und der CC APs/Survivable SoftGates

5.1.2 Vorbereitung

1) Überprüfen Sie die Versionen von OpenScope 4000 Platform und OpenScope 4000 Assistant.

Bei OpenScope 4000 V7 R1

- mindestens OpenScope 4000 Platform Version V7 R1.39.2
- mindestens OpenScope 4000 Assistant Version V7 R1.7.11
- Bei OpenScope 4000 V7 R2
- mindestens OpenScope 4000 Platform Version V7 R2.23.2
- mindestens OpenScope 4000 Assistant Version V7 R2.20.4

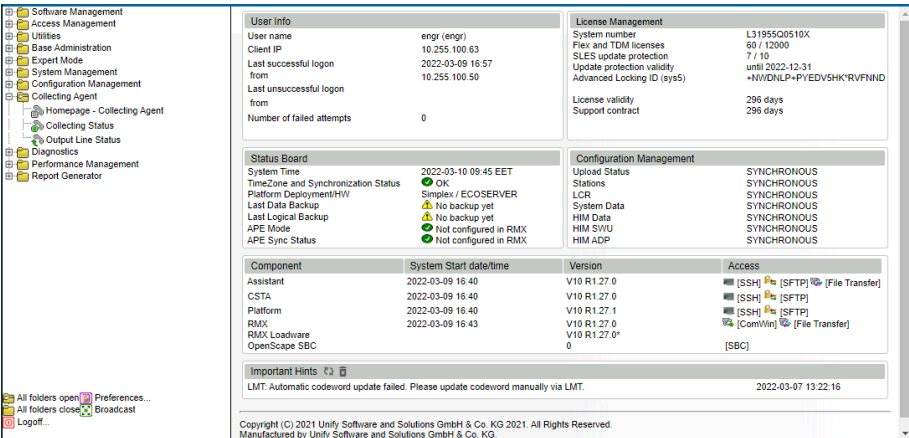


Abbildung 126: OpenScope 4000 Assistant - Startseite

Falls das OpenScope 4000 Assistant Hotfix noch nicht installiert ist, übertragen Sie es mit Software Transfer auf das System und aktivieren Sie es mit Software Activation.

Wichtig: Übertragen Sie nicht gleichzeitig auch das RLC-Paket!

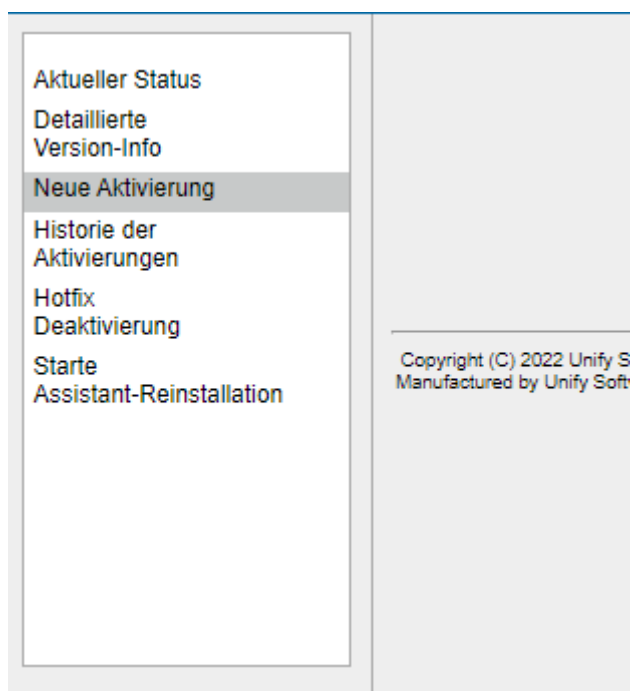


Abbildung 127: Aktivieren des OpenScape 4000 Assistant Hotfix

1) Kontrollierter Reboot für Survivable OpenScape 4000 SoftGate

Jedes Survivable OpenScape 4000 SoftGate wird während des HBR (APE Restore)-Prozesses automatisch neu hochgefahren.

Dieses Standardverhalten kann auf dem Host geändert werden.

Software Management (Software-Management) > Backup & Restore (Sichern & Wiederherstellen) > Configuration (Konfiguration) > Automatic OS Update Activation (BS-Update automatisch aktivieren)

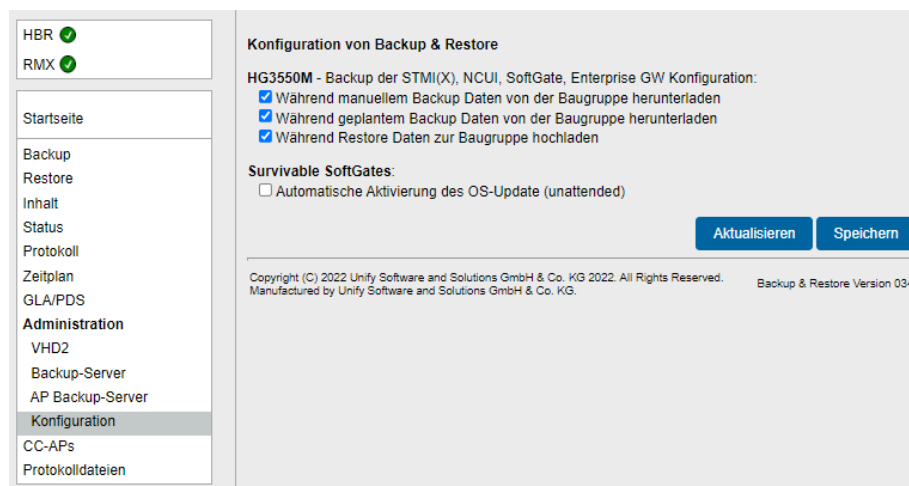


Abbildung 128: Survivable SoftGate - Deaktivieren der automatischen Aktivierung von BS-Updates

Führen Sie ein APE-Backup aus, um sicherzugehen, dass die Survivable OpenScape 4000 SoftGate ebenfalls korrekt eingestellt ist.

Wenn die Option **Automatic OS Update Activation (unattended)** (BS-Update automatisch aktivieren) deaktiviert ist (kontrolliertes Update), muss die Aktivierung des Betriebssystems auf den Survivable OpenScape 4000 SoftGates vor dem Rebooten des Systems im Rahmen des APE Restore-Prozesses vom OpenScape 4000 SoftGate WBM aus bestätigt werden. Dies wird von Software Activation angezeigt. Die Aktivierung des Betriebssystems beim Rebooten während der Aktualisierung wird mit dem folgenden Menübefehl bestätigt:

WBM: Maintenance (Wartung) > SW Update (SW-Update) > OS Update (BS-Update) > OS Update Actions (BS-Update-Aktionen) > Activate OS Update (BS-Update aktivieren)

2) Übertragen Sie das RLC-Paket mit OpenScape 4000 Assistant Software Transfer.

Verwenden Sie OpenScape4000 statt OpenScape4000V70 als File Transfer RLC Root-Verzeichnis, z.B. OpenScape4000\hhd300\.

Wählen Sie mit dem Kontrollkästchen das RLC-Paket aus und klicken Sie auf die Pfeilschaltfläche, um die Übertragung zu starten.

Warten Sie, bis das Popup-Fenster mit dem Link zur SWA erscheint. Dies zeigt an, dass der Transfer abgeschlossen ist, das Paket intern an die SWA übertragen wurde und die Vorbereitungsphase bereits begonnen hat.

Klicken Sie auf den Link im Popup-Fenster, um die Vorbereitungsphase zu verfolgen. Das Fenster **Current Status** (Aktueller Status) der **Software Activation** wird geöffnet.

Zuletzt ausgeführte Aktivierung		Aktuelle Aktivierung	
Version:	Installation OpenScape 4000 Assistant V10 R1.34.0	Version:	---
Datum:	2022-06-09	Datum:	---
Uhrzeit:	10:28	Uhrzeit:	---
Status:	erfolgreich	Status:	---
		Task:	---

Copyright (C) 2022 Unify Software and Solutions GmbH & Co. KG
2022. All Rights Reserved.
Manufactured by Unify Software and Solutions GmbH & Co. KG.

Software-Aktivierung Version: ASswa2-10.001-0027.adp
ASswa2ui-10.001-0025.adp

Abbildung 129: Vorbereitungsphase des Updates ist abgeschlossen

3) Überprüfen Sie den Aktivierungsstatus in OpenScape 4000 Assistant.

Historie der Aktivierungen					
Aktivierungsprotokolle sammeln					
2022-06-09 10:28	Installation	OpenScape 4000 Assistant V10 R1.34.0	erfolgreich	Protokolldatei	Detaillierte Protokolldatei

Copyright (C) 2022 Unify Software and Solutions GmbH & Co. KG
2022. All Rights Reserved.
Manufactured by Unify Software and Solutions GmbH & Co. KG.

Software-Aktivierung Version: ASswa2-10.001-0027.adp
ASswa2ui-10.001-0025.adp

Software Activation > Activation History (Aktivierungshistorie)

4) Überprüfen Sie den REGEN&GENDB-Status in OpenScape 4000 Assistant.

Software Activation > Auto REGEN&GENDB

Siehe:

[OpenScape 4000 Assistant / Manager V10, Software-Aktivierung, Administratordokumentation](#)

5) Optional: Öffnen Sie den Gateway Manager auf dem aktiven Knoten.

Mit dem Gateway Manager des OpenScape 4000 Assistant können Sie die Verteilung der Loadware der IP-Baugruppen überwachen.

OpenScape 4000 Assistant > Expert Mode (Experten-Modus) > Gateway Manager

5.1.3 Aktivierung

Starten Sie die Aktivierungsphase:

OpenScape 4000 Assistant > Software Activation > New activation (Neue Aktivierung)

Wählen Sie die Version **Minor Release OpenScape 4000 V10 R0.x** aus.

Um die Ausfallzeit des Systems zu minimieren, wird dringend empfohlen, folgende **Loadware-Update-Optionen** auszuwählen:

- **Enable reduce downtime LW update during activation (LW für kürzere Ausfallzeit während der Aktivierung aktualisieren)**
- **Update SoftGate (SoftGate aktualisieren)**

Wichtig: Bei einem Upgrade von V7 R1.39.2 erfolgt die Übertragung und Vorbereitung des OpenScape 4000 SoftGate Betriebssystems automatisch im Rahmen des RLC-Updates; die Aktivierung des Betriebssystems erfolgt jedoch manuell über GW-Manager - Registerkarte Betriebssystem-Update.

Wichtig: Bei einem Upgrade von V7 R2.23 erfolgt die Übertragung und Vorbereitung des OpenScape 4000 SoftGate Betriebssystems automatisch im Rahmen des RLC-Updates. Das Standalone SoftGate wird während der Aktivierung neu gestartet.

Wichtig: Wichtig: Um bei einem Upgrade von V7 R2.23 den Neustart des Standalone SoftGates zu verhindern, müssen Sie vor Beginn der RLC-Aktivierung die Option "Aktivieren Sie das Betriebssystem auf dem Standalone-SoftGate nach dem Transfer" deaktivieren. In diesem Fall erfolgt nur eine Übertragung und Vorbereitung des OpenScape 4000 SoftGate Betriebssystems; die Aktivierung des Betriebssystems sollte manuell über GW-Manager - Registerkarte Betriebssystem-Update erfolgen.

- **Continue with activation if LW activation fails (Bei fehlgeschlagener LW-Aktivierung mit Aktivierung fortfahren)**

Klicken Sie auf **Activate immediately** (Sofort aktivieren), um den Update-Prozess jetzt zu starten.

Eine Übersicht der Aufgaben, die während der Aktivierung ausgeführt werden, wird angezeigt.

Die meisten der Aufgaben können mit dem OpenScape 4000 Assistant überwacht werden.

Beispiel: Loadware-Update im **Gateway Manager**.

	PEN IP-Adresse	Typ Funktionalität	RMX Status	Fortschritt	Laufende LW Auf Flash verfügbare LW	Auf RMX verfügbare LW	Übertragungszeit Aktivierungszeit
<input type="checkbox"/>	1-50-2 10.121.121.58	SLMAEB	READY		pzesla40 02/24/15 15:55:44	pzesla40 02/24/15 15:55:44	
<input type="checkbox"/>	1-50-3 10.121.121.58	vHG3500 HG8330	READY		pkskw50 A9.205	pkskw50 A9.205	
<input type="checkbox"/>	1-50-4 10.121.121.58	vHG3500 SIP	READY		pkskw50 A9.205	pkskw50 A9.205	
<input type="checkbox"/>	1-50-5 10.121.121.55	vHG3500 HG8350	READY		pkskw50 A9.205	pkskw50 A9.205	
<input type="checkbox"/>	1-50-6 10.121.121.50	Standalone SoftGate	READY		pkskw50 A9.205	pkskw50 A9.205	

Abbildung 130: Loadware-Update während des Updates

Dasselbe gilt für den Verlauf des Backups von OpenScape 4000 Assistant in **Backup & Restore** (Sichern & Wiederherstellen).

Außerdem können Sie auf der OpenScape 4000 Assistant-Startseite erkennen, dass das Update insgesamt stattfindet (siehe **Wichtige Hinweise**) und im Moment ein logisches Backup ausgeführt wird.

Im Menü **Current Status** (Aktueller Status) der **Software Activation** können Sie feststellen, welche Aktivierung momentan läuft.

Aktueller Status	Zuletzt ausgeführte Aktivierung	Aktuelle Aktivierung
Detaillierte Version-Info Neue Aktivierung Historie der Aktivierungen Hotfix Deaktivierung Starte Assistant-Reinstallation	Version: RLC FR OpenScape 4000 V10 R1.34.0 Datum: 2022-06-09 Uhrzeit: 12:38 Status: erfolgreich	Version: --- Datum: --- Uhrzeit: --- Status: --- Task: ---

Copyright (C) 2022 Unify Software and Solutions GmbH & Co. KG
2022. All Rights Reserved.
Manufactured by Unify Software and Solutions GmbH & Co. KG.

Software-Aktivierung Version: ASswa2-10.001-0027.adp
ASswa2ui-10.001-0025.adp

Abbildung 131: Software Activation > Current Status (Aktueller Status)

Nach Abschluss der Loadware-Übertragung befindet sich die gesamte Loadware der IP-Baugruppe in ihrem Flash-Speicher.

Zwischen den Aufgaben **Waiting for OpenScape 4000 Assistant shutdown** (Warten auf Shutdown des OpenScape 4000 Assistant) und **Starting Telephony Services** (Starten der Telefondienste) sind die Telefonfunktionen nicht verfügbar. Die Loadware wird nun Shelf für Shelf aktualisiert, wobei alle Dienste und Anwendungen angehalten werden.

Wichtig: Die Telefone sollten so konfiguriert sein, dass Sie nun in den Notfallmodus wechseln.

Zustand	LAN	Software	Hardware
Rechnername			ManagerSteroizi
OpenScape System			
Sysinfo Daten			aktuell
OpenScape Status			
Betriebssystem			
Systemzeit			15.06.2022 12:05:19
Uptime			11 22:38
Prozesse und Threads			889
CPU			
Temperatur			28 °C
Auslastung			7%
System			4%
RAM			
insgesamt			31478 MIB
belegt			6747 MIB
verwendet			2423 MIB
Swap			
insgesamt			16384 MIB
belegt			8 MIB
Festplatte 1			
Temperatur			34 °C
Fehlerhafte Blöcke			keine
Fehlermeldungen			keine
Warnhinweise			keine
Festplatte 2			
Temperatur			37 °C
Fehlerhafte Blöcke			keine
Fehlermeldungen			keine
Warnhinweise			keine
Lüfter Geschwindigkeit			
			Lüfter1: 33%
			Lüfter2: 35%

Abbildung 132: sysinfo - Alle Dienste wurden angehalten

Nach einigem Rebooten wird die Installation von OpenScape 4000 Assistant gestartet und anschließend eine logische Wiederherstellung durchgeführt. Anschließend funktionieren die Telefondienste wieder. Warten Sie, bis die Aktivierung des RTC abgeschlossen ist.

Die Dauer des Update-Prozesses können Sie der ausführlichen Protokolldatei im OpenScape 4000 Assistant entnehmen:

Software Activation > Current Status (Aktueller Status)

Aktueller Status

Detaillierte Version-Info

Neue Aktivierung

Historie der Aktivierungen

Hotfix

Deaktivierung

Starte Assistant-Reinstallation

Historie der Aktivierungen

Aktivierungsprotokolle sammeln

2022-06-09 12:38	RLC FR	Aktivierung	OpenScape 4000 V10 R1.34.0	erfolgreich	Protokolldatei	Detaillierte Protokolldatei
2022-06-09 10:59	RLC FR	Aktivierung	OpenScape 4000 V10 R1.34.0 Preparation	erfolgreich	Protokolldatei	Detaillierte Protokolldatei
2022-05-26 20:30	RLC FR	Aktivierung	OpenScape 4000 V10 R1.33.0	erfolgreich	Protokolldatei	Detaillierte Protokolldatei
2022-05-26 09:06	RLC FR	Aktivierung	OpenScape 4000 V10 R1.33.0 Preparation	erfolgreich	Protokolldatei	Detaillierte Protokolldatei
2022-05-17 20:30	RLC FR	Aktivierung	OpenScape 4000 V10 R1.32.0	erfolgreich	Protokolldatei	Detaillierte Protokolldatei

Abbildung 133: Software Activation - Dauer des Updates

Wichtig: Nach dem ersten AP-Backup auf dem Host und der AP-Wiederherstellung durch CC-AP müssen folgende Befehle ausgeführt werden: CHANGE-ZANDE:TYPE=ALLDATA2,NOIPBLWL=NO; EXEC-UPDAT:UNIT=BP,SUSY=DELTA;

Wichtig: Nach erfolgreicher Durchführung des Upgrades läuft das OpenScape 4000 V10 System mit der Grace-Period-Übergangslizenz. Für das System wird eine neue V10-Lizenz

benötigt. Informationen zur V10-Lizenzgenerierung, siehe [Chapter 7, "Lizenzierung"](#)

5.1.3.1 APE und Survivable SoftGate aktivieren

Nach dem Aktualisieren des Hosts muss ein APE-Backup für die APEs eingeleitet werden.

Wenn die Option **Automatic OS Update Activation (unattended)** (BS-Update automatisch aktivieren) deaktiviert ist (kontrolliertes Update), muss die Aktivierung des Betriebssystems auf den Survivable OpenScape 4000 SoftGates vor dem Rebooten des Systems im Rahmen des APE Restore-Prozesses vom OpenScape 4000 SoftGate WBM aus bestätigt werden (siehe **Software Activation > Current Status** [Aktueller Status]).

```

Preparing files for the update
  Checking patch files and version of Applications.....[   done   ]
Preparing Assistant and CSTA for first installation
  Back up OpenScape 4000 Assistant configuration data.....[   done   ]
  Back up OpenScape 4000 CSTA configuration data.....[   done   ]
Updating OpenScape 4000 Platform
  Initiating OpenScape 4000 Platform update.....[   done   ]
  Waiting for local OS Activation trigger from SoftGate (AP 30).....[ working ]
  Starting Telephony Services.....[               ]
  Installing OpenScape 4000 Assistant.....[               ]
  Enabling OpenScape 4000 Assistant login.....[               ]
  Restoring OpenScape 4000 Assistant configuration data.....[               ]
OpenScape 4000 Platform check
  Checking Platform update result.....[               ]
OpenScape 4000 CSTA check
  Checking CSTA restore.....[               ]
Verifying update results.....[               ]
Updating Assistant version in RMX.....[               ]
Finalizing activation.....[               ]

```

Abbildung 134: Software Activation - Warten auf Neustart des Survivable OpenScape 4000 SoftGate

Die Aktivierung des Betriebssystems beim Rebooten während der Aktualisierung wird mit dem folgenden Menübefehl bestätigt:

WBM > Maintenance (Wartung) > SW Update (SW-Update) > OS Update (BS-Update) > OS Update Actions (BS-Update-Aktionen) > Activate OS Update (BS-Update aktivieren)

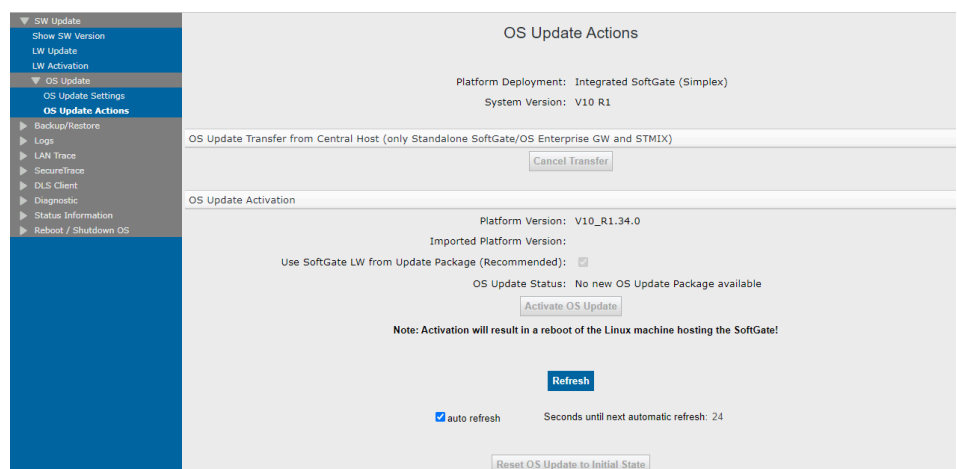


Abbildung 135: WBM - Betriebssystem-Update für Survivable OpenScape 4000 SoftGate

Nach dem Neustart des Survivable OpenScape 4000 SoftGate wird die RLC-Aktivierung fortgesetzt. Der endgültige Status kann in WBM und OpenScape 4000 Assistant überprüft werden.

WBM: **Maintenance (Wartung) > SW Update (SW-Update) > Show SW Version (SW-Version anzeigen)**

Software Version	
System Version (PBX)	
System Version: V8 R0	
Platform Version	
Hardware: Standard Server (From OpenScape 4000 V8 COTS HW is no longer supported. For further details please see Release Notes.)	
Platform Deployment: Survivable SoftGate (20)	
Platform Version: V8_R0.8	
Imported Platform Version:	
OS Update Status: No new OS Update Package available (0)	
Loadware Version	
Loadware Version: pzksqw50.A5.001-008	
APS Version: L0-T4T.A5.001-008	
Component Versions	
IMS SVN Version: Maven_5859_2016.07.06-11.23	
SoftGate SVN Version: Maven_11091_2016.07.07-07.50	
vSLC Version: KV027	
CLA Version: cla-v1-r31.0.1.x86_64	
Soco-common Version: soco-common-8.0-15.x86_64	
OpenSIPS Version: opensips-1.6.3-331.x86_64	
Additional Package Versions	
Java Version: IBM x86-64 java-1_7_1-ibm-1.7.1_sr3.40-13.1	

Abbildung 136: WBM - Software-Version nach dem Update

OpenScape 4000 Assistant: **Software Activation > Activation History (Aktivierungshistorie)**

Software Activation	
Current status	Content of file:
Detailed version info	/var/swa2/activations/log/history/201608090641_1470730404/software_activation.sum
New activation	
Activation history	Preparing files for the update
Hotfix Deactivation	Checking patch files and version of Applications..... [done]
Start Assistant	Preparing Assistant and CSTA for first installation
reinstallation	Back up OpenScape 4000 Assistant configuration data..... [done]
	Back up OpenScape 4000 CSTA configuration data..... [done]
	Updating OpenScape 4000 Platform
	Initiating OpenScape 4000 Platform update..... [done]
	Waiting for local OS Activation trigger from SoftGate (AP 30)..... [done]
	Starting Telephony Services..... [done]
	Installing OpenScape 4000 Assistant..... [done]
	Enabling OpenScape 4000 Assistant login..... [done]
	Restoring OpenScape 4000 Assistant configuration data..... [done]
	OpenScape 4000 Platform check
	Checking Platform update result..... [done]
	OpenScape 4000 CSTA check
	Checking CSTA restore..... [done]
	Verifying update results..... [done]
	Updating Assistant version in RMX..... [done]
	Finalizing activation..... [done]
	!!! UPDATE FINISHED SUCCESSFULLY !!!
	Preparation : 5 minutes 16 seconds
	Waiting for SG Activation trigger : 3 hours 39 minutes 6 seconds
	Downtime : 23 minutes 19 seconds
	Post Actions : 23 minutes 47 seconds
	Home Page
	Activation history

Abbildung 137: OpenScape 4000 Assistant - Software-Version nach dem Update

5.1.3.2 Standalone SoftGate aktualisieren

Die Betriebssystemaktivierung auf den Standalone OpenScope 4000 SoftGates muss auf dem OpenScope 4000 Assistant bestätigt werden:

Expert Mode (Experten-Modus) -> Gateway Manager -> Registerkarte OS Update (BS-Update) -> Activate OS (BS aktivieren)

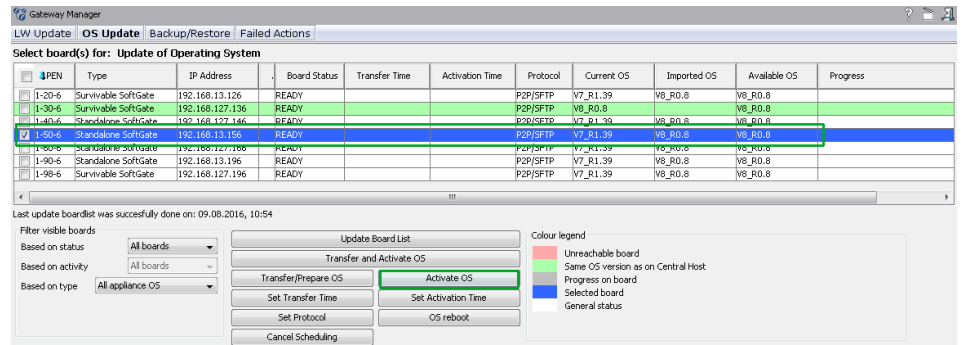


Abbildung 138: SG OS GW-Manager aktivieren

Das neue Betriebssystem ist nach dem Neustart des Standalone SoftGate aktiv.

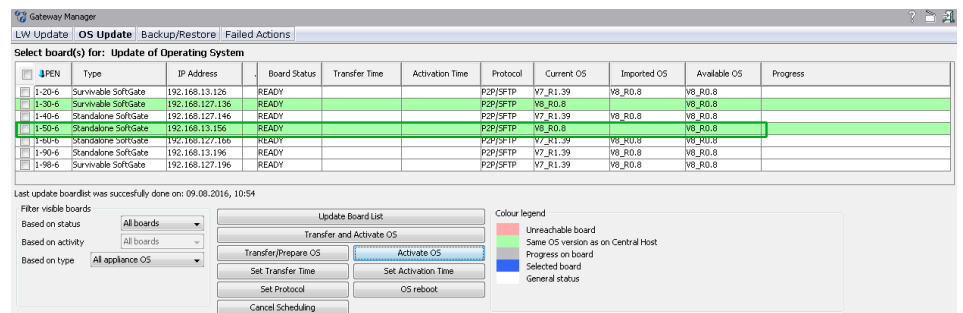


Abbildung 139: SG OS GW-Manager aktivieren

5.2 Major-Release-Upgrade

Wichtig: Ein Major-Release-Upgrade auf V10 mittels SWT/SWA ist ab Assistant V7 R1.7 möglich. Direkte RLC-Upgrades von V7 R0 oder V6 und früher auf V8 werden nicht unterstützt.

Vor Durchführung des Upgrade-Prozesses muss zunächst der jeweilige HotFix angewendet werden:

Release	HotFix-Version
V7 R1 Assistant	V7 R1.7.11
V7 R2 Assistant	V7 R2.20.4

Das HotFix-Paket wird mittels SWT (Software-Transfer) auf das System übertragen und anschließend mittels SWA (Software-Aktivierung) aktiviert. Im nächsten Schritt wird RLC V8R0 über SWT hochgeladen und mittels SWA aktiviert.

Bitte befolgen Sie nach erfolgreicher HotFix-Anwendung und RLC-Upload den in [Chapter 5, "Update-/Upgrade-Prozess für OpenScape 4000"](#) beschriebenen Prozess, um das Upgrade auf die Major-Version durchzuführen.

5.2.1 Kürzere Downtime für LoadWare-Hotfixes

Diese Funktion kann während des Upgrade-Prozesses verwendet werden.

Softwareupdate-Pakete (RLC) enthalten neue LoadWare-Dateien, die über die Funktion "Reduce downtime" (Downtime verkürzen) aktiviert werden können.

LoadWare (LW) Hotfixes können freigegeben werden, kurz bevor das RLC-Paket aktiviert wird.

In solchen Situationen musste der Service bisher das RLC-Paket und den LoadWare (LW) Hotfix aktivieren, was zu einer zweifachen Downtime des Telefonsystems führte. Mit dieser Funktion können nun beide Updates zusammengelegt werden.

Nutzen Sie den Software-Transfer, um RLC und LW HF gemeinsam zu übertragen und zu aktivieren.

Der OpenScape 4000 Assistant verwendet den LoadWare (LW) Hotfix mit neueren Inhalten, und nicht die Loadwares aus dem RLC-Paket. Somit wird nur eine Downtime benötigt. Der Unterschied zwischen diesem Update-Szenario und dem vorherigen liegt darin, dass der LoadWare-Hotfix nicht in der GUI der Software-Aktualisierung angezeigt wird.

- Übertragung des LoadWare-Hotfixes an OpenScape 4000 Assistant.
- Übertragung des Minor/Fix-Releases (RLC).
- Aktivierung des Minor/Fix-Releases - standardmäßig werden bei der Software-Aktivierung (SWA) LW-HF-Dateien für das LW-Update während der Aktivierung des Minor/Fix-Releases verwendet.

6 Ändern der Plattformkonfiguration

6.1 Wichtige Hinweise

Dieses Dokument sollte für ein bereits installiertes System verwendet werden, auf dem einige IP-Adressen/Schnittstellen geändert werden müssen.

Alle Änderungen der IP-Adresskonfiguration sollten mit dem **Recovery/Reconfiguration Tool** vorgenommen werden.

OpenScape 4000, Plattform Administration (Portal)

Es besteht nach wie vor die Möglichkeit, das OpenScape 4000 Plattform Administration-Portal für Änderungen der IP-Adresse zu verwenden, jedoch nur, wenn die alte und die neue IP-Adresse demselben IP-Subnetz angehören. In diesem Fall wird der Telefonbetrieb beim Ändern der IP-Adresse mit dem OpenScape 4000 Plattform Administration-Portal nicht unterbrochen. (Ausnahme: Ändern der IP-Adresse des IPDA-Netzwerks, siehe [Section 6.4.2, "Ändern der IP-Adresse des IPDA-Netzwerks"](#)).

Beispiele für im OpenScape 4000 Plattform Administration-Portal vorgenommene Änderungen, die keine Unterbrechung des Telefonbetriebs verursachen:

- Ändern der IP-Adresse des OpenScape 4000 Plattform Administration-Portals (alte und neue IP-Adresse im selben Subnetz)
- Ändern der IP-Adresse des OpenScape 4000 Assistant (alte und neue IP-Adresse im selben Subnetz)
- Ändern der IP-Adresse des OpenScape 4000 CSTA (alte und neue IP-Adresse im selben Subnetz).
- Atlantic-Schnittstelle (wenn die Zielschnittstelle bereits mit der IP 0.0.0.0/0 konfiguriert ist)

Recovery/Reconfiguration Tool

Das Recovery/Reconfiguration Tool muss verwendet werden, wenn die alte und die neue IP-Adresse nicht demselben Subnetz angehören oder neue Schnittstellen konfiguriert werden müssen.

Wichtig: Beachten Sie, dass der Telefonbetrieb bei Verwendung des Recovery/Reconfiguration Tools unabhängig von den auf den Knoten vorgenommenen Änderungen unterbrochen wird (wie bei einem normalen Neustart des Systems).

Weitere Informationen zum Recovery/Reconfiguration Tool finden Sie in [Section 6.3, "Recovery/Reconfiguration Tool"](#).

Aufruf des Erstinstallationsskript mit der Option -s

Wird das Skript mit der Option **-s** und einem zweiten Parameter aufgerufen, werden nur die folgenden Konfigurationen aus der XML-Datei durchgeführt, ohne Löschen/Reinstallation der Netzwerk-Konfiguration.

Ändern der Plattformkonfiguration

Verwenden des OpenScape 4000 Plattform Administration-Portals

Tabelle 34: firstinst-netw.sh, Option -s

<code>./firstinst-netw.sh -s keyboard</code>	--> Nur das Layout der Tastatur wird konfiguriert
<code>./firstinst-netw.sh -s timezone</code>	--> Nur die Zeitzone wird konfiguriert
<code>./firstinst-netw.sh -s dns</code>	--> Nur der/die DNS-Server wird/werden konfiguriert
<code>./firstinst-netw.sh -s ntp</code>	--> Nur der/die NTP-Server wird/werden konfiguriert
<code>./firstinst-netw.sh -s all</code>	--> Nur die 4 Parameter oben beschrieben werden konfiguriert

Jede bestehende Konfiguration wird mit den Werten der XML-Datei ersetzt, die zum Server passt.

Wichtig: Wenn DNS-Einträge direkt über YaST geändert werden, dann werden alle IP-Schnittstellen neu gestartet, was einen Ausfall des Systems zur Folge hat!

6.2 Verwenden des OpenScape 4000 Plattform Administration-Portals

6.2.1 Ändern der IP-Adresse des Kunden-LAN

6.2.1.1 OpenScape 4000, Plattform Administration (Portal)

Zum Ändern der IP-Adresse des OpenScape 4000 Plattform Administration-Portals navigieren Sie zu **OpenScape 4000 Plattform Administration (Portal) > System > LAN-Assistent** und ersetzen Sie den Eintrag im Feld **IP-Adresse des Portals** durch die neue IP-Adresse.

Klicken Sie dann auf **Next** (Weiter) und anschließend auf **Submit** (Abschicken).

Wichtig: Im Falle einer Duplex- oder einer Geo Separated Duplex-Bereitstellung wird Linux auf dem **active node** neu gestartet.

6.2.1.2 Ändern der IP-Adresse des OpenScape 4000 Assistant

Zum Ändern der IP-Adresse des OpenScape 4000 Assistant navigieren Sie zu **OpenScape 4000 Plattform Administration (Portal) > System > LAN Configuration (LAN-Konfiguration) > System** und ersetzen Sie die

vorhandene IP-Adresse des OpenScape 4000 Assistant durch die neue IP-Adresse.

Klicken Sie dann auf **Next** (Weiter) und anschließend auf **Submit** (Abschicken).

Wichtig: Im Falle einer Duplex- oder einer Geo Separated Duplex-Bereitstellung muss der openais-Dienst neu gestartet werden, um die neue IP zu aktivieren.

6.2.1.3 Ändern der IP-Adresse des OpenScape 4000 CSTA

Zum Ändern der IP-Adresse des OpenScape 4000 CSTA navigieren Sie zu **OpenScape 4000 Plattform Administration (Portal) > System > LAN Configuration (LAN-Konfiguration)> System** und ersetzen Sie die vorhandene IP-Adresse des OpenScape 4000 CSTA durch die neue IP-Adresse.

Klicken Sie dann auf **Next** (Weiter) und anschließend auf **Submit** (Abschicken).

Wichtig: Im Falle einer Duplex- oder einer Geo Separated Duplex-Bereitstellung muss der openais-Dienst neu gestartet werden, um die neue IP zu aktivieren.

6.2.2 Ändern der Atlantic-Schnittstelle

Anmerkung: Die Atlantic-Schnittstelle kann nur ohne Unterbrechung des Telefonbetriebs geändert werden, wenn die Zielschnittstelle bereits mit der IP 0.0.0.0/0 konfiguriert ist.

Navigieren Sie zu **OpenScape 4000 Plattform Administration (Portal) > System > LAN Configuration (LAN-Konfiguration)> System** und ersetzen Sie die vorhandene Atlantic-Schnittstelle durch die neue Atlantic-Schnittstelle.

Klicken Sie dann auf **Next** (Weiter) und anschließend auf **Submit** (Abschicken).

6.2.3 Ändern der IP-Adresse des OpenScape 4000 SoftGate

NOTICE: Dieser Abschnitt gilt für alle Einsatzmodelle mit OpenScape 4000 SoftGate.

Öffnen Sie die Seite **OpenScape 4000 Plattform Administration (Portal) > System > LAN-Konfiguration** und aktualisieren Sie die Daten entsprechend.

NOTICE: Die auf diese Weise vorgenommenen Änderungen gelten nur für den lokalen Server (SoftGate). Wenn Sie die IP-Adresse eines Access Points ändern, muss natürlich auch das Host-System entsprechend umkonfiguriert werden - siehe

dazu den Abschnitt IPDA in OpenScape 4000 V10, Band 4: IP-Lösungen, Servicedokumentation.

6.3 Recovery/Reconfiguration Tool

Wichtig: Beachten Sie, dass der Telefonbetrieb bei Verwendung des Recovery/Reconfiguration Tools unabhängig von den auf den Knoten vorgenommenen Änderungen unterbrochen wird (wie bei einem normalen Neustart des Systems).

Mit dem Recovery/Reconfiguration Tool können Sie ein bereits installiertes OpenScape 4000-System wiederherstellen oder rekonfigurieren. Dies funktioniert in jeder Bereitstellung.

Das Recovery/Reconfiguration Tool verwendet das Skript **recover-H4K.sh** im Verzeichnis `/opt/soco-common`.

Außerdem werden für die ordnungsgemäße Funktion des Tools die beiden folgenden Skripts benötigt:

- `/opt/soco-common/firstinst-netw.sh` ab Version V1.66.
Diese Version des Skripts kann mit dem Befehl `firstinst-netw.sh - v` abgerufen werden.
- `/opt/ha/bin/mount_drbd_partitions.sh` ebenfalls in der neuesten Version von OpenScape 4000 V7.

Anmerkung: Falls diese beiden Skripts nicht verfügbar sind oder nicht in den richtigen Versionen vorliegen, wird das Wiederherstellungsskript mit einer Fehlermeldung beendet.

Das Skript **recover-H4K.sh** nutzt die bereits für die Installation des Systems verwendete XML-Datei (weitere Informationen finden Sie in [Section 10.3, "XML-Konfigurationsdatei"](#)).

Die XML-Quelldatei kann bereits vorhanden sein oder bei der Skriptausführung neu generiert werden. In diesem Fall enthält sie die aktuelle Knotenkonfiguration. Ein Aktualisieren der XML-Datei ist während der Ausführung des Recovery/Reconfiguration Tools mit "vi" möglich.

Während der Wiederherstellung/Rekonfiguration werden alle Netzwerkparameter gelöscht und anhand der XML-Datei neu eingerichtet. Anschließend wird die OpenScape 4000 neu gestartet.

Szenarien

- **Wiederherstellung**

Wenn der Knoten abstürzt oder sich in einem undefinierten/falschen Zustand befindet.

Wichtig: Für eine **Wiederherstellung** sollte das Recovery/Reconfiguration Tool **nur auf dem betroffenen Knoten** ausgeführt werden.

- **Rekonfiguration**

Falls Sie bestimmte Parameter ändern müssen.

Wichtig: Für eine **Rekonfiguration** muss das Recovery/Reconfiguration Tool auf **allen Knoten** (im Falle einer Separated Duplex-Bereitstellung also beispielsweise auf dem Quorum-, dem Standby- und dem aktiven Knoten) ausgeführt werden.

6.3.1 Voraussetzungen auf dem System

Bisher war es notwendig vor der Verwebung des Recovery Tools den openais Service zu stoppen. Seit HiPath 4000 V6 R2 ist das nicht mehr nötig.

Das Skript erkennt automatisch in welchen Situationen es nötig ist die Telefonie-Services zu stoppen und wartet auf eine Bestätigung des Anwenders bevor es fortfährt:

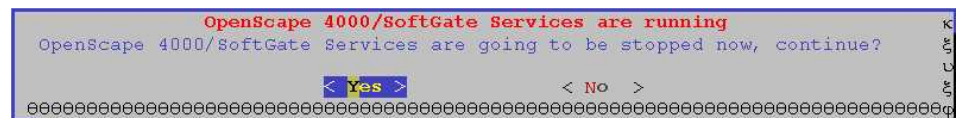


Abbildung 140: Meldung zum Stoppen der Services

Die empfohlene Reihenfolge für die Rekonfiguration von Mehr-Knoten-Systemen mit dem Recovery Tool ist die folgende:

- Duplex Knoten
 - Aktueller Standby-Knoten (auf dem ADP/OpenScape 4000 Administration Plattform (Portal)/OpenScape 4000 Assistant/OpenScape 4000 CSTA nicht laufen)
 - Aktueller aktiver Knoten
- Separated Duplex Knoten
 - Quorum Knoten
 - Aktueller Standby-Knoten (auf dem ADP/OpenScape 4000 Administration Plattform (Portal)/OpenScape 4000 Assistant/OpenScape 4000 CSTA nicht laufen)
 - Aktueller aktiver Knoten
 - Für Simplex Knoten Systeme (inklusive Simplex mit integriertem OpenScape 4000 SoftGate/Survivable OpenScape 4000 SoftGate/APE/OpenScape 4000 SoftGate) gibt es keine Rekonfigurations-Reihenfolge, da nur ein Knoten vorhanden ist.

6.3.2 Skriptausführung

6.3.2.1 Allgemeine Ausführungsschritte

Wechseln Sie zum Verzeichnis `/opt/soco-common` und rufen Sie das Skript **recover-H4K.sh** auf.

```
# cd /opt/soco-common
```

```
# ./recover-H4K.sh
```

Das Skript sucht im Konfigurationsverzeichnis `/var/opt/firstinstall` nach der XML-Datei **firstinst-netw-XXXXX.xml** mit der passenden MAC-Adresse für den Knoten.

Wenn das Skript mehrere XML-Dateien mit einer passenden MAC-Adresse findet, wird eine Liste der verfügbaren Dateien angezeigt, in der Sie die für die Konfiguration des Knotens zu verwendende Datei auswählen müssen. Die übrigen Dateien werden in das Verzeichnis `/var/opt/firstinstall/tmp` verschoben.

Mit der Option **Create from server** (Von Server erstellen) kann automatisch eine XML-Datei für den aktuellen Knoten erstellt werden. In diesem Fall werden alle aufgelisteten Dateien in das Verzeichnis `/var/opt/firstinstall/tmp` verschoben.

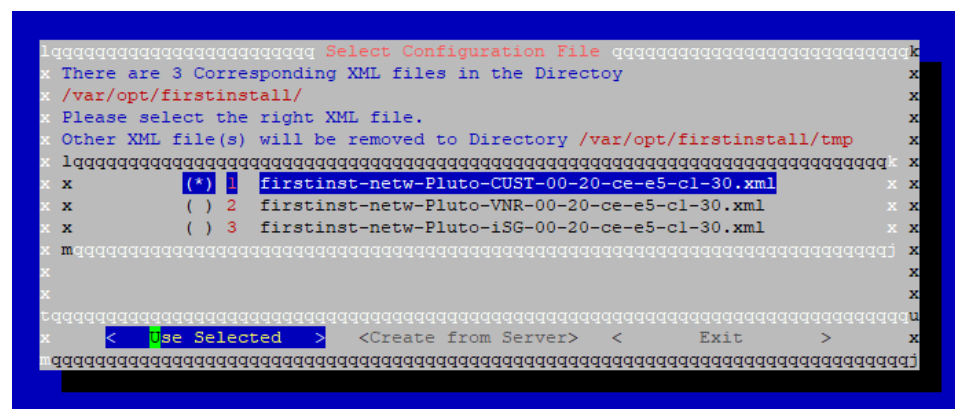
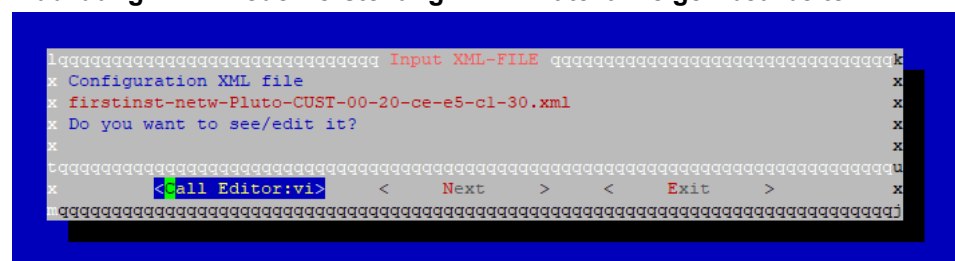


Abbildung 141: Wiederherstellung - XML-Datei auswählen

Im nächsten Bildschirm haben Sie die Möglichkeit, die Funktion **Call Editor:vi** (Editor aufrufen:vi) auszuwählen. Mit dieser Funktion kann die XML-Datei angezeigt/bearbeitet werden.

Abbildung 142: Wiederherstellung - XML-Datei anzeigen/bearbeiten



Wenn Sie **Call Editor:vi** (Editor aufrufen:vi) wählen, wird im nächsten Bildschirm eine kurze Beschreibung der "vi"-Standardbefehle angezeigt.

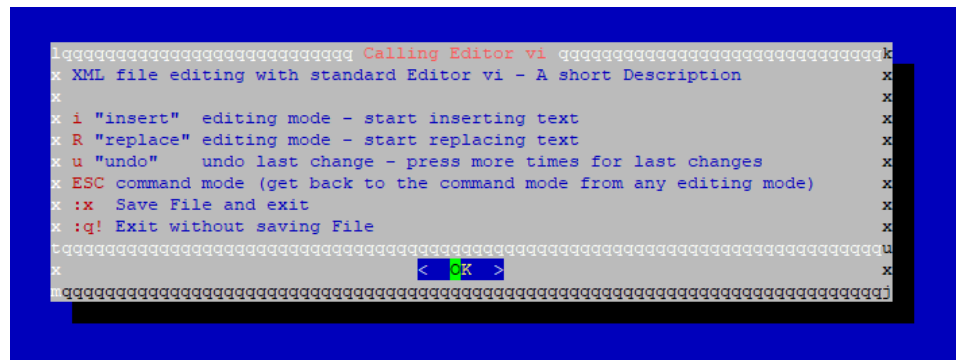


Abbildung 143: Wiederherstellung - vi-Standardbefehle

Durch Klicken auf **OK** wird die XML-Datei in "vi" geöffnet.

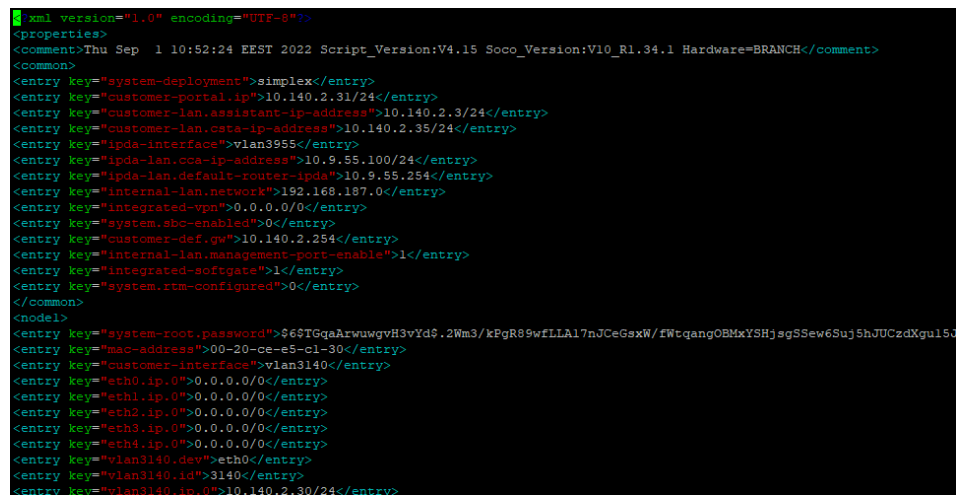


Abbildung 144: Wiederherstellung - XML-Datei im vi-Editor

Nun können Sie die XML-Datei bearbeiten.

Wichtig: Eine Änderung der Bereitstellung ist nicht zulässig. Sie können lediglich die bereits installierte Bereitstellung wiederherstellen/rekonfigurieren. Wenn die Bereitstellung in der XML-Datei geändert wurde, wird im nächsten Bildschirm eine entsprechende Meldung ähnlich der folgenden angezeigt.

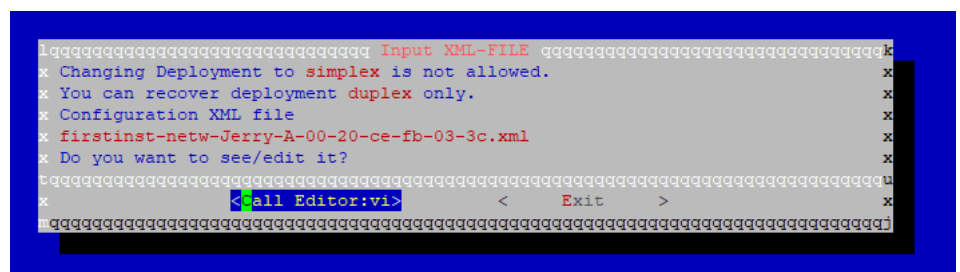


Abbildung 145: Wiederherstellung - Meldung bei geänderter Bereitstellung

Falls die Bereitstellung geändert wurde, müssen Sie die XML-Datei erneut bearbeiten und die Bereitstellung korrigieren, bevor Sie mit dem nächsten Schritt fortfahren können.

Nun wird die Konsistenz der XML-Datei geprüft. Sie können nur mit der Konfiguration fortfahren, wenn keine Fehlermeldungen angezeigt werden.

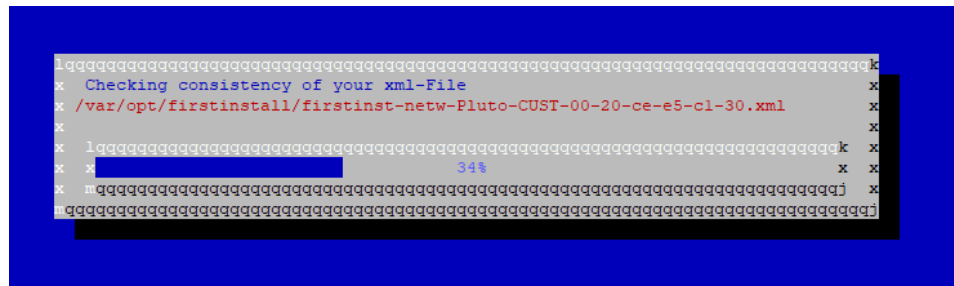


Abbildung 146: Wiederherstellung - Konsistenzprüfung der XML-Datei

Falls Warnungen angezeigt werden, können Sie entscheiden, ob Sie mit der Wiederherstellung/Rekonfiguration fortfahren oder den Vorgang abbrechen möchten.

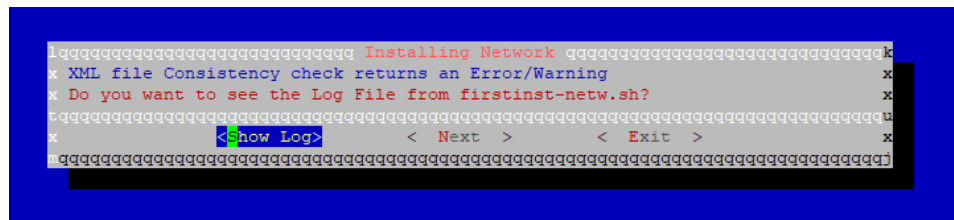


Abbildung 147: Wiederherstellung - Konsistenzprüfung mit Fehler-/Warnmeldung

In der Protokolldatei werden weitere Informationen zu den Fehlern/Warnungen angezeigt.

Wenn die Protokolldatei Fehlermeldungen enthält, müssen Sie die XML-Datei entsprechend korrigieren.

Enthält sie keine Fehlermeldungen, sondern lediglich Warnmeldungen, können Sie auf **Next** (Weiter) klicken und den Vorgang fortsetzen.

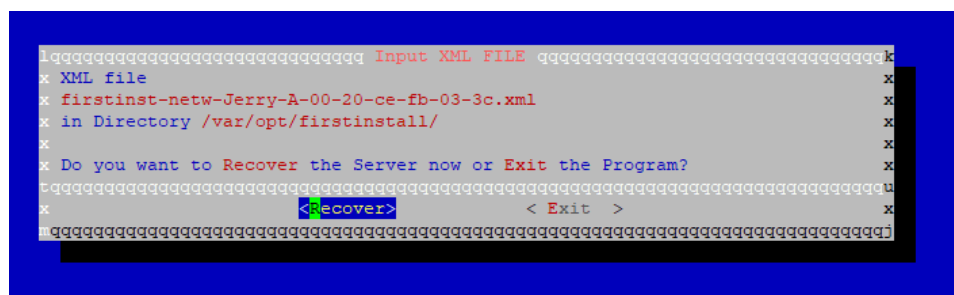


Abbildung 148: Wiederherstellung - Wiederherstellung starten

Für Einzelknoten-Bereitstellungen fahren Sie in [Section 6.3.2.2, "Einzelknoten-Bereitstellungen"](#) fort.

Im Falle einer Mehrknoten-Bereitstellung (z. B. Duplex oder Separated Duplex) fahren Sie bitte in [Section 6.3.2.3, "Mehrknoten-Bereitstellungen"](#) fort.

6.3.2.2 Einzelknoten-Bereitstellungen

- Knotenverbindung über Netzwerk - SSH

Im Falle einer Netzwerk/SSH-Verbindung mit dem Knoten wird die Verbindung beim Löschen/Rekonfigurieren der Netzwerkparameter für einige Minuten unterbrochen. Die für die Wiederherstellung der Verbindung angezeigte IP-Adresse wird der Customer LAN-Konfiguration in der XML-Datei entnommen.

Wählen Sie **Yes** (Ja), um fortzufahren.

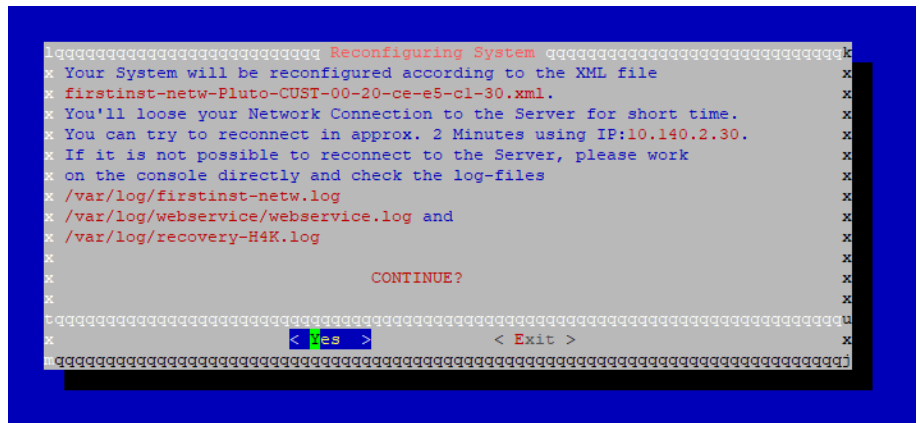
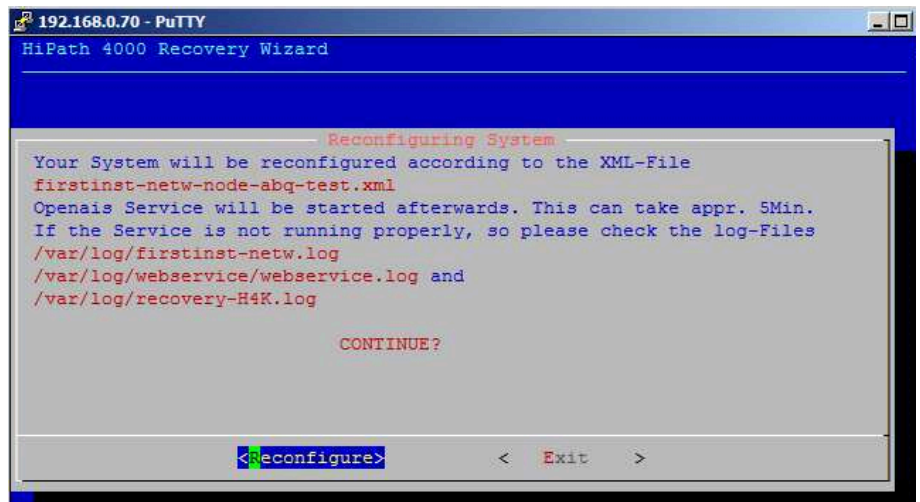


Abbildung 149: Wiederherstellung - Alle Dienste anhalten

- Direkte Konsolenverbindung

Wenn Sie direkt an der Konsole arbeiten, wird anstelle des oben dargestellten Bildschirms der folgende Bildschirm angezeigt.

Wählen Sie **Reconfigure** (Rekonfigurieren), um fortzufahren.



Wiederherstellung - Wiederherstellung/Rekonfiguration starten

Das Skript prüft, ob alle Dienste auf dem lokalen Knoten angehalten wurden. Wenn dies nicht der Fall ist, wird ein Bildschirm angezeigt, in dem Sie den Vorgang bestätigen (d. h. die Wiederherstellung/Rekonfiguration starten oder das Recovery/Reconfiguration Tool beenden) können. Wenn OpenScape

4000 SoftGate auf dem Knoten konfiguriert ist und ausgeführt wird, werden die entsprechenden Dienste ebenfalls angehalten.

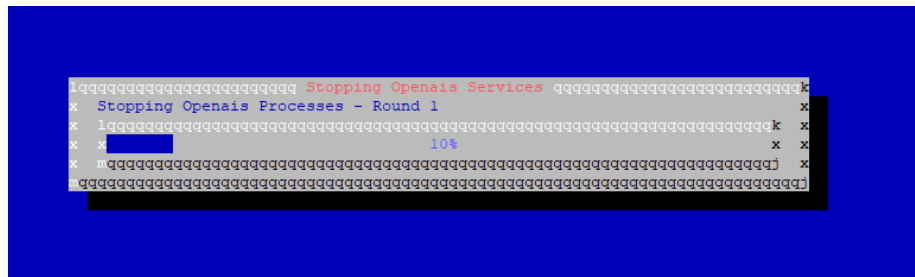


Abbildung 150: Wiederherstellung - Alle Dienste anhalten

Nach dem Anhalten der OpenScape 4000-Dienste wird der Wiederherstellungs-/Rekonfigurationsvorgang gestartet. Wenn die Dienste (vom Skript oder vom Benutzer) in 15 Minuten seit dem Zeitpunkt, zu dem sie gestoppt wurden, nicht gestartet werden, werden sie automatisch gestartet.

6.3.2.3 Mehrknoten-Bereitstellungen

Im Falle eines Mehrknotensystems müssen beim Klicken auf **Recover** (Wiederherstellen) nach der einleitenden XML-Prüfung/Generierung noch einige weitere Schritte ausgeführt werden. Im folgenden Bildschirm müssen Sie den **Installation Type** (Installationstyp) auswählen.

Hier gibt es zwei Möglichkeiten:

- Primär

Wenn der Knoten, auf dem Sie arbeiten, künftig als primärer Knoten verwendet werden soll, müssen Sie die Einstellung **Primary** (Primär) wählen.

- Duplex-Ersetzung

Wenn das System mit dem anderen Knoten als "primärem" Knoten betrieben wird, müssen Sie auf diesem Knoten die Einstellung **Duplex Replacement** (Duplex-Ersetzung) wählen.

Wichtig: Wenn Sie die Einstellung **Primary** (Primär) wählen, obwohl der andere Knoten als primärer Knoten ausgeführt wird, kann ein irreparabler Zustand auftreten,

in dem schlimmstenfalls alle Knoten reinstalliert werden müssen.

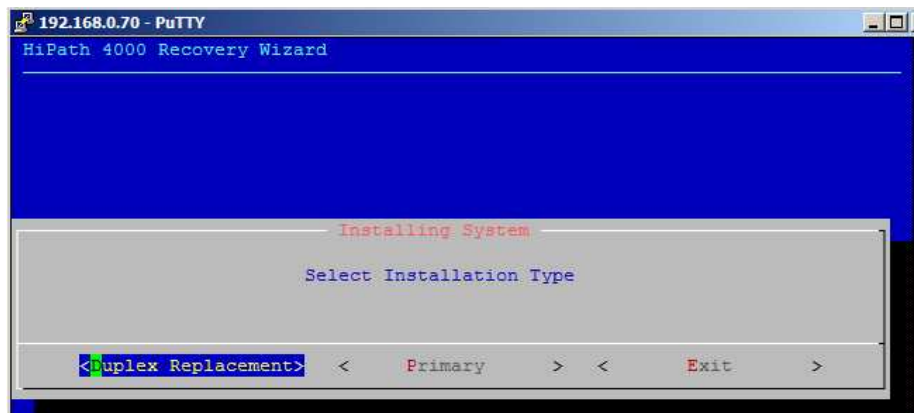


Abbildung 151: Wiederherstellung - Installationstyp für Mehrknoten-Bereitstellungen

Wenn Sie **Primary** (Primär) wählen, wird das folgende Fenster angezeigt:

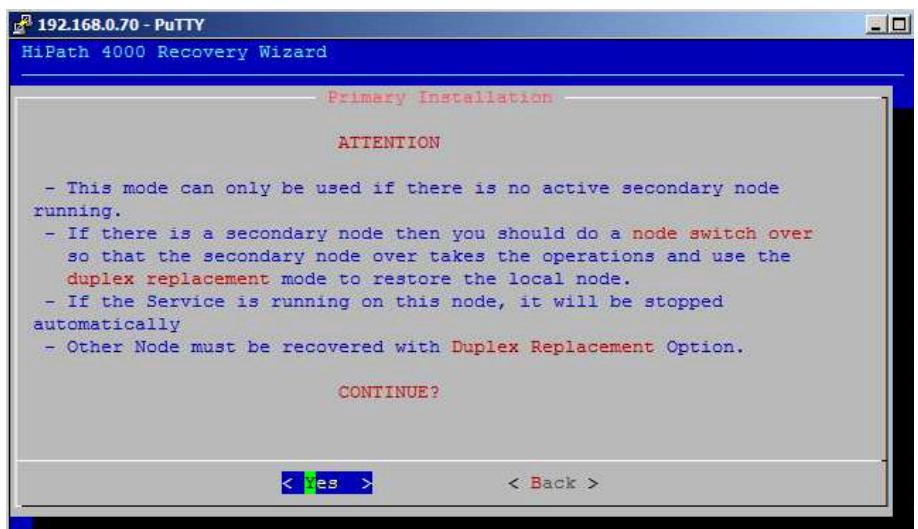


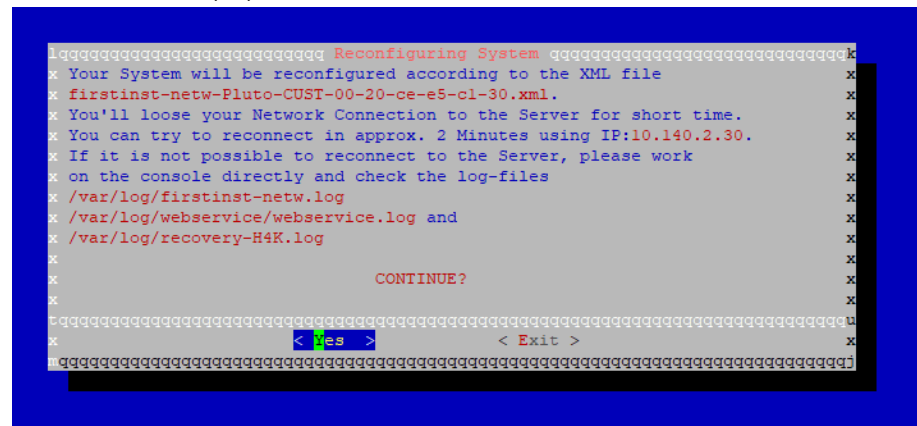
Abbildung 152: Wiederherstellung - Alle Dienste anhalten

- Knotenverbindung über Netzwerk - SSH

Im Falle einer Netzwerk/SSH-Verbindung mit dem Knoten wird die Verbindung beim Löschen/Rekonfigurieren der Netzwerkparameter für einige Minuten unterbrochen. Die für die Wiederherstellung der Verbindung

angezeigte IP-Adresse wird der Customer LAN-Konfiguration in der XML-Datei entnommen.

Wählen Sie **Yes** (Ja), um fortzufahren.



Wiederherstellung - Alle Dienste anhalten

- Direkte Konsolenverbindung

Wenn Sie direkt an der Konsole arbeiten, wird anstelle des oben dargestellten Bildschirms der folgende Bildschirm angezeigt.

Wählen Sie **Reconfigure** (Rekonfigurieren), um fortzufahren.

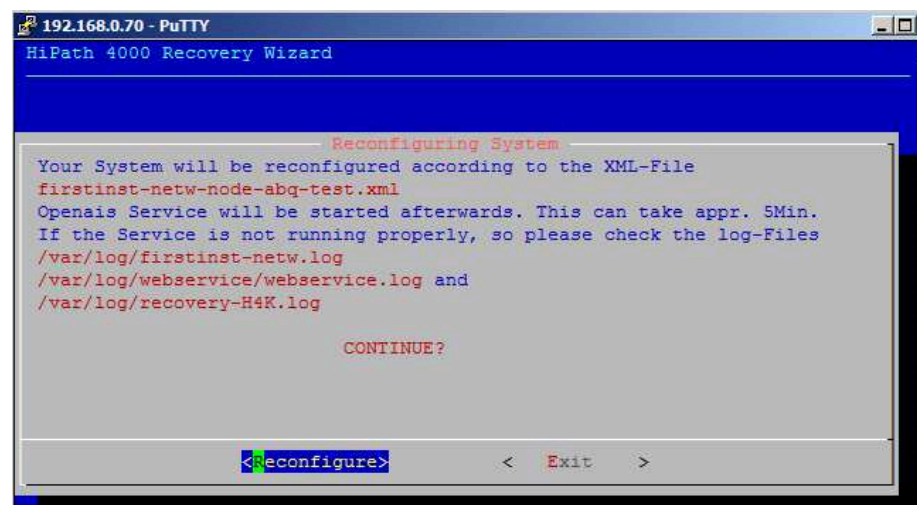


Abbildung 153: Wiederherstellung - Wiederherstellung/Rekonfiguration starten

Außerdem werden die drbd-Festplattenlaufwerke im Hintergrund synchronisiert.

Das Skript prüft, ob alle Dienste auf dem lokalen Knoten angehalten wurden. Wenn dies nicht der Fall ist, wird ein Bildschirm angezeigt, in dem Sie den Vorgang bestätigen (d. h. die Wiederherstellung/Rekonfiguration starten oder das Recovery/Reconfiguration Tool beenden) können. Nach dem Anhalten der OpenScape 4000-Dienste wird der Wiederherstellungs-/Rekonfigurationsvorgang gestartet.

Wenn die Dienste (vom Skript oder vom Benutzer) in 15 Minuten seit dem Zeitpunkt, zu dem sie gestoppt wurden, nicht gestartet werden, werden sie automatisch gestartet.

6.3.2.4 Wiederherstellung von Mehrknoten-Bereitstellungen

Um eine Systemzerstörung bei einer Duplex- oder getrennten Duplex-Wiederherstellung (Multi-Knoten-Bereitstellungen) zu vermeiden, kann das Skript recover-H4K.sh nur auf jedem Knoten einzeln ausgeführt werden und sollte in der richtigen Reihenfolge gestartet werden:

- Quorum-Knoten (GSD)
- Standby-Knoten
- Aktiver Knoten

Die Funktionalität ist abhängig von den folgenden Skripten (zusätzlich zu den aktuellen recover-H4K.sh-Abhängigkeiten):

- /opt/websevice/scripts/swupdated
- /opt/websevice/scripts/gethaipsetupentry.sh

Schritt 1. Melden Sie sich auf allen 3 Knoten an, starten Sie das Wiederherstellungsskript und wählen Sie **Einzelknoten** (wählen Sie "Nur diesen Knoten wiederherstellen"),

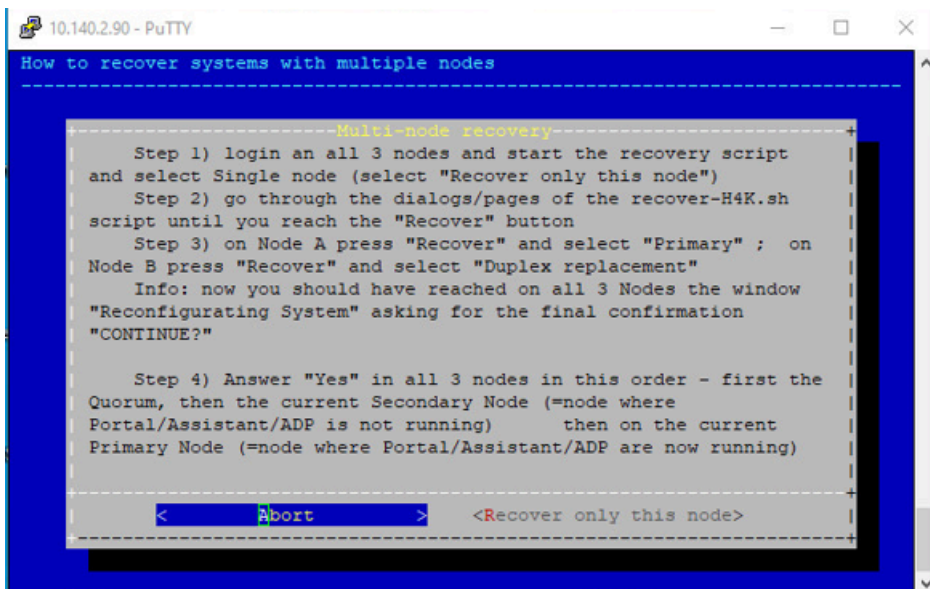


Figure 154: Reihenfolge der Knoten für die Wiederherstellung

Der Benutzer wird aufgefordert, die XML-Erstinstallationsdatei auszuwählen, die für die Wiederherstellung verwendet werden soll.

Ändern der Plattformkonfiguration

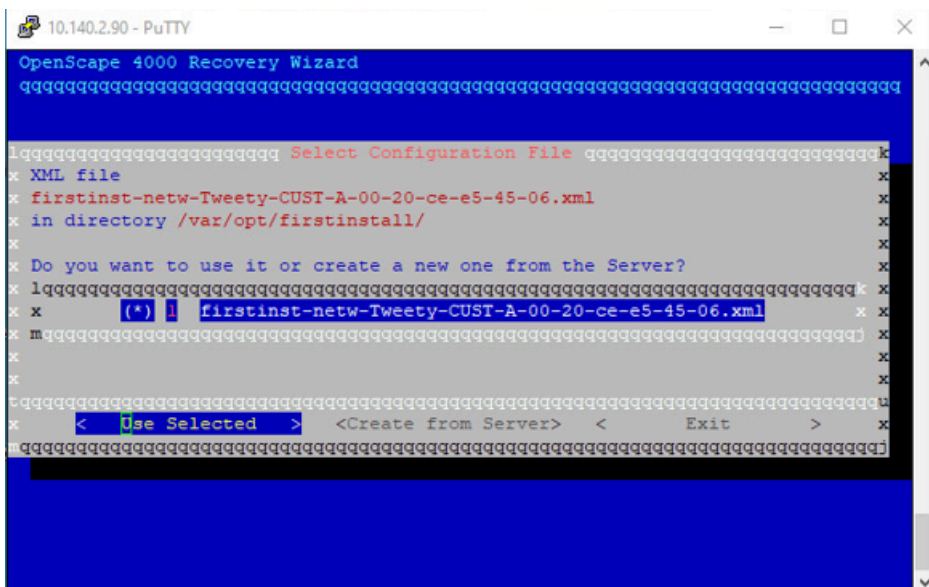


Figure 155: Wiederherstellungsassistent

Schritt 2. Gehen Sie durch die Dialoge/Seiten des Skripts recover-H4K.sh, bis Sie die Schaltfläche **"Wiederherstellen"** erreichen

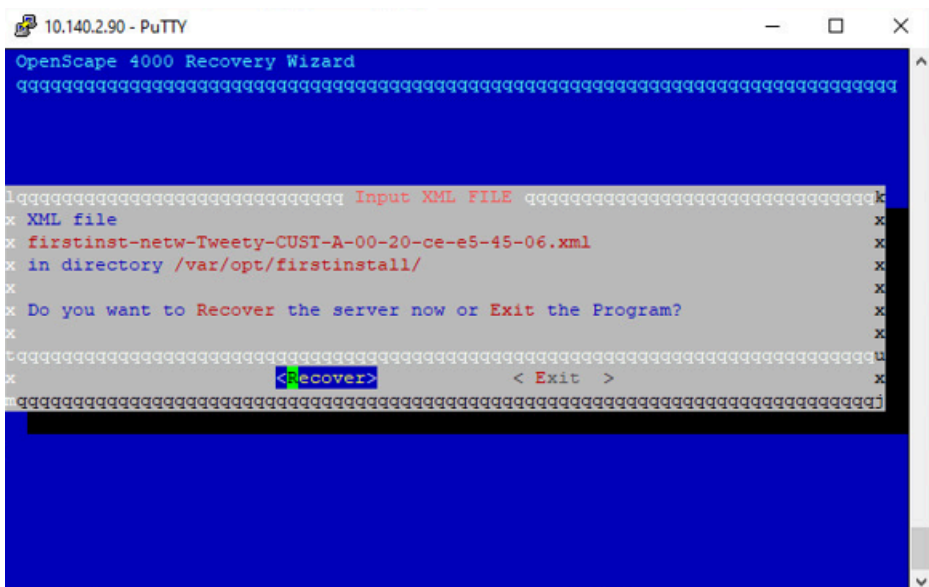


Figure 156: Wiederherstellen

Schritt 3. Auf Knoten A drücken Sie **"Wiederherstellen"** und wählen Sie **"Primär"**; auf Knoten B drücken Sie **"Wiederherstellen"** und wählen Sie **"Duplex-Ersatz"**

NOTICE: Nun sollten Sie auf allen 3 Nodes das Fenster **"System neu konfigurieren"** erreicht haben, in dem die endgültige Bestätigung **"WEITER?"** gebeten wird

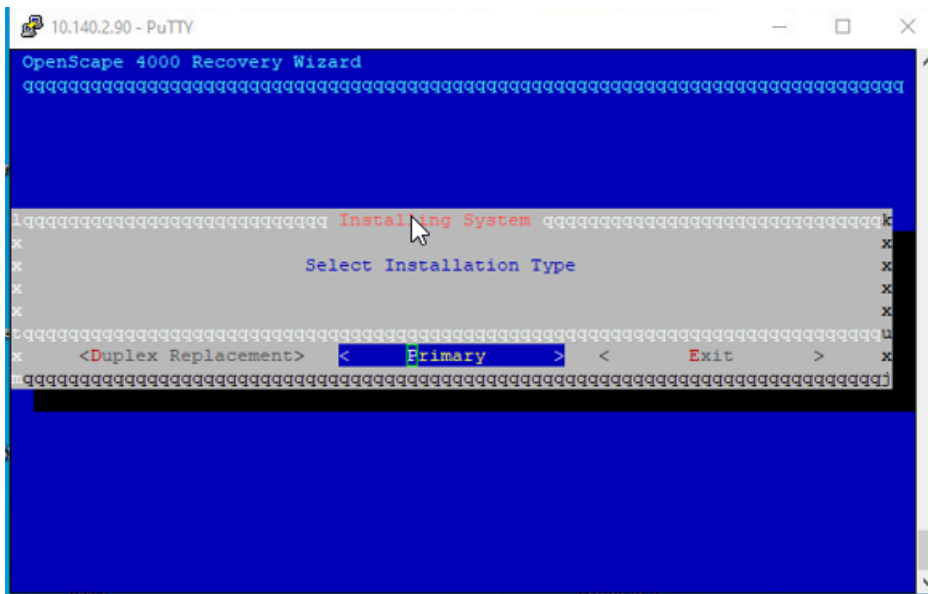


Figure 157: Wiederherstellung von Primärknoten

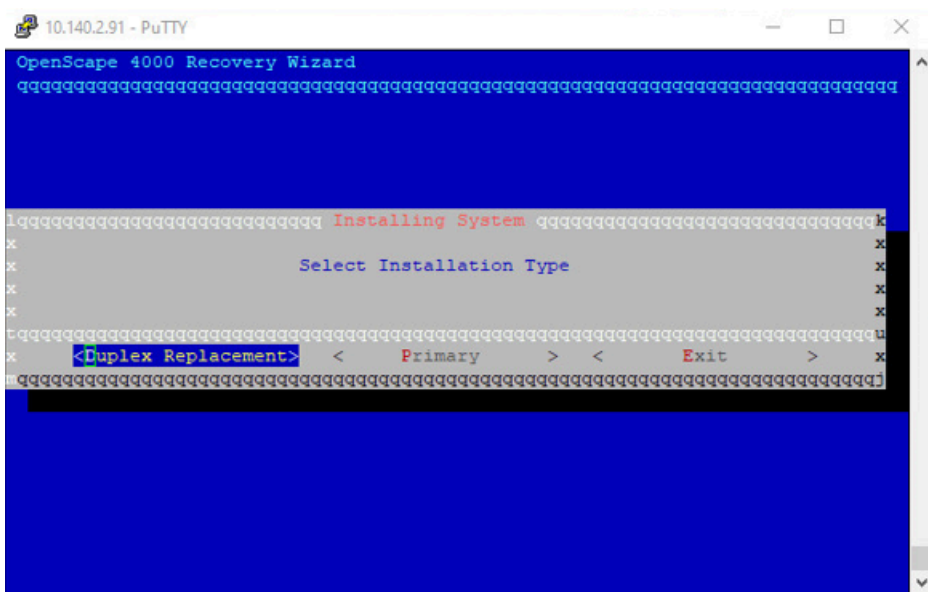


Figure 158: Wiederherstellung von Sekundärknoten

Für den Primärknoten haben wir ein Fenster **Achtung**

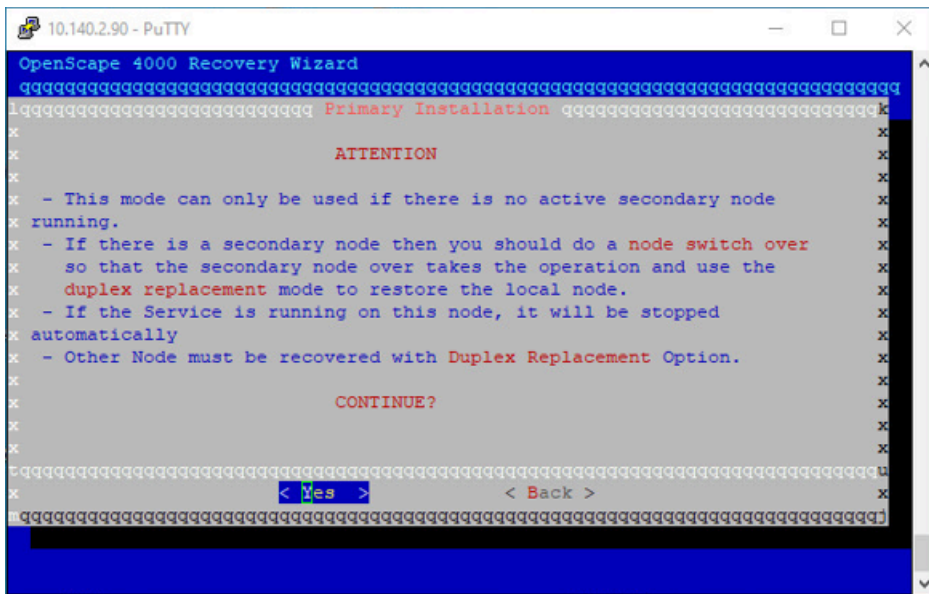


Figure 159: Achtung

Schritt 4. Antwort "Ja" in allen 3 Knoten in dieser Reihenfolge - zuerst das Quorum, dann der aktuelle Sekundärknoten (= Knoten, wobei Portal/Assistant/ADP nicht ausgeführt wird), dann auf dem aktuellen Primärknoten (= Knoten, wobei Portal/Assistant/ADP jetzt ausgeführt wird)

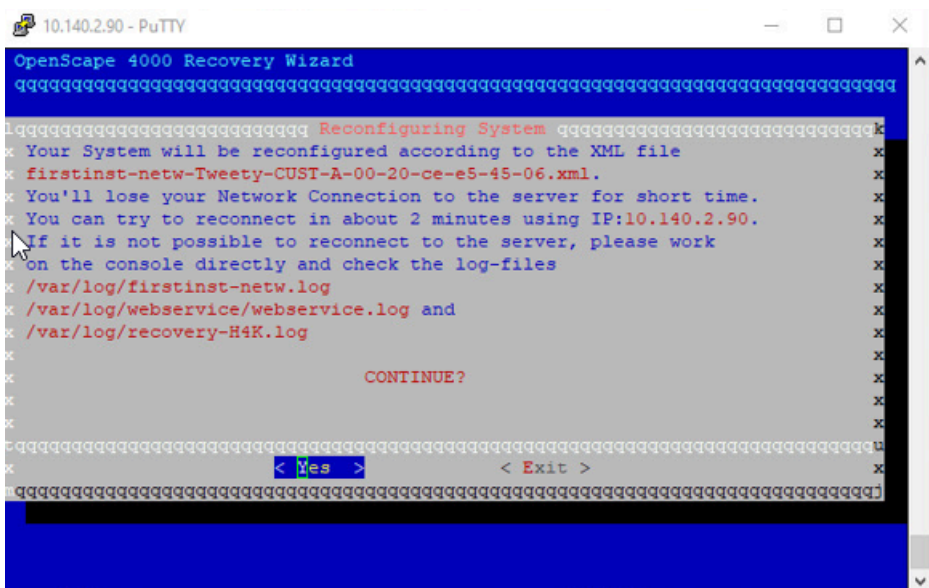


Figure 160: Systemneukonfiguration & Protokolle

Wenn kein Fehler gefunden wurde und der Benutzer fortfahren möchte, werden die OpenAIS-Dienste auf allen Knoten in der richtigen Reihenfolge angehalten (zuerst der Quorumsknoten, sofern vorhanden, dann Standby-Knoten, dann aktiver Knoten). Wenn die Dienste (vom Skript oder vom Benutzer) in 15 Minuten seit dem Zeitpunkt, zu dem sie gestoppt wurden, nicht gestartet werden, werden sie automatisch gestartet.

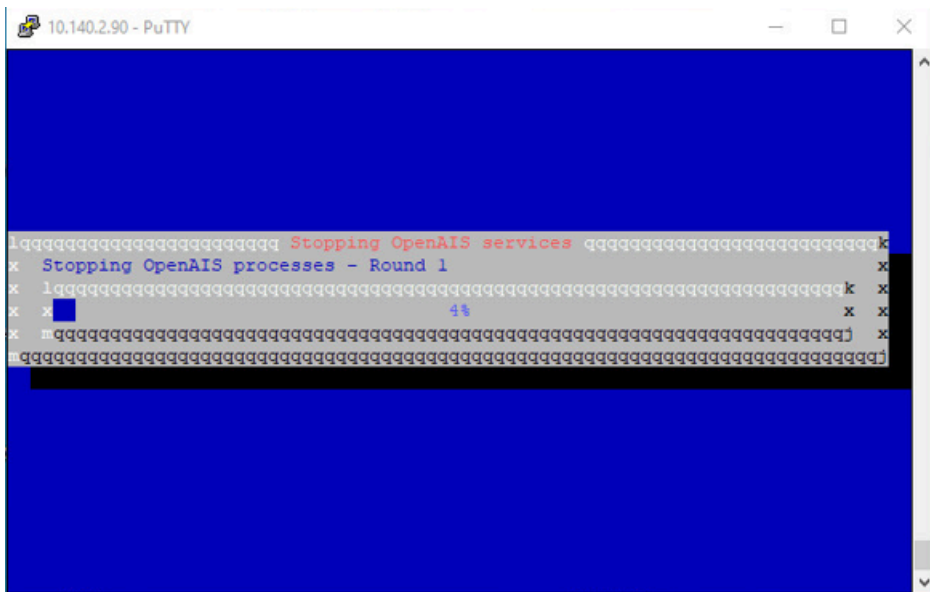


Figure 161: Stoppen von OpenAIS-Diensten

Bei der Fehlerbehebung sind die zu überprüfenden Protokolle:

- /var/log/firstinst-netw.log
- /var/log/webservice/webserive.log
- /var/log/recovery-H4K.log

6.4 Recover/Reconfiguration Tool verwenden

6.4.1 Standard-Gateway

Verwenden Sie das Recovery/Reconfiguration Tool (siehe [Section 6.3, "Recovery/Reconfiguration Tool"](#)) auf jedem Knoten.

6.4.2 Ändern der IP-Adresse des IPDA-Netzwerks

Anmerkung: Dieses Thema gilt für beide Fälle (Ändern der IP-Adresse im selben Netzwerk oder in unterschiedlichen Netzwerken), da das Ändern der CCA/CCB-Adressen in beiden Fällen eine Unterbrechung des Telefonbetriebs verursacht.

Schritt 1:

Wenn Sie die IP-Adressen durch **IP-Adressen desselben Netzwerks** (Subnetzes) ersetzen möchten, ändern Sie die RMX-Konfiguration mit AMO-Befehlen für CCA, CCB, "direct link" Access Points/OpenScape 4000 SoftGates und alle anderen erforderlichen IP-Adressen (z. B. STMI4).

Wenn Sie die IP-Adressen durch **IP-Adressen eines anderen Netzwerks** (Subnetzes) ersetzen möchten, müssen Sie die Änderungen auch für "networked" Access Points/OpenScape 4000 SoftGates vornehmen.

- Ändern Sie die IP-Adressen von CCA/CCB mit AMO SIPCO.
- Ändern Sie die IP-Adressen der Access Points mit AMO UCSU.
- Ändern mit Signalisierungs-IP-Adressen mit AMO APRT.
- Aktualisieren Sie die Konfiguration mit AMO UPDAT.

Schritt 2: : (oder alternative AMO USSU, Paramter UPDATAP verwenden)

Ändern Sie die Konfiguration auf jedem NCUI über V24.

Ändern Sie anschließend die Daten des Access Points/OpenScape 4000 SoftGate mit dem OpenScape 4000 Plattform Administration-Portal:

Rufen Sie die Seite **OpenScape 4000 Plattform Administration (Portal) > System > LAN Configuration (LAN-Konfiguration)** auf und nehmen Sie die erforderlichen Änderungen vor.

Nachdem Sie die Schritte 1 und 2 ausgeführt und sich vergewissert haben, dass alle Änderungen vorgenommen wurden, führen Sie Schritt 3 aus.

Schritt 3:

Verwenden Sie das Recovery/Reconfiguration Tool (siehe [Section 6.3, "Recovery/Reconfiguration Tool"](#)) auf jedem Knoten.

Anmerkung: Es wird mindestens ein Softrestart benötigt um die HSR-Verbindung herzustellen (wenn das Recovery/Reconfiguration Tool bereits einen automatischen Softrestart durchgeführt hat, muss keiner mehr initiiert werden).

6.4.3 Ändern von Corosync-Hostname und -IP-Adresse

Verwenden Sie das Recovery/Reconfiguration Tool (siehe [Section 6.3, "Recovery/Reconfiguration Tool"](#)) auf jedem Knoten.

6.4.4 Atlantic-Schnittstelle

Wenn die IP-Adresse der neuen Schnittstelle, die Sie verwenden möchten, noch nicht als 0.0.0.0 /0 konfiguriert ist, müssen Sie sie mit dem Recovery/Reconfiguration Tool ändern.

6.4.5 Änderungen an OpenScape 4000 SoftGate / Enterprise Gateway

NOTICE: Dieser Abschnitt gilt für alle Einsatzmodelle mit OpenScape 4000 SoftGate.

Wenn Sie die

- physikalische LAN-Schnittstelle ändern (z. B. von eth0 in eth1)

oder

- der physikalischen Schnittstelle eine IP-Adresse aus einem anderen Subnetz zuweisen möchten,

müssen Sie das Recovery/Reconfiguration Tool verwenden (siehe [Abschnitt 6.3, "Recovery/Reconfiguration Tool"](#)).

Die Konfiguration der LAN-Redundanz für SoftGate / EntGW WAN oder Signaling Survivability ist über das Portal nicht möglich. Verwenden Sie den **XML-Konfigurationsdateigenerator**, um das Bonding während der Installation zu konfigurieren, und weisen Sie dann das Bonding als Schnittstelle zu, die anstelle des eth verwendet werden soll.

Wenn das SG bereits installiert ist, können Sie das Bonding über das Tool „**recover-H4K.sh**“ konfigurieren und es anschließend über das WBM zuweisen.

NOTICE: Die auf diese Weise vorgenommenen Änderungen gelten nur für den lokalen Server (SG / EntGW). Wenn Sie die IP-Adresse eines Access Points ändern, muss natürlich auch das Host-System entsprechend umkonfiguriert werden - siehe dazu den Abschnitt IPDA in OpenScape 4000 V10, Band 4: IP-Lösungen, Servicedokumentation.

NOTICE: Das Recovery/Reconfiguration Tool kann auch verwendet werden, um andere IP-Adressen am SoftGate zu ändern (z. B. Assistant / CSTA).

7 Lizenzierung

Wichtig: Siehe OpenScape 4000 Assistant/Manager V8, Lizenzverwaltung, Administratordokumentation für detaillierte Informationen zur Lizenzierung der OpenScape 4000-Software. Alle Dokumente, die in E-Doku zur Verfügung stehen, stehen auch im Unify Partner Portal zur Verfügung. Wenn Sie keinen Zugriff auf E-Doku haben, verwenden Sie bitte das Partner Portal.

7.1 Übersicht

Ab HiPath 4000 V6 basiert das Lizenzkonzept auf dem **HiPath License Management (HLM)**. Die SIM Karte wird nicht mehr benötigt.

Für die älteren OpenScape 4000 Systeme (V5 und niedriger) wird die Lizenzierung nicht verändert.

Anstelle der MAC-Adresse werden die Lizenzen für Advanced Locking Identifier (ALI) gesperrt. Diese ID ist eine vom zentralen Lizenzagenten (Central License Agent, CLA) auf Basis der Systemkonfiguration generierte Textzeichenfolge. Der CLA verwendet folgende Konfigurationsparameter des Systems, um ALI zu generieren:

Hostname

IP-Adresse des Hosts

Gateway-IP-Adresse derselben Netzwerkschnittstelle wie die Host-IP-Adresse

Primäre DNS-IP-Adresse

Zeitzone (GMT-Versatz)

Alle oben angezeigten Elemente sind für die Generierung der ALI-Zeichenfolge obligatorisch. Wenn einige der Parameter nicht konfiguriert sind, kann die ALI nicht generiert werden.

Ab V8 sind die Trunks ohne die Lizenzgebühr. Dies bedeutet, dass der RMX die Konfiguration der Amtsleitungen nicht in Anzahl der verwendeten FLEX-Lizenzen zählt.

Die Anzahl der von Trunks verwendeten B-Kanäle wird jedoch weiterhin von OpenScape 4000 Manager als Anzahl der verwalteten Ports gezählt. Dies bedeutet, dass die Anzahl der verwalteten Ports pro V8-System (für OpenScape 4000 Manager erforderlich) genauso wie in V7 gezählt wird.

Welche Lizenzen es im einzelnen gibt, entnehmen Sie bitte der Vertriebsinformation zu OpenScape 4000 V10.

Beim Erstkonfigurieren mit dem Portal wird automatisch eine "grace period" Lizenz erzeugt. Diese hat eine Gültigkeit von 30 Tagen.

Eine Kundenlizenz muss mit Angabe der MAC Adresse (z.B. eth0 der DSCXL2 Baugruppe/EcoServer) und Anlagennummer im CLS erzeugt werden. Dort gibt man die Anzahl der gewünschten Lizenzen an. Die so erzeugte ".lic Datei" kann im OpenScape 4000 Assistant mit Hilfe der Applikation "Lizenzverwaltung" eingespielt werden. Der OpenScape 4000 Assistant erzeugt daraus ein Codew für das RMX.

Im OpenScope 4000 Assistant können im Menü **Zugangsverwaltung > Lizenzverwaltung** Lizenzen eingespielt bzw. angezeigt werden. Mit der Schaltfläche **Durchsuchen** können Sie auf ihrem PC bzw. Laufwerken das Lizenzfile suchen und auswählen. Dann bestätigen Sie Ihre Auswahl mit **Upload license** (Lizenz hochladen). Damit wird die Lizenzdatei in das vordefinierte Verzeichnis kopiert.

Informationen über die Anzahl der gekauften, benutzten, freien und gesperrten Lizenzen bekommen Sie nach wie vor auch im AMO CODEW.

Mehr Informationen über die Lizenzverwaltung finden Sie in der Online-Hilfe oder in der Administratordokumentation **OpenScope 4000 Assistant/Manager, Lizenzverwaltung**.

Für mehr Informationen zur Lizenzverwaltung siehe Partner Portal: <https://enterprise-businessarea.unify.com/hlm/default.aspx>

Für mehr Informationen über den zentralen Lizenzserver siehe Partner Portal: <https://www.central-license-server.com/license-management/session/login.htm>

7.2 Übergangszeit und Installation der Lizenzdatei

Nach der erfolgreichen Erstinstallation des OpenScope 4000 Assistant beginnt die 30-tägige Lizenzübergangszeit.

Informationen zur verbleibenden Übergangszeit finden Sie im OpenScope 4000 Assistant unter:

Zugangsverwaltung > Lizenzverwaltung

OpenScope 4000 System		SLES Upgrade Protection	
License Version	V10 (Grace Period)	Used value	Validity
Advanced Locking ID(Simba-IntegratedSOS)	QMMLARJ6Z7A7TRP7RVFNH-	1	30 days
Used Network Management Ports	0	Details of SLES Upgrade Protection license count	
		OpenScope 4000 Host system	1
		CC-AP for AP-Emergency (VGA units)	0
		Selfgate (including OpenScope Access)	0
		STMX Host	0
		OpenScope Enterprise Gateway	0

OpenScope 4000 SMAX		Used Value	
System Number	N/A	L3198G05E2X00000	Expired
Support contract			
File	12000	0 (counted at: Tue Oct 18 09:25:17 2022)	30 days
TSM (enabling Uplink, USDM, Cordless, PSM, PSM devices)	12000	0 (counted at: Tue Oct 18 09:25:17 2022)	30 days
OpenScope Module	12000	0	30 days
Unity Phone	0	0	30 days
Duplex	Yes	Yes	30 days

Abbildung 162: OpenScope 4000 Assistant - Installierte Lizenzdaten anzeigen

Fügen Sie in der OpenScope 4000 Assistant-Firewall eine Ausnahme für die Verbindung mit Expert Access hinzu:

Basis Administration > Webmin > Abschnitt WAN Configuration > Firewall > Neue Einträge für CLAN Host / Netz

In RMX können Sie die verbleibende Übergangszeit mit DIS-CODEW ; überprüfen.

Die Lizenz ist der Anlagennummer zugeordnet. Diese ist im Namen der Lizenzdatei angegeben.

Vor dem Importieren der Lizenz muss die Anlagennummer mit AMO ANUM konfiguriert werden.

Wichtig: Dieser Schritt kann nur ein Mal ausgeführt werden! Die konfigurierte Anlagennummer kann aus Sicherheitsgründen nicht geändert werden. Gegebenenfalls müssen Sie eine neue Nummer generieren.

Lizenzierung

Lizenz für OpenScape 4000 SoftGate and OpenScape Enterprise Gateway installieren

EINR-ANUM:TYP=ANLNUM,MODUL=A1,ANLNUM=Anlagennummer;

EXEC-UPDAT:MODUL=A1,SUSY=ALL;

Nun kann die offizielle Lizenz aktiviert werden.

Importieren Sie die offiziellen Lizenzdateien über das Lizenzmanagement des OpenScape 4000 Assistant:

Lizenzverwaltung > Browse... > Lizenzdatei auswählen > Lizenz hochladen

Wichtig: In Mehrknoten-Bereitstellungen sollten die Lizenzen sowohl für den aktiven als auch für den Standby-Knoten importiert werden!

Nach ca. 15 bis 20 Minuten wird eine automatische CODEW-Generierung gestartet.

Anschließend können Sie die Gültigkeit wie zuvor beschrieben überprüfen.

7.3 Lizenz für OpenScape 4000 SoftGate and OpenScape Enterprise Gateway installieren

Wichtig: Die OpenScape Access/EcoBranch-Module sind durch die normale Flex-Lizenz abgedeckt!

Die Lizenz kann vom CLS-Server heruntergeladen werden.

Nach dem einspielen der Lizenz liegt diese im Verzeichnis `opt/cla/license`.

Sie haben zwei Möglichkeiten zum Einspielen der Lizenz:

1) Lizenz einspielen mittels CLM (Customer License Manager).

CLM kann auf einem anderem Rechner im Netz oder nach der CLA-Installation auf dem lokalem Host installiert werden.

2) Alternativ kann die Lizenz auch durch Kopieren des Lizenzfiles in das CLA-Import-Verzeichnis `opt/cla/import` importiert werden.

Wenn die Lizenz in das CLA-Import-Verzeichnis kopiert wird, wird sie aus dem Import-Verzeichnis gelesen, geprüft und dann im Verzeichnis `opt/cla/license` abgelegt. Im Import-verzeichnis wird das Lizenzfile dann gelöscht.

3) Ab V10R1 kann die Lizenz über das webbasierte Management installiert werden (Konfiguration - > Grundeinstellungen -> Lizenzimport).

Nach dem Laden der Lizenzdatei wird eine Bestätigungsmeldung angezeigt, die bestätigt, dass die Datei ordnungsgemäß importiert wurde. Der Status kann auf der Lizenzinformationsseite eingesehen werden. Das Einrichten einer neuen Lizenzierungssitzung kann einige Zeit in Anspruch nehmen.

Für integriertes SoftGate auf Enterprise GW verwenden Sie das WBM von Enterprise Gateway selbst, um die SoftGate-Lizenzdatei hochzuladen.

Wichtige Hinweise

- Die „Locking ID“ wurde durch die „Advanced Locking ID“ ersetzt. Die Zeichenfolge wird nun aus mehreren Parametern anstelle der IP-Adresse

generiert. Die "Erweiterte Sperr-ID" finden Sie im webbasierten Management oder im Gateway Dashoboard (Konfiguration -> Grundeinstellungen -> Lizenzinformationen).

- Mit dem Start des OpenScape 4000 SoftGates wird die Grace-Period von 30 Tagen automatisch aktiviert, wenn die Lizenz noch nicht eingespielt ist.
- Wenn innerhalb der Grace-Period von 30 Tagen keine gültige Lizenz aktiviert wird, kann das OpenScape 4000 SoftGate nicht mehr administriert werden.
- Ist bereits lokal ein CLM installiert, bevor der CLA installiert wird, dann legt die CLA-Installation keinen CLA-Admin-Account an! In diesem Fall entweder nur den lokalen CLM (ohne Account) verwenden, oder mittels lokalem CLM einen Account anlegen (Details siehe CLM-Handbuch).
- Wenn das integrierte SoftGate (iSG) konfiguriert ist, ist keine sekundäre SLES-Update-Schutzlizenz im Host erforderlich, aber für den iSG wird dennoch eine normale SoftGate Base-Lizenz benötigt.
- Wenn ein integriertes SoftGate (iSG) auf RMX gelöscht oder nicht konfiguriert ist, ist das Deaktivieren über das Portal erforderlich, um den SLES-Update-Schutz genau und synchronisiert zu halten.

7.4 OpenScape 4000 Appliance Software Lizenz JeOS

7.4.1 Betriebssystem SUSE Linux Enterprise JeOS für OpenScape 4000

Das SUSE Linux Enterprise JeOS (Just enough Operating System basierend auf SLES 15 SP3) wird als Betriebssystem für folgende Lösungskomponenten verwendet:

- OpenScape 4000 Communication Server (Simplex, Duplex und Separated Duplex)
- OpenScape 4000 SoftGate Applikation mit oder ohne AP-Emergency Software
- OpenScape Enterprise Gateway Applikation mit oder ohne AP-Emergency Software
- OpenScape Access 500/OpenScape 4000 EcoBranch mit oder ohne AP-Emergency Software
- AP-Emergency Server für IP Access Points (AP3700 IP)
- Survivable-Bereitstellungen
- STMIX

Das Betriebssystem SLES 15 SP3 JeOS wird mit den zuvor aufgeführten OpenScape 4000 Lösungskomponenten als Software Appliance Model vermarktet.

Die SLES 15 JeOS Betriebssystem-Software und Korrekturen (Fixed Release, Hot Fixes,...) werden auf dem Software Server bereitgestellt.

Das Betriebssystem darf nicht separat durch den Kunden bereitgestellt werden. Zusätzliche Wartungsverträge mit Novell sind nicht notwendig.

Nach 6 Jahren muss ein neuer Vertrag abgeschlossen werden, anderenfalls können Software-Fixes (Fix, Minor und Major Release) und Sicherheits-Patches für das SLES 15 JeOS nicht aktualisiert werden.

Die Lizenz-Vereinbarung ist in der EULA.

7.4.2 Grundsatz der JeOS Lizenzierung

Das von SUSE bereitgestellte Software Appliance Model für die Nutzung des Betriebssystems ist unterteilt in: Reporting und Ablauf der Lizenzen und Kontrolle.

7.4.2.1 Reporting

Wenn Sie eine OpenScape 4000 V10, SoftGate oder STMIX-Karten bestellen, wird automatisch die Bestellung einer entsprechenden Anzahl von JeOS-Lizenzen (Update Protection Keys) ausgelöst.

7.4.2.2 Ablauf der Lizenzen und Kontrolle

Die JeOS Lizenzierung für die OpenScape 4000 Familie ist so geregelt. Dass eine gemeinsame Lizenzposition das Grundsystem, den APE, die Duplexeinheit und das OpenScape 4000 SoftGate, OpenScape Access/EcoBranch abdeckt. Damit wird auch die Kontrolle für die OpenScape 4000 SoftGate Lizenz in den OpenScape 4000 Assistant des Grundsystems verlagert.

7.4.3 OpenScape 4000 - JeOS

Anmerkung: In den nachfolgenden Kapiteln wird nur die OpenScape 4000 erwähnt, Entsprechendes gilt auch für OpenScape Access/EcoBranch in Zusammenhang mit dem OpenScape 4000 SoftGate.

Ab Freigabe der HiPath 4000 V6 wird das von Novell bereitgestellte Software Appliance Model (JeOS) eingesetzt. Mit der Bestellung einer OpenScape 4000 oder eines OpenScape 4000 SoftGate wird die Royalty SLES Appliance für OpenScape 4000-Familie über SAP erfasst, sodass die Abrechnung mit Novell für diese Systeme zu einem festgelegten Zeitpunkt erfolgen kann.

Software Upgrade OpenScape 4000 V10

Es erfolgt eine Kontrolle der JeOS Lizenz durch das System. Dazu muss der JeOS Lizenzschlüssel vom CLS abgeholt und am OpenScape 4000 System eingespielt werden. Danach kann der Upgrade von HiPath 4000 V6 R1 auf OpenScape 4000 V10 durchgeführt werden. Der OpenScape 4000 Assistant erlaubt die Aktivierung der OpenScape 4000 V10 Software nur dann, wenn die JeOS Lizenz vorhanden ist. Die Restlaufzeit der JeOS Lizenz wird um die bereits genutzte Zeit ab Aktivierung der HiPath 4000 V6 R1 Software reduziert. Dadurch kann, je länger die HiPath 4000 V6 R1 bereits im Einsatz war, eine JeOS Lizenz Erneuerung anstehen. Die Restlaufzeit wird im Dashboard am OpenScape 4000 Assistant angezeigt.

Neuanlage OpenScape 4000 V10

OpenScape 4000 Bestellungen beinhalten neben den regulären Lizenzen (z. B. Flex-Lizenzen) auch die JeOS-Lizenzen. Diese werden automatisch am CLS im Lizenzfile bereitgestellt. Durch die Aktivierung der Lizenz am CLS wird

die Laufzeit der JeOS Lizenz gestartet. Damit startet der Kontrollvorgang im OpenScape 4000 Assistant.

Ablauf der JeOS Lizenz

Die JeOS Lizenz ist begrenzt auf 3 Jahre. Mit dem Ablauf der Lizenz erlischt die rechtliche Voraussetzung ein Update des Operating Systems durchzuführen.

Durch die Nachbestellung der JeOS Lizenz (siehe [Section 7.4.6.2, "Verlängerung der JeOS Lizenz um 3 Jahre"](#)) kann aber die Einschränkung aufgehoben und somit der Update durchgeführt werden.

Vereinfachung

Zur Vereinfachung der Ablauf-Szenarien wurde festgelegt, dass das OpenScape 4000 Grundsystem der Master ist.

Das bedeutet, das Ablaufdatum aller zugehörigen Steuereinheiten wie OpenScape 4000 SoftGates, Duplexeinheiten, APEs orientiert sich an dem Ablaufdatum der Grundeinheit der OpenScape 4000.

Die Anlage bestimmt, wann eine Warnung oder eine Sperrung des Systems für das Update des Operating System erfolgt. Alle an den Switch gebundenen Geräte müssen dem Upgrade folgen, obwohl deren Ablaufdatum möglicherweise noch nicht erreicht ist.

Der Vorteil liegt darin, dass nur zu einem Zeitpunkt, nämlich alle 3 Jahre, ein Update der JeOS Royalties nötig wird!

7.4.4 Central License Server (CLS)

Der CLS wird alle bereits installierten Systeme mit der OpenScape 4000 Software, auch OpenScape 4000 SoftGates mit der JeOS Lizenz nachversorgen und die Ablaufzeit aus der Aktivierung festlegen. Diese Aktion wird nur einmal ausgeführt.

Die JeOS Lizenz in den Bestellpositionen vorhanden sein. Somit enthält die Neubestellung einer OpenScape 4000 Anlage und eines OpenScape 4000 SoftGate auch die zur Ablaufkontrolle nötige JeOS Lizenz. Diese Lizenz wird mit der Laufzeit von 3 Jahren in der CLS-Datenbank abgespeichert. Alle nachfolgenden JeOS-Lizenzen für APE, Duplex oder OpenScape 4000 SoftGate werden dieser Ablaufzeit untergeordnet.

Ablaufdiagramme

- JeOS Lizenz innerhalb der Neubestellung Hardware (Beispiel):

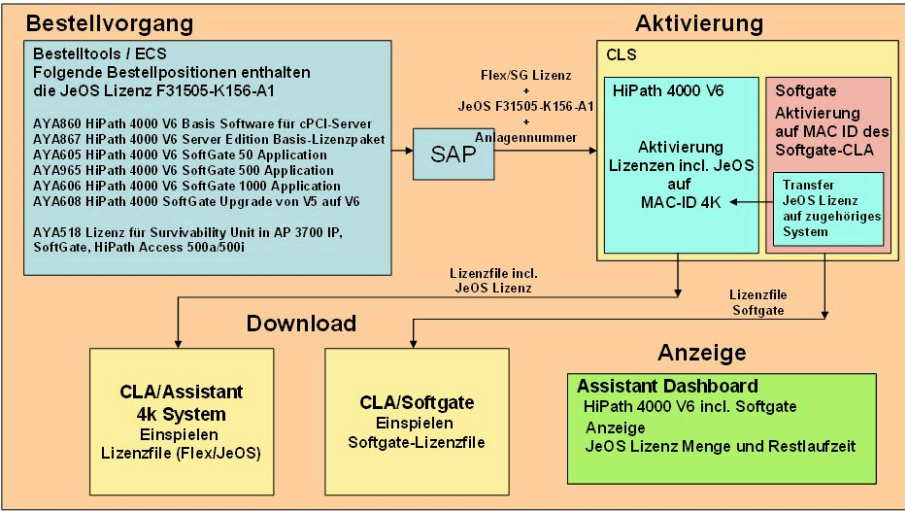


Abbildung 163: JeOS Lizenz innerhalb Neubestellung Hardware

- Nachbestellung der JeOS Lizenz (Beispiel)

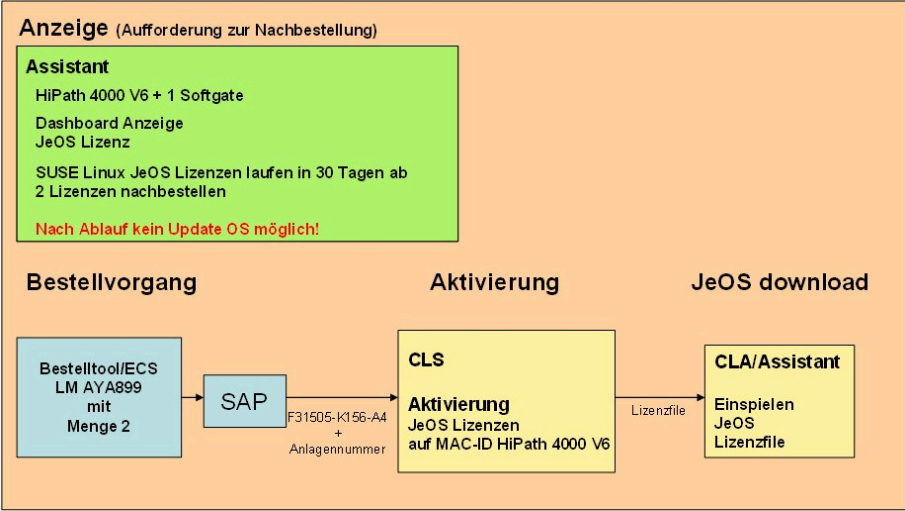


Abbildung 164: Nachbestellung JeOS Lizenz

7.4.5 Systemzustände abhängig von der Lizenz

7.4.5.1 Zustände und Hinweismeldungen

Im Dashboard des OpenScope 4000 Assistant wird je System die System Id (L31....), die Anzahl der vorhandenen JeOS-Lizenzen und die Anzahl der genutzten JeOS-Lizenzen angezeigt. Der OpenScope 4000 Assistant bereitet diese Information in einem Report am Dashboard auf. Der OpenScope 4000 Assistant gibt 6 Monate vor Ablauf der Appliance-Lizenz eine Warnung im LAP2 Dashboard aus. Der Anwender erhält 3 Monate vor Ablauf zusätzlich eine Pop-Up-Meldung beim Einloggen.

>>OpenScape 4000 V10 SLES Upgrade Protection for 3 years wird in x Tagen ablaufen, danach ist kein Update des Betriebssystems SuSE Linux möglich. Nur noch das Update von RMX, CSTA und Assistant-Hotfixes ist erlaubt.

Das LICM_SLES_UPDATE_PROTECTION sendet 30 Tage vor Ablauf der anstehende Situation einen Minor Alarm zum Logging Management. Abschließend wird ein SNMP Trap generiert.

Nach Ablauf der JeOS Lizenz (siehe [Section 7.4.3, "Vereinfachung"](#)) kann kein Update der Operation Software mehr durchgeführt werden. Der OpenScape 4000 Assistant fordert deswegen zur Erneuerung der JeOS Lizenz auf. Dabei erhält der Anwender die Information am Dashboard, wie viele Appliance-Lizenzen (JeOS) benötigt werden.

Die Anzeige unterscheidet nach folgenden Produkten:

- OpenScape 4000 Host System
- CC-AP für AP Emergency (nur IPDA)
- OpenScape 4000 SoftGate inkl. OpenScape Access und OpenScape 4000 Branch.

7.4.5.2 JeOS Verlängerung

Die Verlängerung der JeOS-Lizenzen über den Bestellvorgang erzeugt eine Lizenzdatei durch CLS, mit entsprechender Menge und einer max. Laufzeit von 3 Jahren. Die Lizenzdatei kann von der CLS-Schnittstelle heruntergeladen und auf dem CLA des OpenScape 4000 Assistant installiert werden.

7.4.6 Bestellprozess

7.4.6.1 Erstbestellung über Hardware

Die JeOS Lizenz wird in der Erstbestellung einer OpenScape 4000 V10 Anlage und OpenScape 4000 SoftGate inkl. OpenScape Access/EcoBranch unter dem jeweiligen LM geführt. Diese Lizenz läuft in 3 Jahren ab.

Weitere Details sind bereits im [Section 7.4.3, "OpenScape 4000 - JeOS"](#) beschrieben.

7.4.6.2 Verlängerung der JeOS Lizenz um 3 Jahre

Nachdem die Aufforderung am OpenScape 4000 Assistant erfolgt ist JeOS-Lizenzen aufzufrischen, kann über die Salestools die Bestellung erfolgen. Das Dashboard meldet die Summe der JeOS-Lizenzen, die erneuert werden müssen.

Anmerkung: Die Menge JeOS-Lizenzen schließt das OpenScape 4000 SoftGate mit ein.

Durch die Aktivierung der JeOS Verlängerungslizenz am OpenScape 4000 Assistant wird eine Sperre des Updates der Operating Systems aufgehoben bzw. vermieden.

7.4.7 Zusammenfassung der JeOS Aktivitäten

7.4.7.1 Erneuerung JeOS Lizenz

Der Bedarf der Erneuerung der JeOS Lizenz nach erreichter Ablaufzeit wird über die Anzeige am OpenScape 4000 Assistant gemacht. Bereits 6 Monate vor Ablauf gibt der OpenScape 4000 Assistant eine Hinweismeldung über den Ablauf der JeOS Lizenz aus.

Darüber hinaus gibt der OpenScape 4000 Assistant 1 Monat vor Ablauf der Laufzeit eine Nachricht aus, wie viele JeOS-Lizenzen bestellt werden müssen, einschließlich der OpenScape 4000 SoftGates.

Wird auf diese Meldung nicht reagiert erfolgt die Sperre der Updatemöglichkeit des Operating Systems.

Um das zu vermeiden, müssen die JeOS-Lizenzen bestellt werden. Über den Bestellvorgang werden die Lizenzen über SAP an den CLS übertragen. Nachdem diese Lizenzen bereits an den Host gebunden sind, ist eine Zuweisung der OpenScape 4000 SoftGate nicht mehr nötig. Der Service aktiviert dieses Lizenzfile und spielt es am CLA ein. Damit wird die mögliche oder anstehende Sperre des Betriebssystems behoben. Wenn jedoch die Anzahl der JeOS-Lizenzen nicht mit der gewünschten Anzahl übereinstimmt, lehnt der OpenScape 4000 Assistant die Lizenzdatei ab. OpenScape 4000 Assistant benachrichtigt über diese Situation durch eine Fehlermeldung und verweist auf die Anzahl der fehlenden JeOS-Lizenzen. Während der Lizenzmangel auftritt, kann kein Update der Betriebssystemsoftware durchgeführt werden, bis die gewünschten Lizenzen installiert sind. Das bedeutet, dass in diesem Fall eine zusätzliche Bestellung von JeOS-Lizenzen erforderlich ist.

7.4.7.2 Erweiterung um OpenScape 4000 SoftGates

Zusätzliche OpenScape 4000 SoftGates müssen wiederum 2 Lizenzschlüssel erhalten. Die JeOS Lizenz ist der MAC-ID zugehörigen OpenScape 4000 V10 zuzuordnen und für diese zu aktivieren und am CLA des OpenScape-Systems einzuspielen. Zusätzlich muss der Lizenzschlüssel für das OpenScape 4000 SoftGate aktiviert werden und am CLA der OpenScape 4000 SoftGates eingespielt werden.

8 Zeitsynchronisation

Die OpenScape 4000 Plattform ist die Zeitquelle für alle Server im Netz (z.B. OpenScape 4000 Assistant, OpenScape 4000 CSTA, ADP, CCs, Access Points, OpenScape 4000 SoftGates, CC-APs, OpenScape Access Module, Survivable OpenScape 4000 SoftGates, etc.).

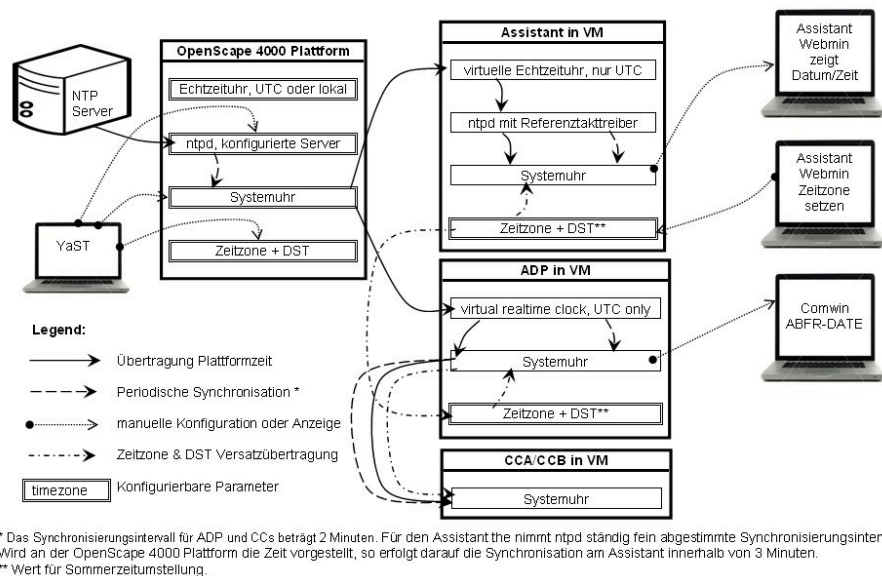


Abbildung 165: Zeitsynchronisation - Überblick

8.1 Network Time Protocol-Server

- Es muss ein NTP-Server als exakte Zeitquelle für die Zeitsynchronisation aller OpenScape 4000 Netzwerkkomponenten verwendet werden. Eine zuverlässige Zeitquelle stellt sicher, dass die Cluster-Komponenten synchronisiert bleiben und dass Software-Watchdogs anderer Komponenten nicht auf Grund von Zeitverschiebungen oder einer schlechten Zeitquelle getriggert werden. Zulässige NTP-Quellen sind direkte Verbindungen zu öffentlichen NTP-Servern oder ein lokaler NTP-Server, der eine Nebenuhr entweder vom öffentlichen NTP-Server oder einer GPS-/Atom-Uhr (falls keine Verbindung zu einer öffentlichen NTP-Infrastruktur vorhanden ist) ist.
- Fehlerhafte NTP-Synchronisationen wurden beobachtet, wenn der Kunde versucht hat einen NTP-Server mit einer schlechten Zeit-Quelle zu simulieren (z.B. unter der Verwendung von Shareware). Obwohl manche Shareware-Programme die Manipulation der Stratum-Information erlauben, ist das Stratum selbst kein Indikator für eine stabile Uhrzeit. Eine genaue Zeit-Quelle ist eine zwingende Notwendigkeit für die Stabilität der OpenScape 4000.
- OpenScape 4000 Knoten verfügen über keine geeignete Zeit und sollten nicht als NTP-Server verwendet werden.
- Alte HiPath 4000-Systeme dürfen aufgrund von Performance-Problemen mit UnixWare 7 ebenfalls nicht als NTP-Server verwendet werden.
- Systeme mit SNTP sind nur dann als Server geeignet, wenn sie mit einem Hardware-Referenztaktgeber (zum Beispiel einem GPS-Taktempfänger) verbunden sind.

- Die Hardware-Uhr im BIOS muss auf UTC und nicht auf die lokale Zeit eingestellt werden. Das muss während der Erst-Installation gemacht werden. Eine spätere Einstellung kann zu Ausfällen auf Grund von Zeitsprüngen führen.
- Die UTC-Zeit muss einmal während dem Hochlauf von Linux gesetzt werden und dann über eine verlässliche NTP-Quelle synchronisiert werden, um große Zeitsprünge nach vorne oder zurück zu vermeiden. Der NTP-Server kann in der XML-datei, die für die Erst-Installation verwendet wird, konfiguriert werden.
- Weitere Informationen [Chapter 13, "Zeiteinstellung / Zeitsynchronisation"](#).

8.1.1 Größere Vorwärts-Sprünge der Systemzeit

Größere Sprünge der Systemzeit können vom NTP-Daemon abgewiesen werden. Um solche größeren Sprünge der Systemzeit zu vermeiden, die möglicherweise abgewiesen werden, können Sie das System mit den folgenden Linux-Kommandos zwingen, sich mit der Zeit des NTP-Servers zu synchronisieren:

```
sntp -P no -r x.x.x.x
```

(x.x.x.x ist die IP-Adresse Ihres NTP-Servers)

```
hwclock --systohc --noadjfile --utc
```

Nach der Konfiguration des NTP-Servers können Sie mit dem folgenden Linux-Kommando überprüfen, ob das System mit dem NTP-Server synchronisiert wird:

```
service ntp status
```

8.1.2 Wichtige Informationen zum Einstellen oder Ändern der Uhrzeit

- Nach der Synchronisierung des Systems mit dem Remote-Zeit-Server im Anschluss an die Konfiguration des NTP-Servers (z. B. per Yast2) kann es vorkommen, dass die Uhrzeit um einen größeren Zeitschritt zurückfällt.

Bitte sorgen Sie dafür, dass alle Virtual Machines neu gestartet werden (z. B. durch einen Linux-Neustart). Andernfalls bleibt der virtuelle Realtime-Takt von OpenScape 4000 Assistant/OpenScape 4000 CSTA und ADP hängen, was zu unvorhersehbaren Ergebnissen führt.

- Wenn die Zeit auf dem NTP-Server vom ntpd lediglich um einen kleinen Zeitschritt (bis zu 60 Sekunden) zurückgesetzt wird, erfolgt die Synchronisierung automatisch. Hierzu ist es nicht notwendig, die Virtual Machines herunterzufahren oder einen Neustart durchzuführen.
- Vorwärts-Zeitschritte (manuell oder per ntpd) werden unabhängig von ihrer Größe auf allen Virtual Machines stets automatisch korrigiert.

- Wenn die Host-Zeit zurückspringt, geht das RMX-OS davon aus, dass die Hardware-Uhr defekt ist, und stoppt die Synchronisierung.

Das RMX benötigt 0-2 Minuten, um zu erkennen, dass die Host-Zeit zurückgesprungen ist.

In HISTA wird Folgendes angezeigt:

```
F8102 E8 N4856 OUT SERV A1 TIMEDATE NOT READY 10-06-25
13:05:31
```

```
ALARM CLASS:CENTRAL:028
```

```
FORMAT:0
```

```
A9001 M5 N4857 NO ACT A1 NMCALARM MAJOR ALARM ON 10-06-25
13:05:40
```

```
ALARM CLASS:CENTRAL:028
```

```
ALARM NAME:SYSTEM TIME FAILURE
```

```
FORMAT:2C
```

Es gibt zwei Möglichkeiten, dieses Problem zu beheben:

Manuell resynchronisieren (Aufruf von AMO "aendern-date")

```
REG-DATE;
```

Ausgabe verwenden von REG-DATE ;

z. B. AENDERN-

```
DATE:GMTRTG=OST, ZEITDIFF=60, MODE=NT, DSTOFFS=0 ;
```

und in das System zurückspeisen.

OpenScape 4000 Assistant erkennt den Fehler in HISTA via AFR3 und resynchronisiert RMX (durch Aufruf von "aendern-date").

Die folgenden Kommandos müssen aktiv sein, damit die Zeitänderungen wirksam werden.

```
EINSCHALTEN-AFR:LDU=AFR3,TYP=LDU&PROT;
```

```
EINSCHALTEN-SIGNL:SWITCH=ALLMSG,GER=AFR3;
```

Wenn der Fehler wie in [1](#) oder [2](#) beschrieben behoben wurde, wird in HISTA "TIMEDATE READY" und "MAJOR ALARM OFF" angezeigt.

Wichtig: AENDERN-DATE sollte nicht in Zeiten mit hohem Verkehrsaufkommen verwendet werden, da hierdurch (unter anderem) eine sofortige Aktualisierung der Uhrzeit auf allen Telefongeräten erzwungen wird. Für jedes Gerät werden in BP mehrere einzelne Meldungen generiert und diese an die Geräte übertragen. Im Falle einer großen PBX führt dies zu einem enormen Verkehrsaufkommen mit hoher Auslastung der BP und LTUs. Die Verarbeitung aller Geräte nimmt einige Minuten in Anspruch und kann andere CP-Aktivitäten behindern (Verzögerungen beim Verbindungsaufbau, ...).

8.2 Konfiguration der Zeit in allen Servern

Beim Starten aller virtuellen Maschinen wird die Systemzeit der OpenScape 4000 Plattform in allen Servern übernommen.

Die Synchronisation des OpenScape 4000 Assistant erfolgt über ntpd innerhalb von ca. 3 Minuten. Die Synchronisation des ADP erfolgt innerhalb von ca. 2 Minuten.

Überprüfen Sie im OpenScape 4000 Assistant, ob Datum und Uhrzeit korrekt synchronisiert wurden:

Basis Administration > Webmin > Systemverwaltung > Datum/Uhrzeit

Wichtig: Datum und Uhrzeit können nicht mit dem OpenScape 4000 Assistant konfiguriert werden!

8.3 Konfiguration der Zeitzonen mit OpenScape 4000 Assistant

Im OpenScape 4000 Assistant wird die Zeitzone zentral für die gesamte OpenScape 4000 einschließlich ADP, OpenScape 4000 CSTA und Host-Plattform verwaltet.

In allen diesen Subsystemen sollte dieselbe Zeitzone angezeigt werden. Eine abweichende Zeitzone kann mit dem OpenScape 4000 Assistant geändert werden (siehe [Section 8.3.1, "Einstellung von Zeitzone und Sommerzeit für OpenScape 4000 Assistant und RMX"](#)).

8.3.1 Einstellung von Zeitzone und Sommerzeit für OpenScape 4000 Assistant und RMX

Während der Installation des OpenScape 4000 Assistant wird seine Zeitzone von der OpenScape 4000 Plattform übernommen. Aber dann ist sie unabhängig von der OpenScape 4000 Plattform.

Die Einstellung der Zeitzone und der Sommerzeit erfolgt über den OpenScape 4000 Assistant.

Basis Administration > Webmin > Systemverwaltung > Zeitzone

Andere Zeitzone wählen

Konfigurierte Zeitzone	
ADP Diff. zu GMT:	GMT +03:00
Assistant Zeitzone:	Europe/Bucharest (GMT +03:00)
CSTA Zeitzone:	Europe/Bucharest (GMT +03:00)
Linux Host Zeitzone:	Europe/Bucharest (GMT +03:00)

Zeitzone einstellen

Neue Zeitzone:

Tipp: Bitte seien Sie bei der Auswahl der +/- Werte für die GMT-bezogenen relativen Zeitzone aus der Auswahlliste sehr vorsichtig. Gemäß POSIX-Standard hat die Zeitverschiebung nach Osten (GMT Offset East) einen negativen Wert und die Zeitverschiebung nach Westen (GMT Offset West) einen positiven Wert; allgemein üblich wird jedoch genau das Gegenteil erwartet. "Etc/GMT-3" entspricht zum Beispiel UTC+0300, also in östlicher Richtung relativ zu GMT. Bei den in der obigen Tabelle dargestellten "Konfigurierten Zeitzone" wird die Zeitverschiebung (Offset) auf übliche Art und Weise angegeben.

Abbildung 166: Konfigurieren der Zeitzone mit OpenScape 4000 Assistant

Sie können die Zeitzone und Sommerzeit einstellen, indem Sie die gewünschte Zeitzone aus der Liste **Neue Zeitzone** wählen und anschließend auf die Schaltfläche **Modifizieren** klicken. Die Änderung der Zeitzone tritt sofort in Kraft.

Änderungen der Zeitzone werden automatisch für die Host-Plattform, OpenScape 4000 CSTA und ADP übernommen.

Die Abweichung der Sommerzeit wird ebenfalls vom OpenScape 400 Assistant gesteuert und automatisch an den ADP weitergeleitet.

Wichtig: Die Zeitzone am ADP sollte nicht manuell mittels AMO DATE geändert werden!

8.3.2 Einstellung von Zeitzone und Sommerzeit am Access Point/ OpenScape 4000 SoftGate

Da die Access Points/OpenScape 4000 SoftGates auch in einer anderen Zeitzone stehen können als das Host System, kann deren Zeitzone/Sommerzeit mit Hilfe von AMO SIPCO und AMO UCSU konfiguriert werden.

Im AMO SIPCO stellen Sie die Zeitverschiebung ein, die der Access Point gegenüber dem Host hat (Parameter **OFFSET** und **RICHT**). Außerdem können Sie die Parameter für Sommerzeitumstellung angeben.

AENDERN-

SIPCO:TYP=TCLASS,**TCLASS=1**,OFFSET=120,RICHT=WEST,SONUS=AUTO,MONATSTUNDESZ=2,MINSZ=30,MONATNZ=1,WOTAGNZ=SA,TAGNRNZ=ERSTER,STUNDE

Im AMO UCSU weisen Sie dann die Access Points den entsprechenden Zeitklassen zu Parameter **TCLASS**).

AENDERN-UCSU:ART=AP,LTU=nummer,**TCLASS=1**;

Relevante AMOs

AMO	Parameter	Sprache/ Sprache	Beschreibung/ Discription
SIPCO	TCLASS	d	Zeitklassen-Index
		e	Time Class Index
	OFFSET	d	Der Parameter OFFSET gibt die Zeitverschiebung in dieser Zeitklasse in Minuten an.
	OFFSET	e	The parameter OFFSET defines the time shift of this time class in minutes.

AMO	Parameter	Sprache/ Sprache	Beschreibung/ Discription
	RICHT	d	Der Parameter RICHT gibt die Richtung der Zeitverschiebung an. Eine Verschiebung nach OST ergibt immer eine spätere Zeit, d. h. der Zeit-Offset wird zur aktuellen Systemzeit addiert. Hingegen wird bei einer Verschiebung nach WEST der Zeit-Offset von der aktuellen Systemzeit subtrahiert, d.h., es wird fruher.
	DIRECT	e	The parameter DIRECT specifies the direction of the time shift. A shift to EAST results in a later time, which means that the time offset will be added to the actual system time. A shift to WEST results in an earlier time because the time offset will be subtracted from the actual system time.
UCSU	TCLASS	d	Zeitklassen-Index
	TCLASS	e	Time Class Index

8.3.3 Einstellung der Zeitzone für OpenScape 4000 CSTA

Die virtuelle Maschine hat Regionen etc., Zeitzone UTC. Die Zeitzone ist unabhängig von der OpenScape 4000 Plattform und kann mit Hilfe von YaST konfiguriert werden.

9 Anhang A: Tabellen für die Infrastrukturplanung

Kunden LAN und IPDA LAN befinden sich im selben Subnetz

Tabelle 35: Leere Tabellen für die Infrastruktur-Planung (Kunden und IPDA LAN in einem Subnetz)

Kunden & IPDA LAN			
	IP-Adresse	Netzmaske	Hostname
phys. IP Knoten 1 (YaST)			
phys. IP Knoten 2 (YaST)			
phys. IP Quorum (YaST)			
OpenScape 4000 Plattform Administration (Portal)			
OpenScape 4000 Assistant			
OpenScape 4000 CSTA			
CCA			
CCB			
NGS			
Default Gateway/Router			
Corosync LAN			
	IP-Adresse	Netzmaske	Hostname
phys. IP Knoten 1 (YaST)			
phys. IP Knoten 2 (YaST)			
phys. IP Quorum (YaST)			
Atlantic LAN			
Schnittstelle			
Schnittstelle			
Schnittstelle			
Schnittstelle			

Kunden LAN und IPDA LAN befinden sich in unterschiedlichen Subnetzen

Tabelle 36: Leere Tabellen für die Infrastruktur-Planung (Kunden und IPDA LAN in verschiedenen Subnetzen)

Kunden LAN

Anhang A: Tabellen für die Infrastrukturplanung

	IP-Adresse	Netzmaske	Hostname	Inter
phys. IP Knoten 1 (YaST)				
phys. IP Knoten 2 (YaST)				
phys. IP Quorum (YaST)				
OpenScape 4000 Plattform Administration (Portal)				
OpenScape 4000 Assistant				
OpenScape 4000 CSTA				
Default Gateway/Router				
IPDA LAN				
	IP-Adresse	Netzmaske	Hostname	Inter
phys. IP Knoten 1 (YaST)				
phys. IP Knoten 2 (YaST)				
CCA				
CCB				
NGS				
Default Router				
Corosync LAN				
	IP-Adresse	Netzmaske	Hostname	Inter
phys. IP Knoten 1 (YaST)				
phys. IP Knoten 2 (YaST)				
phys. IP Quorum (YaST) ⁶				
Atlantic LAN				
				Schr
Schnittstelle				
Schnittstelle				
Schnittstelle				
Schnittstelle				

⁶ Für Quorum kann eine passende Schnittstelle gewählt werden

10 Anhang B: Erstinstallationsskript und XML-Konfigurationsdatei

10.1 Einführung

Die Erstinstallation einer OpenScape 4000-Anlage wird mit dem Skript **firstinst-netw.sh** durchgeführt.

Geben Sie zum Aufrufen des Skripts Folgendes ein: **./firstinst-netw.sh [Optionen]**

Es wird dringend empfohlen, das Skript beim ersten Mal mit der Option **-c** aufzurufen, um es auf Netzwerkplausibilität, Syntaxfehler und OpenScape 4000-bedingte Abhängigkeiten zu überprüfen. Eine Liste der möglichen Optionen finden Sie in [Abschnitt 10.2, "Erstinstallationsskript - Befehlszeilenoptionen"](#).

Das Erstinstallationsskript sollte auf einer frisch installierten OpenScape 4000-Anlage ausgeführt werden. Auf einer Anlage mit vorhandener Netzwerkkonfiguration lässt sich das Skript nicht starten.

Sollte es wirklich einmal notwendig sein, das Skript ein zweites Mal zu starten (z. B. nach einer fehlerhaften Installation), müssen zuvor alle auf der Anlage konfigurierten IP-Adressen entfernt werden (z.B. durch Aufruf des Erstinstallationsskript mit Option **-d**).

Das Skript schreibt relevante Informationen, Fehlermeldungen und Warnhinweise in die Datei **firstinst-netw.log**, die im Verzeichnis **/var/log** angelegt wird. Die durch den Aufruf mit der Option **-c** ermittelten Ergebnisse werden ebenfalls in diese Datei geschrieben.

Im Falle einer Fehlermeldung wird das Erstinstallationsskript abgebrochen. Warnmeldungen hingegen beeinträchtigen die Skriptausführung nicht.

Die Installation erfolgt anhand einer XML-Datei, die alle relevanten Konfigurationsdaten enthält. Weitere Informationen zu der XML-Datei finden Sie in [Abschnitt 10.3, "XML-Konfigurationsdatei"](#).

10.2 Erstinstallationsskript - Befehlszeilenoptionen

1) Aufruf ohne Optionen

Das Skript sucht im Verzeichnis **/var/opt/firstinstall** nach XML-Dateien, deren Name mit **firstinst-netw** beginnt. Alle diese XML-Dateien müssen eine XML-Zeile mit der MAC-Adresse eines Netzwerkgeräts enthalten. Das Skript durchsucht alle XML-Dateien in diesem Verzeichnis nach dieser MAC-Adresse und vergleicht die aufgefundenen Adressen mit der MAC-Adresse des laufenden Servers. Die XML-Datei, die die MAC-Adresse des Servers enthält, wird für die Installation verwendet.

• Nur gültig für OpenScape 4000 V7 R0

Bei der Konfiguration des OpenScape 4000 SoftGate sucht das Skript in demselben Verzeichnis nach XML-Dateien, deren Name mit **initialcfg** beginnt. Anschließend muss der Dateiname die MAC-Adresse eines Netzwerkgeräts enthalten (z. B. **initialcfg_00-19-99-2D-CC-FC.xml** oder

initialcfg_00:19:99:2d:cc:fc.xml). Die XML-Datei mit der MAC-Adresse, die mit einer der MAC-Adressen des Servers übereinstimmt, wird für die OpenScape 4000 SoftGate-Konfiguration verwendet.

- **Nur gültig ab OpenScape 4000 V7 R1**

Ab OpenScape 4000 V7 R1 können die OpenScape 4000 SoftGate Konfigurationsdaten auch in die XML-Konfigurationsdatei übernommen werden. Wenn Sie die Installation mit einer separaten initialcfg-Datei starten, dann werden die oben beschriebenen Voraussetzungen angewandt und der Inhalt automatisch in die XML-Konfigurationsdatei integriert. Nach der Installation wird die vorhandene initialcfg-Datei aus dem Installationsverzeichnis gelöscht.

Wenn eine gültige initialcfg-Datei und ein gültiger OpenScape 4000 SoftGate Installationsabschnitt in der XML-Konfigurationsdatei (MAC-adresse) existiert, dann werden die Daten für die Installation aus der XML-Konfigurationsdatei übernommen und die existierende initialcfg-Datei wird aus dem Installationsverzeichnis gelöscht.

In einer Duplex- oder Separated Duplex-Umgebung muss bei jedem Aufruf des Skripts ohne Optionen die folgende Frage beantwortet werden:

Is this a First Installation (i) or Recovery (r)?

Das Skript wartet 10 Sekunden lang auf eine Antwort. Hierbei wird ein Countdown angezeigt.

Wenn bis zum Ablauf des Countdowns keine Eingabe erfolgt, wird das Skript wie gewöhnlich fortgesetzt. Dies bedeutet, dass je nach der in der XML-Datei festgelegten Konfiguration eine Erstinstallation oder eine Knotenwiederherstellung ausgeführt wird (siehe [Abschnitt 10.3.2.2, "Knotenabschnitt" > node-replacement](#)).

Antwort **i** (Erstinstallation): Ein vorhandenes Tag **entry key="node-replacement"** wird aus dem entsprechenden Knotenabschnitt entfernt.

Antwort **r** (Wiederherstellung): Der Parameterwert des Tags **entry ="node-replacement"** wird von **0** in **1** geändert. Falls das Tag im entsprechenden Knotenabschnitt (**entry ="node-replacement"1**) nicht vorhanden ist, wird es hinzugefügt.

Die ursprüngliche XML-Datei bleibt unverändert. Diese Informationen werden in einer anderen XML-Datei an das OpenScape 4000 Plattform Administration-Portal übergeben.

- Aufruf mit der Option **-h**

Hilfe zu allen möglichen Optionen wird angezeigt.

- Aufruf mit der Option **-i** oder **-r**

- **-i**: installiert das System, kennzeichnet den Primary Server in einem Duplex oder Separated Duplex Deployment
- **-r**: installiert das System, kennzeichnet den Replacement Server in einem Duplex oder Separated Duplex Deployment

Weitere Informationen finden Sie unter [Aufruf ohne Optionen](#).

- Aufruf mit der Option **-c XML-Datei Knotenname**

Das Skript nimmt keine Konfigurationseinstellungen vor, sondern überprüft die betreffende XML-Datei auf Netzwerkplausibilität, Syntaxfehler und OpenScape 4000-bedingte Abhängigkeiten (z. B.

Corosync-Konfiguration). In Verbindung mit dieser Option muss der Dateiname im zweiten und der Knotenname im dritten Argument angegeben werden. Hierbei können Sie wahlweise den vollständigen Pfadnamen der Datei oder nur den Dateinamen angeben. Wenn Sie nur den Dateinamen angeben, sucht das Skript die betreffende Datei im Verzeichnis /var/opt/firstinstall.

Im Idealfall wird diese Option natürlich auf der Anlage ausgeführt, auf der später das Netzwerk installiert wird. Hierbei gibt das Skript auch eventuelle Hardwarefehler aus, z. B. wenn bereits eine Netzwerkkarte installiert ist.

Mit dem dritten Argument (Knotenname) können alle Fehler mit Ausnahme von Hardwarefehlern erkannt und korrigiert werden, indem das Skript auf einem anderen Linux-System gestartet wird.

Beispiel: **firstinst-netw.sh -c firstinst-netw-node1.xml node1**

Diese Option bewirkt, dass nur die Daten in der XML-Datei geprüft und Fehler im Kopf- oder Endabschnitt daher ignoriert werden. Sie sollten diese Abschnitte jedoch nicht aus der Datei entfernen, da sie bei der Berechnung der Zeilennummern berücksichtigt werden. Ein Fehler im Kopfabschnitt wird in die Protokolldatei geschrieben, aber bei der Skriptausführung ignoriert.

Wichtig: In diesem Prüfmodus wird das Skript bei einer Fehlermeldung nicht abgebrochen.

2) Entfernen aller vorhandenen Netzwerkkonfigurationen

Beachten Sie, dass beim Aufruf des Skripts mit den folgenden Optionen alle konfigurierten IP-Adressen mit Ausnahme der Schleifenadresse (127.0.0.x) auf der Anlage entfernt werden.

Beachten Sie, dass nach dem Aufruf mit dieser Option keine Netzwerkverbindung zum Server besteht und diese Option daher nicht über eine Remoteverbindung aufgerufen werden sollte.

Diese Option sollte nicht auf einer bereits konfigurierten und laufenden Anlage verwendet werden, weil hierbei alle manuell vorgenommenen Konfigurationseinstellungen verloren gehen.

Anschließend sollten Sie das Skript zur Konfiguration des Netzwerks auf normalem Wege erneut starten.

Eine einzelne IP-Adresse kann auch mittels einer XML-Datei mit dem Parameter `system-delete.ip` entfernt werden. Weitere Informationen finden Sie in [Abschnitt 10.3.2, "Mögliche Parameter und ihre Werte"](#) > `system-delete.ip`.

a) Aufruf mit der Option **-d**

Diese Option bewirkt, dass vor dem Entfernen aller konfigurierten IPs eine Rückfrage (**Do you really want to remove all configured IPs from the System?**) angezeigt wird, die Sie bestätigen müssen. Wenn Sie diese Frage mit **n** oder **N** (Nein) beantworten, wird das Skript

abgebrochen. Antworten Sie mit **y** oder **Y** (Ja), werden alle IP-Adressen gelöscht.

Aufruf mit der Option **-d -y**

Diese Option bewirkt, dass das Skript alle konfigurierten IP-Adressen ohne Rückfrage löscht.

3) Aufruf mit der Option **-w oder **-n** oder **-w hostname** oder **-n hostname****

Diese Optionen bewirken, dass eine XML-Datei anhand einer laufenden Anlage erstellt wird. Die erstellte XML-Datei wird automatisch auf Plausibilitätsfehler und Warnungen geprüft. Diese Datei kann dann als XML-Datei für eine Erstinstallation verwendet werden.

Der einzige Unterschied zwischen den Optionen ist, dass ab OpenScape 4000 V7 R1 mit Hilfe der **-w** Option bei einem Duplex oder Separated Duplex Deployment eine XML-Datei aller Knoten erstellt wird (eine zusammengeführte XML-Datei).

Mit der **-n** Option wird nur der Abschnitt des betreffenden Knotens ausgefüllt. Die weiteren Knotenabschnitte bleiben leer. Aus diesem Grund kann die Ausgabedatei nur für den Knoten verwendet werden, auf dem sie erstellt wurde.

Bei Bedarf kann der Benutzer später verschiedene XML-Dateien zusammenführen und die Knotenabschnitte in eine gemeinsame XML-Datei kopieren. Vergessen Sie beim Zusammenführen der Dateien nicht, die Zeile mit dem Tag **customer-interface** zu entfernen. Duplizierte Zeilen verursachen einen Fehler!

Anmerkung: Vorlagen/Beispiele verschiedener XML-Konfigurationsdateien für alle Arten der Bereitstellung finden Sie in der ISO-Datei/auf dem Installationsstick im

Verzeichnis \Documentation (z.B.: `firstinst-netw-xml_examples_v4.zip`).

Die Anlage muss installiert und mit OpenScape 4000-Daten konfiguriert sein. In der Erstkonfigurationsphase kann das Skript keine XML-Datei erstellen.

Die Ausgabedatei wird unter dem Namen **firstinst-netw-ersten 36 Zeichen des Hostname-MAC-Adresse.xml** im Verzeichnis `/var/opt/firstinstall` abgelegt.

Im Block der Ausgabedatei wird der Hardwaretyp, wie im folgenden Beispiel dargestellt, angezeigt:

Wed Oct 16 16:12:27 CEST 2013 Firstinstall Script Version : V2.59
Hardware=DSCXL

Der Hardwaretyp kann auch **HPA** oder **Standard** sein. Somit ist es möglich die Plattform zu identifizieren auf der die XML-Datei erstellt worden ist.

Anstelle des Hostnamen kann der Anwender einen eigenen Namen definieren (z.B. den Kundennamen). Hierfür muss er die Option **-w/-n** mit einem zweiten Parameter aufrufen.

Beispiel : `firstinst-netw.sh -w simplex` oder `firstinst-netw.sh -n simplex`

Die Ausgabedatei wird dann unter dem Namen **firstinst-netw-simplex-MAC-Adresse.xml** im Verzeichnis `/var/opt/firstinstall` abgelegt.

XML-Datei: `/var/opt/firstinstall/firstinst-netw-simplex-00-19-99-5f-df-51.xml`

Anmerkung: Die Option **-w/-n** kann auch für OpenScape 4000 SoftGate Deployments verwendet werden.

Es werden nur die Konfigurationsparameter wiederhergestellt, die auch in der XML-Datei für die Erstinstallation enthalten sind. Alle übrigen Netzwerkparameter, wie Routing- oder Hostnamen-Einträge müssen, vom Benutzer manuell wiederhergestellt werden.

4) Aufruf mit der Option **crypt-pwd**

Diese Option bewirkt, dass ein Passwort mit SHA-512-Hashing verschlüsselt wird. Der Ausgabestring muss unter dem Tag-Namen **system-root.password** in die XML-Datei kopiert werden.

Im nächsten Schritt wird der Benutzer aufgefordert, das Passwort einzugeben. Das Passwort selbst wird auf dem Bildschirm nicht angezeigt.

Für die interaktive Verwendung kann das Passwort mit dem zweiten Argument übergeben werden, z. B. `./firstinst-netw crypt-pwd password092013`.

Diese Option sollte von einem anderen Skript aus verwendet werden, da das Passwort sonst im Befehlsverlauf eingesehen werden kann.

5) Aufruf mit der Option **set-pwd**

Mit dieser Option kann ein Root-Passwort direkt festgelegt werden. Das Passwort wird bei einem späteren Aufruf des Skripts mit der Option **-w** gespeichert.

Im nächsten Schritt wird der Benutzer aufgefordert, das Passwort einzugeben. Das Passwort selbst wird auf dem Bildschirm nicht angezeigt.

Für die interaktive Verwendung kann das Passwort mit dem zweiten Argument übergeben werden, z. B. **./firstinst-netw set-pwd password092013**.

Diese Option sollte von einem anderen Skript aus verwendet werden, da das Passwort sonst im Befehlsverlauf eingesehen werden kann.

6) Aufruf mit der Option **-e**

Wird das Skript mit der Option **-e** aufgerufen, so werden alle notwendigen Daten vom Server gesammelt und dann archiviert, komprimiert und im **/tmp**-Verzeichnis gespeichert. Wenn dieser Vorgang beendet ist, bekommt man eine Meldung über den Dateinamen der Datei im **/tmp**-Verzeichnis. Die Datei ist ungefähr 50kB groß.

Diese Datei kann dann an ein Problem Ticket zu Diagnosezwecken angehängt werden.

Die Meldung ist ähnlich der folgenden:

Compressed Diagnosys File : /tmp/fnetw-28022013-10-36-53-537.bz2

7) Aufruf mit der Option **-s**

Wird das Skript mit der Option **-s** und einem zweiten Parameter aufgerufen, werden nur die folgenden Konfigurationen aus der XML-Datei durchgeführt ohne Löschen/Reinstallation der Netzwerk-Konfiguration.

Wichtig: Die XML-Datei muss in das Verzeichnis **/var/opt/firstinstall** kopiert werden.

Verwendung:

Tabelle 37: firstinst-netw.sh, Option -s

./firstinst-netw.sh -s keyboard	--> Nur das Layout der Tastatur wird konfiguriert
./firstinst-netw.sh -s timezone	--> Nur die Zeitzone wird konfiguriert
./firstinst-netw.sh -s dns	<p>--> Nur der/die DNS-Server wird/werden konfiguriert</p> <p>Hinweis: Wenn DNS-Einträge direkt über YaST geändert werden, dann werden alle IP-Schnittstellen neu gestartet, was einen Ausfall des Systems zur Folge hat!</p>
./firstinst-netw.sh -s ntp	--> Nur der/die NTP-Server wird/werden konfiguriert

<code>./firstinst-netw.sh -s all</code>	--> Nur die 4 Parameters oben beschrieben werden konfiguriert
---	---

Jede bestehende Konfiguration wird mit den Werten der XML-Datei ersetzt, die zum Server passt.

8) Aufruf mit der Option -v

Wird das Skript mit der **-v** Option aufgerufen, wird die Skript-Version angezeigt.

9) Aufruf mit der Option -p XML-Datei Tag-Name node1|node2|node3

Wird das Skript mit der **-p** Option und den obigen Parametern aufgerufen, dann wird in der entsprechende XML-Datei und Knoten nach dem Wert des Tag-Names gesucht.

10) Aufruf mit der Option -m add XML-Datei Tag-Name Tag-Wert common|node1|node2|node3

Wird das Skript mit der **-m** Option und den obigen Parametern aufgerufen, dann wird der angegebene Tag-Name in dem angegebenen Abschnitt in der angegebenen XML-Datei eingefügt/überschrieben.

11) Aufruf mit der Option -m del XML-Datei Tag-Name Tag-Wert common|node1|node2|node3

Wird das Skript mit der **-m** Option und den obigen Parametern aufgerufen, dann wird der angegebene Tag-Name in den angegebenen Abschnitt aus der angegebenen XML-Datei gelöscht.

12) Aufruf mit der Option -x

Wird das Skript mit der Option **-x** aufgerufen, so wird nur der Status der XML-Datei im Verzeichnis **/var/opt/firstinstall** überprüft.

Die folgenden Ausgaben sind möglich

- Normalfall: eine passende XML-Datei, Exit Code=0

Configuration XML file : /var/opt/firstinstall/firstinst-netw-node-a-00-20-ce-df-8a-70.xml

- Fehlerfall: keine XML-Datei, Exit Code=5

***** Configuration XML file not found *****

- Fehlerfall: mehr als eine XML-Datei, Exit Code=1

There are several XML files, that corresponds with a MAC-Address from this Server.

File 1 : /var/opt/firstinstall/firstinst-netw-dscxl-simplex-00-20-ce-f0-bd-80.xml

File 2 : /var/opt/firstinstall/firstinst-netw-simplex-00-20-ce-f0-bd-80.xml

Please copy only the right one into the directory and remove all others.

Die folgenden Ausgaben sind möglich, wenn es sich um ein Deployment mit OpenScape 4000 SoftGate handelt

- Normalfall: eine passende XML-Datei, Exit Code=0

Configuration XML file : /var/opt/firstinstall/firstinst-netw-dscxl-simplex-00-20-ce-f0-bd-80.xml

initialcfg XML file : /var/opt/firstinstall/initialcfg-simplex-00-20-ce-f0-bd-80.xml

- Normalfall: initialcfg Datei oder Installationsabschnitt in XML Konfigurationsdatei für OpenScape 4000 SoftGate existiert nicht, Exit Code=0

Configuration XML file : /var/opt/firstinstall/firstinst-netw-dscxl-simplex-00-20-ce-f0-bd-80.xml

Softgate Initial Config file is missing in directory /var/opt/firstinstall/

- Fehlerfall: mehr als eine initialcfg XML Datei, Exit Code=1

Configuration XML file : /var/opt/firstinstall/firstinst-netw-dscxl-simplex-00-20-ce-f0-bd-80.xml

There are several initialcfg.xml files, that corresponds with a MAC-Address from this Server.

File 1 : /var/opt/firstinstall/initialcfg-dscxl-simplex-00-20-ce-f0-bd-80.xml

File 2 : /var/opt/firstinstall/initialcfg-simplex-00-20-ce-f0-bd-80.xml

Please copy only the right one into the directory and remove all others.

10.3 XML-Konfigurationsdatei

NOTICE: Vorlagen und Beispiele für verschiedene XML-Konfigurationsdateien für alle Bereitstellungstypen sind im

XML Config File Generator (unter Datei > Laden von Dateien) enthalten, die mit der neuesten ComWin-Version verfügbar sind.

10.3.1 Format

10.3.1.1 Verzeichnis der XML-Datei

Die XML-Datei muss in das Verzeichnis **/var/opt/firstinstall** kopiert werden.

10.3.1.2 Name der XML-Datei

Der Name der XML-Datei muss das Format **firstinst-netw-XXXXX.xml** aufweisen, wobei XXXXX für eine beliebige Zeichenfolge steht.

Wichtig: XXXXX darf nur Buchstaben, Ziffern und/oder "-" (Bindestrich), "." (Punkt), "_" (Unterstrich) enthalten!

Nur gültig für OpenScape 4000 V7 R0

Wenn ein OpenScape 4000 Softgate konfiguriert werden muss, wird auch die XML-Datei für die OpenScape 4000 Softgate-Konfiguration benötigt.

Der Dateiname muss mit **initialcfg_** beginnen und muss eine gültige MAC-Adresse des Zielsystems enthalten (z.B. **initialcfg_...00-1a-e8-3c-e1-33....xml**, **initialcfg_00-1a-e8-3c-e1-33-eth.xml**, **initialcfg_Sys01_00-1a-e8-3c-e1-33-eth.xml**).

10.3.1.3 Struktur der XML-Datei

Wichtig: Die Struktur der XML-Datei sollte nicht geändert werden.

Die XML-Datei weist immer einen Abschnitt "common" sowie einen eigenen Abschnitt für jeden Knoten auf.

Jeder Knotenabschnitt muss eine gültige MAC-Adresse enthalten (siehe auch [Abschnitt 10.3.2, "Mögliche Parameter und ihre Werte"](#)).

Für Simplex-Bereitstellungen (wie Simplex, APE, RG 8350a, Standalone-Softgate usw.) wird nur ein Knotenabschnitt benötigt.

Für eine Duplex-Bereitstellung werden zwei Knotenabschnitte (für Knoten a und Knoten b) benötigt, und für eine getrennte Duplex-Bereitstellung sind drei Knotenabschnitte (für Knoten a, Knoten b und Quorumknoten) erforderlich.

```
<common>
```

```
....
```

```
</common>
```

```
<node1>
...
</node1>
<softGateInitialConfiguration>
<Property value=...>
...
</softGateInitialConfiguration>
<node2>
...
</node2>
<node3>
...
</node3>
```

Anmerkung: Bei Enterprise Gateway wird der Abschnitt `<softGateInitialConfiguration>` in `<EntGWInitialConfiguration>` umbenannt.

Datenzeile

Beispiel:

```
<entry="system-deployment">simplex>
```

Der mittlere Teil, in diesem Beispiel **system-deployment**, ist der **Parametername**, der auch als "Schlüssel" bezeichnet wird. Diese Parameternamen sind fest codiert.

Der zweite Teil, in diesem Beispiel simplex, ist der Parameterwert, der nach Belieben festgelegt werden kann. Allerdings gelten auch für diese Werte bestimmte Einschränkungen, z. B. IP-Adresskonventionen. Eine Liste aller Einschränkungen und Regeln finden Sie in [Abschnitt 10.3.2, "Mögliche Parameter und ihre Werte"](#).

Die Einträge `<entry="...">` und `</entry>` geben den Anfang und das Ende einer Datenzeile an und müssen exakt dieses Format aufweisen.

Kommentar-Tag

Ebenso wie HTML, steht auch in XML ein Kommentar-Tag zur Verfügung, das mit diesen Zeichen beginnt:

- Ein Kommentar kann beliebig viele Zeilen umfassen.
- Er kann an einer beliebigen Stelle in einer XML-Datei beginnen und enden.
- Es ist nicht möglich, mehrere Kommentare ineinander zu verschachteln.
- Kommentare können verwendet werden, um die Funktionsweise der verschiedenen Abschnitte Ihrer XML-Datei zu beschreiben.

Beispiele:

```
<entry="eth1.ip.0">10.0.0.10/24</entry>
```



```
<entry="eth1.hostname.0">node-a</entry>
<entry="eth1.domainname.0">h4k.com</entry>
oder
<entry="eth1.ip.0">10.0.0.10/24</entry>
oder
<entry="eth1.ip.0">10.0.0.10/24</entry>
<entry="eth1.hostname.0">node-a</entry>
<entry="eth1.domainname.0">h4k.com</entry>
oder
<entry="customer-timezone">Asia/Manila</entry>
```

Regeln

- Bei allen Variablen ist zwischen Groß- und Kleinschreibung zu unterscheiden.
- Das Skript ignoriert alle Daten, die für die betreffende Bereitstellung nicht benötigt werden. Dies bedeutet, dass Sie für die eingegebene Bereitstellung nicht benötigte Datenzeilen nicht zu löschen brauchen. Beispiel:

Corosync-Daten brauchen aus einer für eine Simplex-Bereitstellung definierten XML-Datei nicht entfernt zu werden. In diesem Fall werden die Corosync-Datenzeilen bei der Skriptausführung ignoriert.

- Eine nicht vorhandene Zeile und eine Zeile mit einem leeren Wertefeld haben denselben Effekt. Beispiel:

Die Zeile **<entry="eth0.hostname.0"></entry>** hat denselben Effekt, wie wenn diese Zeile nicht vorhanden wäre.

10.3.2 Mögliche Parameter und ihre Werte

Folgende Eintragsschlüssel sind definiert.

10.3.2.1 Allgemeiner Abschnitt

system-deployment

In jeder XML-Datei muss die Bereitstellung mit der folgenden Datenzeile definiert werden. Wenn diese Datenzeile in der XML-Datei fehlt, wird die Installation nicht ausgeführt.

```
<entry ="system-deployment">[deployment name]>
```

Die folgenden Bereitstellungen sind möglich und müssen wie unten dargestellt eingegeben werden:

- simplex
- duplex
- separated_duplex
- standalone_softgate
- survivable_softgate
- ape

- rg8350
- enterprise_gw
- survivable_enterprise_gw

Wichtig: Jede andere Benennung verursacht einen Fehler und führt zum Stoppen des Skripts. Achten Sie daher auf die Vermeidung von Eingabefehlern!

Die Bereitstellungen **standalone_softgate**, **survivable_softgate**, **rg8350**, **ape**, **enterprise_gw** und **survivable_enterprise_gw** werden wie eine Simplexserver-Konfiguration behandelt.

Weitere Informationen zu einer Duplex/Separated Duplex-Bereitstellung finden Sie in [Abschnitt 10.3.3.2, "Regeln für Duplex/Separated Duplex-Bereitstellungen"](#).

Weitere Informationen zu allen Bereitstellungen, die wie eine Simplex-Bereitstellung behandelt werden (Simplex, Standalone SoftGate, RG 8350 usw.), finden Sie in [Abschnitt 10.3.3.1, "Regeln für Simplex-Bereitstellungen"](#).

system-hpa.type

OpenScape Access Typ.

Dieses Tag muss angegeben werden, wenn das System eine OpenScape Access ist.

Beispiel:

```
<entry="system-hpa.type">hpa500i>
```

Mögliche Werte:

- hpa500i
- hpa500a

Anmerkung: The values are not case sensitive.

customer-portal.ip

IP-Adresse/Präfixlänge des OpenScape 4000 Plattform Administration-Portals

Beispiel:

```
<entry="customer-portal.ip">218.1.17.8/26>
```

Hinweise

- Wenn der Parameter **customer-portal.ip** angegeben ist, wird Folgendes geprüft: Der Parameter **customer-interface** im Knotenabschnitt der XML-Datei gibt die Netzwerkschnittstelle des Customer LAN an. Die erste IP-Adresse auf dieser Schnittstelle gibt die IP-Adresse des Customer LAN an. Das Skript prüft, ob die Schnittstelle/IP-Adresse des Customer LAN definiert ist. Wenn dies der Fall ist, prüft das Skript, ob beide Adressen gültig und im selben Subnetz konfiguriert sind.
- In einer Simplex-Anlage kann der Parameter **customer-portal.ip** für eine Schnittstelle dauerhaft konfiguriert werden. In einer Duplex-Anlage ist dies nicht zulässig.
- Das Skript prüft, ob das Standard-Gateway definiert und im selben Subnetz wie die IP-Adresse des Customer LAN eingerichtet ist.

Hier sehen Sie ein Beispiel für diese Konfiguration.

```
<entry="customer-interface">eth5>
```

```
<entry="eth5.ip.0">192.168.0.72/24>
```

```
<entry="customer-portal.ip">192.168.0.75/24>
```

```
<entry="customer-def.gw">192.168.0.1>
```

ccap-number

Für die Bereitstellungen **ape** und **survivable_softgate** muss die **ccap-number** als Access Point-Nummer eingegeben werden.

Beispiel:

```
<entry="ccap-number">17>
```

Mögliche Werte: 17 - 99, Standardwert: 17

Wenn die "ccap-number" nicht angegeben wurde, wird stattdessen der "ltu"-Wert aus der SoftGate-Konfiguration verwendet. Wenn beide Werte ("ccap-number" und "ltu") in der Konfigurationsdatei fehlen, wird der Standardwert verwendet.

corosync-name.node1

Hostname von Knoten 1 (z. B. node-a)

Beispiel:

```
<entry="corosync-name.node1">node-a>
```

corosync-name.node2

Hostname von Knoten 2 (z. B. node-b)

Beispiel:

```
<entry="corosync-name.node2">node-b>
```

corosync-name.quorum

Hostname des Quorum-Knotens (z. B. node-q)

Beispiel:

```
<entry="corosync-name.quorum">node-q>
```

corosync-ip.node1

IP-Adresse/Präfixlänge von Knoten 1 (z. B. 10.0.0.10/24)

Beispiel:

```
<entry="corosync-ip.node1">10.0.0.10/24>
```

corosync-ip.node2

IP-Adresse/Präfixlänge von Knoten 2 (z. B. 10.0.0.11/24)

Beispiel:

```
<entry="corosync-ip.node2">10.0.0.11/24>
```

corosync-ip.quorum

IP-Adresse/Präfixlänge des Quorum-Knotens (z. B. 10.0.0.12/24)

Beispiel:

```
<entry="corosync-ip.quorum">10.0.0.12/24>
```

customer-lan.assistant-ip-address

IP-Adresse/Präfixlänge (z. B. 10.7.117.105)

Beispiel:

```
<entry="customer-lan.assistant-ip-address">10.7.117.105/19>
```

customer-lan.csta-ip-address

IP-Adresse/Präfixlänge (z. B. 10.7.117.106/19)

Beispiel:

```
<entry="customer-lan.csta-ip-address">10.7.117.106/19>
```

customer-dns.server.0

IP-Adresse des Domain Name Service (DNS)-Servers

Beispiel:

```
<entry="customer-dns.server.0">192.168.1.1>
```

```
<entry="customer-dns.server.1">211.22.33.04>
```

```
<entry="customer-dns.server.2">112.32.43.111>
```

- Die Indexnummer 0 ist obligatorisch, die folgenden Indexnummern können optional angegeben werden (z. B. customer-dns.server.1, customer-dns.server.2).
- Der erste Eintrag mit der Indexnummer 0 gibt den bevorzugten Server an.

ipda-interface

Netzwerkschnittstelle für IPDA LAN (z. B. eth2, bond1, vlan123)

Beispiel:

```
<entry="ipda-interface">eth2>
```

Konfiguration ohne IPDA:

Löschen Sie den kompletten Eintrag für die IPDA-Schnittstelle oder lassen Sie den Wert leer (<entry="ipda-interface">>).

Wenn IPDA nicht konfiguriert ist, dann muss ein RTM konfiguriert sein:

```
<entry="system.rtm-configured">1>
```

Mehr Informationen über RTM finden Sie unter [system.rtm-configured](#).

ipda-lan.cca-ip-address

IP-Adresse/Präfixlänge für IPDA LAN (z. B. 172.16.2.11/16)

Beispiel:

```
<entry="ipda-lan.cca-ip-address">172.16.2.11/16>
```

ipda-lan.ccb-ip-address

IP-Adresse/Präfixlänge für IPDA LAN (z. B. 172.16.2.12/16)

Beispiel:

```
<entry="ipda-lan.ccb-ip-address">172.16.2.12/16>
```

ipda-lan.ngs-ip-address

IP-Adresse/Präfixlänge (z. B. 172.16.2.41/16)

Beispiel:

<entry="ipda-lan.ngs-ip-address">172.16.2.41/16>

ipda-lan.default-router-ipda

IP-Adresse des Standard-Routers für IPDA LAN (z. B. 172.16.3.1)

Beispiel:

<entry="ipda-lan.default-router-ipda">172.16.3.1>

internal-lan.network

IP-Adresse des internen LAN-Subnet

Beispiel:

<entry="internal-lan.network">192.168.187.0>

- Es handelt sich um ein 24-Bit-Netz (Netzmaske: 255.255.255.0)
- Es darf keine andere Adresse in diesem Subnet eingerichtet werden.
- Das letzte Octet muss immer 0 sein. Wenn das nicht der Fall ist, so wird es während der Installation mit 0 gesetzt.
- Wenn dieses Tag nicht angegeben ist, so wird das Netz mit der Default-Adresse 192.168.187.0 initialisiert.

atlantic-interface.0

Netzwerkschnittstelle für Atlantic LAN

Wenn mehrere Atlantic LAN-Schnittstellen vorhanden sind, verwenden Sie die jeweils nächsthöhere Indexnummer.

Beispiel:

<entry="atlantic-interface.0">eth5>

<entry="atlantic-interface.1">eth6>

customer-def.gw.dev

Netzwerkschnittstelle des Standardgateways (z.B. eth5)

Das Skript nimmt die Standardgateway-Schnittstelle aus **customer-interface**. Falls keine **customer-interface** konfiguriert ist, kann die Schnittstelle aber auch über die folgende Zeile definiert werden.

Beispiel:

<entry="customer-def.gw.dev">eth5>

Ein Standardgateway kann auch ohne Schnittstelle konfiguriert werden; daher ist diese Zeile bei der Standardgateway-Konfiguration nicht obligatorisch.

integrated-softgate

Wenn auf einem Simplex-Server oder in einer Separated Duplex-Bereitstellung ein weiteres OpenScape 4000 SoftGate konfiguriert werden soll, muss auf dem betreffenden Server das Tag **integrated-softgate** auf **1** gesetzt werden.

<entry="integrated-softgate">1>

Im Falle der Bereitstellungen **standalone_softgate**, **survivable_softgate** und **rg8350** wird dieses Flag nicht benötigt, da die Analysesoftware den internen Wert implizit auf **1** setzt.

In einer Separated Duplex-Bereitstellung mit integriertem SoftGate wird das SoftGate auf dem Quorum-Knoten ausgeführt.

Mögliche Werte: **0** oder **1**

system.rtm-configured

Im Falle einer Simplex- oder Duplex-Bereitstellung (auf dem EcoServer) muss das Tag

`<entry="system.rtm-configured">[0 oder 1]>`

auf **0** oder **1** gesetzt werden, um anzuzeigen ob ein Rear Transition Module (RTM) konfiguriert ist oder nicht.

Mögliche Werte: **0** oder **1**

0	RTM ist nicht konfiguriert
1	RTM ist konfiguriert

node-replacement

Wenn in einer Duplex- oder Separated Duplex-Anlage ein Knoten ersetzt werden soll, während andere Knoten aktiv sind, muss ein zusätzliches Tag in den Abschnitt des betreffenden Knotens eingefügt und auf **1** gesetzt werden.

Dieser Parameter muss im Abschnitt des abhängigen Knotens festgelegt werden und gibt an, ob es sich um eine neue Installation oder um einen Ersatz für diesen Knoten handelt.

`<entry="node-replacement">1>`

Mögliche Werte: **0** oder **1**

0	neue Installation
1	Ersatzknoten

Beispiel:

`<common>`

`<entry="system-deployment">separated_duplex>`

.

.

`</common>`

`<node1>`

`<entry="mac-address">00:20:ce:df:88:e0>`

.

`</common>`

`<node2>`

`<entry="mac-address">00-4c-ce-df-5e-e2>`

`<entry="node-replacement">1>`

.

`</node2>`

`<node3>`

`<entry="mac-address">00-4c-ce-df-5e-e2>`

</node3>

10.3.2.2 Knotenabschnitt

system-root.password

Verschlüsseltes Passwort

<entry="system-root.password">[verschlüsseltes Passwort]>

mac-address

MAC-Adresse des Servers

Beispiel:

<entry="mac-address">14-fe-b5-db-b2-82</entry>

customer-interface

Netzwerkschnittstelle für Customer LAN (z. B. eth0)

Beispiel:

<entry="customer-interface">eth0</entry>

corosync-interface

Netzwerkschnittstelle für Corosync LAN (z. B. eth4)

Beispiel:

<entry="corosync-interface">eth4</entry>

system-route.destination.0

IP-Adresse oder IP-Adresse/Präfixlänge

Wenn mehrere Routen konfiguriert sind, verwenden Sie die jeweils nächsthöhere Indexnummer (z. B. system-route.destination.1).

Weitere Informationen finden Sie in [Abschnitt 10.3.3.4, "Regeln für die Routenkonfiguration"](#).

system-route.via.0

IP-Adresse

Wenn mehrere Routen benötigt werden, verwenden Sie die jeweils nächsthöhere Indexnummer (z. B. system-route.via.1).

Weitere Informationen finden Sie in [Abschnitt 10.3.3.4, "Regeln für die Routenkonfiguration"](#).

system-route.dev.0

Netzwerkschnittstelle (z. B. eth0)

Wenn mehrere Routen benötigt werden, verwenden Sie die jeweils nächsthöhere Indexnummer (z. B. system-route.dev.1).

Weitere Informationen finden Sie in [Abschnitt 10.3.3.4, "Regeln für die Routenkonfiguration"](#).

eth0.ip.0

dhcp oder IP-Adresse/Präfixlänge

Wenn mehrere IP-Adressen konfiguriert sind, verwenden Sie die jeweils nächsthöhere Indexnummer (z. B. eth1.ip.0).

Schnittstellenname: eth[0-9]

Beispiel:

```
<entry="eth0.ip.0">218.1.17.41/26</entry>
```

```
<entry="eth0.ip.1">145.23.23.12/24</entry>
```

```
<entry="eth0.ip.2">172.17.3.39/16</entry>
```

Weitere Informationen finden Sie in [Abschnitt 10.3.3.3, "Regeln für die Schnittstellenkonfiguration"](#).

eth0.hostname.0

Hostname

Wenn mehrere IP-Adressen konfiguriert sind, verwenden Sie die jeweils nächsthöhere Indexnummer (z. B. eth1.hostname.0).

Schnittstellenname: eth[0-9]

Beispiel:

```
<entry="eth0.hostname.0">SIMPLEX-PCI44</entry>
```

```
<entry="eth0.hostname.1">SIMPLEX-PCI44-IPDA</entry>
```

Weitere Informationen finden Sie in [Abschnitt 10.3.3.3, "Regeln für die Schnittstellenkonfiguration"](#).

eth0.domainname.0

Domänenname

Wenn mehrere IP-Adressen konfiguriert sind, verwenden Sie die jeweils nächsthöhere Indexnummer (z. B. eth1.domainname.0).

Schnittstellenname: eth[0-9]

Beispiel:

```
<entry="eth0.domainname.0">eth0.com</entry>
```

```
<entry="eth0.domainname.1">SIMPLEX-PCI44-IPDA</entry>
```

Weitere Informationen finden Sie in [Abschnitt 10.3.3.3, "Regeln für die Schnittstellenkonfiguration"](#).

eth0.speed-duplex

Bitrate der ethx Schnittstelle

Dieses Tag wird für die Hardware-Konfiguration der Netzwerk-Geräte verwendet. Für jede Schnittstelle kann ein unterschiedlicher Wert konfiguriert werden.

Beispiel:

```
<entry="eth0.speed-duplex">100-full</entry>
```

Mögliche Werte:

- Der erste Wert konfiguriert die Geschwindigkeit in Mbit/s:
 - 10
 - 100
 - 1000 (für eine 1 GB Schnittstelle)

- Der zweite Wert legt die Duplex-Übertragung fest:
 - full
 - half

Anmerkung: Wenn dieses Tag nicht existiert, wird die Schnittstelle im Auto-Negotiation Mode gestartet.

bond0.dev.0

Schnittstelle 1

Wenn mehrere IP-Adressen konfiguriert sind, verwenden Sie die jeweils nächsthöhere Indexnummer (z. B. bond1.dev.0).

Beispiel:

```
<entry="bond0.dev.0">eth0</entry>
```

```
<entry="bond0.dev.1">eth1</entry>
```

Weitere Informationen finden Sie in [Regeln für Bond-Schnittstellen](#).

bond0.ip.0

dhcp oder IP-Adresse/Präfixlänge

Wenn mehrere IP-Adressen konfiguriert sind, verwenden Sie die jeweils nächsthöhere Indexnummer (z. B. bond1.ip.0).

Beispiel:

```
<entry="bond0.ip.0">0.0.0.0/0</entry>
```

Weitere Informationen finden Sie in [Regeln für IP 0.0.0.0/0](#) und [Regeln für Bond-Schnittstellen](#).

bond0.hostname.0

Hostname

Wenn mehrere IP-Adressen konfiguriert sind, verwenden Sie die jeweils nächsthöhere Indexnummer (z. B. bond0.hostname.1).

Beispiel:

```
<entry="bond0.hostname.0">bond0</entry>
```

Weitere Informationen finden Sie in [Regeln für Bond-Schnittstellen](#).

bond0.domainname.0

Domänenname

Wenn mehrere IP-Adressen konfiguriert sind, verwenden Sie die jeweils nächsthöhere Indexnummer (z. B. bond0.domainname.1).

Beispiel:

```
<entry="bond0.domainname.0">bond0.com</entry>
```

Weitere Informationen finden Sie in [Regeln für Bond-Schnittstellen](#).

bond0.speed-duplex

Bitrate des Bonds

Alle Bonding-Slave-Geräte werden mit der selben Konfiguration betrieben. Es ist nicht nötig für jedes Bond-Gerät ein XML-Tag zu definieren.

Beispiel:

```
<entry="eth0.speed-duplex">100-full</entry>
```

Mögliche Werte:

- Der erste Wert konfiguriert die Geschwindigkeit in Mbit/s:
 - 10
 - 100
 - 1000 (für eine 1 GB Schnittstelle)

- Der zweite Wert legt die Duplex-Übertragung fest:
 - full
 - half

Anmerkung: Wenn dieses Tag nicht existiert, wird die Schnittstelle im Auto-Negotiation Mode gestartet.

vlan<vlanid>.dev

Schnittstelle

Beispiel:

```
<entry="vlan1031.dev">bond1</entry>>
```

```
<entry="vlan1127.dev">bond0</entry>
```

Weitere Informationen finden Sie in [Regeln für VLAN-Schnittstellen](#).

vlan<vlanid>.id

VLAN-ID-Nummer

Für jede VLAN-ID muss ein Eintrag konfiguriert werden.

Beispiel:

```
<entry="vlan1031.id">1031</entry>
```

```
<entry="vlan1127.id">1127</entry>
```

Weitere Informationen finden Sie in [Regeln für VLAN-Schnittstellen](#).

vlan<vlanid>.ip.0

dhcp oder IP-Adresse/Präfixlänge

Für jede VLAN-ID muss ein Eintrag konfiguriert werden.

Beispiel:

```
<entry="vlan1031.ip.0">10.7.17.108/19</entry>
```

```
<entry="vlan1127.ip.0">10.7.117.108/19</entry>
```

Weitere Informationen finden Sie in [Regeln für VLAN-Schnittstellen](#).

vlan<vlanid>.hostname.0

Hostname

Für jede VLAN-ID muss ein Eintrag konfiguriert werden.

Beispiel:

```
<entry="vlan1031.hostname.0">PCI07-APE17-IPDA</entry>
```

```
<entry="vlan1127.hostname.0">PCI07-APE17</entry>
```

Weitere Informationen finden Sie in [Regeln für VLAN-Schnittstellen](#).

vlan<vlanid>.domainname.0

Domänenname

Für jede VLAN-ID muss ein Eintrag konfiguriert werden.

Beispiel:

```
<entry="vlan1031.domainname.0">vlan1031.com</entry>
```

```
<entry="vlan1127.domainname.0">vlan1127.com</entry>
```

Weitere Informationen finden Sie in [Regeln für VLAN-Schnittstellen](#).

system-delete.ip

IP-Adresse/Präfixlänge der IP-Adresse, die Sie von der Anlage entfernen möchten.

Beispiel:

```
<entry="system-delete.ip">192.168.0.2/24</entry>
```

customer-ntp.server.0

IP-Adresse oder Name des Network Time Protocol (NTP)-Servers

Beispiel:

```
<entry="customer-ntp.server.0">ntp1.ptb.de</entry>
```

```
<entry="customer-ntp.server.1">ntp1-0.uni-erlangen.de</entry>
```

```
<entry="customer-ntp.server.2">187.168.2.22</entry>
```

- Die Indexnummer 0 ist obligatorisch, die folgenden Indexnummern können optional angegeben werden (z. B. customer-ntp.server.1, customer-ntp.server.2).
- Der erste Eintrag mit der Indexnummer 0 gibt den bevorzugten Server an.

customer-timezone

Konfiguration der Zeitzone

Beispiele:

```
<entry="customer-timezone">Europe/Berlin</entry>
```

```
<entry="customer-timezone">America/Los_Angeles</entry>
```

```
<entry="customer-timezone">Asia/Kuala_Lumpur</entry>
```

Die Angabe aller Zeitzonevariablen erfolgt über die Verzeichnisstruktur /usr/share/zoneinfo

Mögliche Werte: siehe [Abschnitt 10.3.5, "Zeitzonewerte"](#).

customer-keyboard-layout

Konfiguration des Tastaturlayouts

Beispiel:

```
<entry="customer-keyboard-layout">german</entry>
```

Mögliche Werte:

arabic belgian canadian chinese croatian czech czech-qwerty danish dutch
dvorak english-uk english-us estonian finnish french french-ca french-ch
german german-ch german-deadkey greek hungarian icelandic italian japanese
khmer korean lithuanian norwegian polish portugese portugese-br portugese-br-
usa russian serbian slovak slovak-qwerty slovene spanish spanish-lat swedish
taiwanese turkish ukrainian

customer-def.gw

IP-Adresse des Standardgateways (z.B. 218.1.17.1)

Beispiel:

```
<entry="customer-def.gw">218.1.17.1</entry>
```

10.3.3 Regeln

10.3.3.1 Regeln für Simplex-Bereitstellungen

Das Skript bestimmt die Customer IP-Adresse anhand des Parameters **customer-interface**, Indexnummer 0.

Die Indexnummer ist die Nummer am Ende des Parameternamens **eth0.ip.0**.

Der Hostname aus dem Customer LAN wird als Server-Hostname eingestellt.

10.3.3.2 Regeln für Duplex/Separated Duplex-Bereitstellungen

Das Skript vergleicht die zwei/drei angegebenen IP-Adressen mit der einen IP-Adresse, die anhand des Parameters **corosync-interface** bestimmt wird. Die IP-Adresse aus dem Corosync-Server muss auf dieser Schnittstelle die Indexnummer **0** aufweisen. Die Indexnummer ist die Nummer am Ende des Parameternamens **eth1.ip.0**.

Auf diese Weise wird auch der eigene Server bestimmt und dessen Hostname als Server-Hostname eingestellt.

Außerdem prüft das Skript die folgenden Bedingungen in dieser Bereitstellung:

- Es prüft, ob die beiden/drei Hostnamen und IP-Adressen unterschiedlich sind.
- Es prüft, ob die IP-Adressen gültig sind.
- Es prüft, ob die Netzmaskeneinträge gültig sind. Die Netzmaske wird durch die Präfixlänge am Ende der jeweiligen IP-Adresse angegeben, die in diesem Fall den Wert **24** aufweist. **24** entspricht der Netzmaske 255.255.255.0. Eine Liste aller 32 Präfixlängen und der entsprechenden Netzmasken finden Sie am Ende dieses Dokuments ([Abschnitt 10.3.4, "Netzmaske und Präfixlänge"](#)).
- Es prüft, ob alle Corosync-IP-Adressen im selben Subnetz konfiguriert sind.

10.3.3.3 Regeln für die Schnittstellenkonfiguration

Ein Schnittstellenkonfigurationsabschnitt enthält die folgenden Zeilen.

```
<entry="eth0.ip.0">192.168.0.72/24</entry>
```

```
<entry="eth0.hostname.0">first-host</entry>
```

```
<entry="eth0.domainname.0">site.com</entry>
```

Jede Schnittstellenkonfiguration muss mindestens eine IP-Adresse für **eth0.ip.0** aufweisen. Wenn für **eth0.hostname.0** kein gültiger Wert eingegeben wurde und der Eintrag **eth0.domainname.0** oder die Zeilen selbst nicht vorhanden sind, werden die betreffenden Zeilen ignoriert (siehe unten stehendes Beispiel).

Wenn Sie Ihre IP-Adresse über einen DHCP-Server beziehen möchten, können Sie anstelle einer IP-Adresse die Zeichenfolge **dhcp** eingeben.

```
<entry="eth0.ip.0">dhcp</entry>
```

eth0.hostname.0 und **eth0.domainname.0** werden in diesem Fall ignoriert.

Wichtig: DHCP kann nur auf der IP mit der Indexnummer 0 konfiguriert werden.

Wichtig: DHCP wird nur für Standalone SoftGates und Survivable SoftGates unterstützt.

Wichtig: DHCP darf nicht auf Host-System-Knoten (nodeA, nodeB, quorum) verwendet werden.

Auf demselben Gerät können weitere IP-Adressen konfiguriert werden:

```
<entry="eth0.ip.0">dhcp</entry>
```

```
<entry="eth0.ip.1">192.168.1.45/24</entry>
```

```
<entry="eth0.hostname.1">host1</entry>
```

```
<entry="eth0.domainname.1">site.com</entry>
```

```
<entry="eth0.ip.2">10.35.44.45/24</entry>
```

```
<entry="eth0.hostname.2">host2</entry>
```

```
<entry="eth0.domainname.2">site2.com</entry>
```

Der Domänennameneintrag wird anhand des Hostnamens und des Domänennamens bestimmt. In diesem Beispiel werden der Datei /etc/hosts die folgenden Zeilen hinzugefügt.

192.168.1.45	host1.site.com	host1
10.35.44.45	host2.site2.com	host2

Der erste Teil dieses Parameters definiert die Schnittstelle selbst und kann folgende Werte aufweisen:

eth0 - eth[numerisch] (eth8 wird in einer dscxl-Umgebung nicht verwendet)

vlan0 - vlan[numerisch]

bond0 - bond[numerisch]

Wichtig: Die IDs **eth**, **vlan** und **bond** sind obligatorisch. Bei einem **vlan**- oder **bond**-Gerät kann der numerische Teil aus einer beliebigen Nummer bestehen. Bei einem **eth**-Gerät muss die angegebene Schnittstellennummer tatsächlich auf der Anlage vorhanden sein.

Die Nummer am Ende des Parameternamens gibt die IP-Indexnummer an, in diesem Fall **0** (null). Die Nummer **0** wird für die Haupt-IP-Adresse dieser Schnittstelle verwendet. Weitere Adressen sind sekundäre IP-Adressen.

Im Folgenden sehen Sie ein Beispiel hierfür.

```
<entry="eth0.ip.0">192.168.0.72/24</entry>
```

```
<entry="eth0.hostname.0">host0</entry>
<entry="eth0.domainname.0">site0.com</entry>
<entry="eth0.ip.1">192.168.0.74/24</entry>
<entry="eth0.hostname.1">host1</entry>
<entry="eth0.domainname.1">site1.com</entry>
<entry="eth0.ip.2">192.168.0.76/24</entry>
<entry="eth0.hostname.2">host2</entry>
<entry="eth0.domainname.2">site2.com</entry>
```

In dieser Konfiguration werden die folgenden IP-Adressen auf der eth0-Schnittstelle konfiguriert.

eth0	192.168.0.72	Netmask: 255.255.255.0	Broadcast: 192.168.1.255
eth0:1	192.168.0.74	Netmask: 255.255.255.0	Broadcast: 192.168.1.255
eth0:2	192.168.0.76	Netmask: 255.255.255.0	Broadcast: 192.168.1.255

Die Netzmaske und die Broadcast-Adresse werden anhand der angegebenen IP-Adresse und Präfixlänge errechnet.

Jede Schnittstelle muss eine Haupt-IP-Adresse aufweisen, die anhand der Nummer **0** (null) am Ende des Parameternamens bestimmt wird. Wenn keine IP-Zeile mit der Indexnummer 0 vorhanden ist, wird die nächste IP-Adresse als Haupt-IP-Adresse verwendet. Im unten stehenden Beispiel wird die IP-Adresse 192.168.0.74 als Haupt-IP-Adresse eingestellt.

```
<entry="eth0.ip.1">192.168.0.74/24</entry>
<entry="eth0.ip.2">192.168.0.76/24</entry>
```

- IP-Adressen und Netzmasken werden auf ihre Gültigkeit geprüft. Anhand dieser beiden Werte wird sodann die Broadcast-Adresse errechnet.
- IP-Adressen werden auf doppelte Einträge überprüft. Wenn eine doppelte IP-Adresse vorhanden und keiner der beiden Einträge als zu löschende IP-Adresse (**ip to delete**) konfiguriert ist, wird das Skript abgebrochen.
- Sie können eine oder mehrere IP-Adressen für das Entfernen aus dem System konfigurieren (siehe [Abschnitt 10.3.2, "Mögliche Parameter und ihre Werte"](#) > [system-delete.ip](#)).

Regeln für IP 0.0.0.0/0

Wenn die erste IP-Adresse als **0.0.0.0/0** konfiguriert ist, werden alle weiteren Konfigurationen auf diesem Gerät ignoriert.

In der folgenden Konfiguration werden die IP-Adressen 1 und 2 (zweite und dritte Zeile) ignoriert.

```
<entry="eth0.ip.0">0.0.0.0/0</entry>
<entry="eth0.ip.1">192.168.0.74/24</entry>
<entry="eth0.ip.2">192.168.0.76/24</entry>
```


Die IP-Adresse **0.0.0.0/0** muss als Hauptadresse mit dem Suffix **0** (null) konfiguriert werden. Andernfalls wird sie ignoriert.

In der folgenden Beispielkonfiguration wird die IP-Adresse 1 (zweite Zeile) ignoriert:

```
<entry="eth0.ip.0">192.168.0.72/24</entry>
<entry="eth0.ip.1">0.0.0.0/0</entry>
```

Regeln für Bond-Schnittstellen

Eine Bond-Schnittstelle kann auf jedem nicht konfigurierten eth-Gerät konfiguriert werden. Dies bedeutet, dass das betreffende eth-Gerät keine IP-Konfiguration aufweisen darf. Außerdem kann eine Bond-Schnittstelle nicht auf einem eth-Gerät konfiguriert werden, das einem vlan-Gerät zugeordnet ist.

Hier sehen Sie ein Beispiel für eine mögliche Bond-Konfiguration.

```
<entry="bond0.dev.0">eth2</entry>
<entry="bond0.dev.1">eth4</entry>
<entry="bond0.ip.0">192.168.1.51/24</entry>
<entry="bond0.hostname.0">bond0</entry>
<entry="bond0.domainname.0">bond0.com</entry>
<entry="bond0.ip.1">192.168.1.53/24</entry>
<entry="bond0.hostname.1">bond0-1</entry>
<entry="bond0.domainname.1">bond0.com</entry>
<entry="bond1.dev.0">eth5</entry>
<entry="bond1.dev.1">eth3</entry>
<entry="bond1.ip.0">0.0.0.0/0</entry>
```

Wenn für die Bond-Schnittstelle keine IP-Adresse konfiguriert ist, wird diese Bond-Schnittstelle mit der IP-Adresse **0.0.0.0/0** initialisiert und gestartet.

Im Folgenden sehen Sie ein Beispiel hierfür.

```
<entry="bond0.dev.0">eth2</entry>
<entry="bond0.dev.1">eth4</entry>
```

In diesem Beispiel wird die Bond-Schnittstelle **bond0** mit den Slave-Geräten **eth2** und **eth4** mit der IP-Adresse **0.0.0.0/0** initialisiert und anschließend gestartet. In diesem Fall wird der angegebene Hostname und der angegebene Domänenname ignoriert.

Regeln für VLAN-Schnittstellen

Ein virtuelles LAN kann auf jedem Gerät (einschließlich Bond-Schnittstellen) konfiguriert werden, nicht jedoch auf einer eth-Schnittstelle, die bereits von einer Bond-Schnittstelle zugeordnet ist.

Die VLAN-ID darf nicht mit dem VLAN-Schnittstellennamen übereinstimmen, sollte aber für YaST-Kompatibilität identisch sein.

Hier sehen Sie ein Beispiel für eine mögliche VLAN-Konfiguration.

```
<entry="vlan4.dev">eth7</entry>
<entry="vlan4.id">4</entry>
```

```
<entry="vlan4.ip.0">192.168.1.68/24</entry>
<entry="vlan4.hostname.0">vlan4-0</entry>
<entry="vlan4.domainname.0">vlan4.com</entry>
<entry="vlan4.ip.1">192.168.1.64/24</entry>
<entry="vlan4.hostname.1">vlan4-1</entry>
<entry="vlan4.domainname.1">vlan4.com</entry>
<entry="vlan7.dev">bond0</entry>
<entry="vlan7.id">7</entry>
<entry="vlan7.ip.0">192.168.1.88/24</entry>
<entry="vlan7.hostname.0">vlan7-0</entry>
<entry="vlan7.domainname.0">vlan7.com</entry>
<entry="vlan7.ip.1">192.168.1.86/24</entry>
<entry="vlan7.hostname.1">vlan7-1</entry>
```

Wenn für die VLAN-Schnittstelle keine IP-Adresse konfiguriert ist, wird diese VLAN-Schnittstelle mit der IP-Adresse **0.0.0.0/0** initialisiert und gestartet.

Im Folgenden sehen Sie ein Beispiel hierfür.

```
<entry="vlan4.dev">eth2</entry>
<entry="vlan4.id">4</entry>
```

In diesem Beispiel wird die VLAN-Schnittstelle **vlan4** mit dem Slave-Gerät **eth2** und der VLAN-ID **4** mit der IP-Adresse **0.0.0.0/0** initialisiert und anschließend gestartet. In diesem Fall wird der angegebene Hostname und der angegebene Domänenname ignoriert.

10.3.3.4 Regeln für die Routenkonfiguration

Routen können mit den folgenden Tags konfiguriert werden.

- Das Routenziel ist ein einzelner Host:

```
key="system-route.destination.0">192.56.76.0
```

- Das Routenziel ist ein Netzwerk:

```
<entry="system-route.destination.0">192.56.76.0/24</entry>
```

Zusätzlich können die folgenden Tags konfiguriert werden:

```
<entry="system-route.via.0">192.168.0.1</entry>
```

```
<entry="system-route.dev.0">eth0</entry>
```

Alle auf der Customer LAN-Schnittstelle konfigurierten Routen werden auch in die spezielle OpenScape 4000-Routentabelle aufgenommen.

10.3.4 Netzmaske und Präfixlänge

Tabelle 38: Beziehung zwischen Netzmasken und Präfixlängen auf einem IPv4-System

1	128.0.0.0	192.0.0.0	224.0.0.0	240.0.0.0	4
5	248.0.0.0	252.0.0.0	254.0.0.0	255.0.0.0	8
9	255.128.0.0	255.192.0.0	255.224.0.0	255.240.0.0	12
13	255.248.0.0	255.252.0.0	255.254.0.0	255.255.0.0	16
17	255.255.128.0	255.255.192.0	255.255.224.0	255.255.240.0	20
21	255.255.248.0	255.255.252.0	255.255.254.0	255.255.255.0	24
25	255.255.255.128	255.255.255.192	255.255.255.224	255.255.255.240	28
29	255.255.255.248	255.255.255.252	255.255.255.254	255.255.255.255	32

10.3.5 Zeitzonewerte

Africa/

Abidjan Asmara Banjul Bujumbura Conakry Douala Harare Kigali

Lome Malabo Mogadishu Niamey Sao_Tome Windhoek Accra Asmera

Bissau Cairo Dakar El_Aaiun Johannesburg Kinshasa Luanda Maputo

Monrovia Nouakchott Timbuktu Addis_Ababa Bamako Blantyre Casablanca
Dar_es_Salaam

Freetown Kampala Lagos Lubumbashi Maseru Nairobi Ouagadougou Tripoli

Algiers Bangui Brazzaville Ceuta Djibouti Gaborone Khartoum Libreville

Lusaka Mbabane Ndjamena Porto-Novo Tunis

America/

Adak Barbados Catamarca Dawson_Creek Goose_Bay Inuvik Managua
Monterrey

Pangnirtung Resolute St_Kitts Virgin Anchorage Belem Cayenne Denver

Grand_Turk Iqaluit Manaus Montevideo Paramaribo Rio_Branco St_Lucia
Whitehorse

Anguilla Belize Cayman Detroit Grenada Jamaica Marigot Montreal

Phoenix Rosario St_Thomas Winnipeg Antigua Blanc-Sablon Chicago
Dominica

Guadeloupe Jujuy Martinique Montserrat Port-au-Prince Santa_Isabel
St_Vincent Yakutat

Araguaina Boa_Vista Chihuahua Edmonton Guatemala Juneau Matamoros
Nassau

Port_of_Spain Santarem Swift_Current Yellowknife Argentina Bogota
Coral_Harbour Eirunepe

Guayaquil Kentucky Mazatlan New_York Porto_Acre Santiago Tegucigalpa
Aruba Boise Cordoba El_Salvador Guyana Knox_IN Mendoza Nipigon
Porto_Velho Santo_Domingo Thule Asuncion Buenos_Aires Costa_Rica
Ensenada Halifax
La_Paz Menominee Nome Puerto_Rico Sao_Paulo Thunder_Bay Atikokan
Cambridge_Bay
Cuiaba Fort_Wayne Havana Lima Merida Noronha Rainy_River Scoresbysund
Tijuana Atka Campo_Grande Curacao Fortaleza Hermosillo Los_Angeles
Mexico_City
North_Dakota Rankin_Inlet Shiprock Toronto Bahia Cancun Danmarkshavn
Glace_Bay
Indiana Louisville Miquelon Ojinaga Recife St_Barthelemy Tortola
Bahia_Banderas Caracas Dawson Godthab Indianapolis Maceio Moncton
Panama
Regina St_Johns Vancouver
America/Argentina/
Buenos_Aires Catamarca ComodRivadavia Cordoba Jujuy La_Rioja Mendoza
Rio_Gallegos Salta
San_Juan San_Luis Tucuman Ushuaia
America/Indiana/
Indianapolis Knox Marengo Petersburg Tell_City Vevay Vincennes Winamac
America/Kentucky/
Louisville Monticello
America/North_Dakota/
Center New_Salem
Antarctica/
Casey Davis DumontDURville Macquarie Mawson McMurdo Palmer Rothera
South_Pole Syowa Vostok
Arctic/
Longyearbyen
Asia/
Aden Ashkhabad Bishkek Dacca Harbin Jayapura Katmandu Macau
Novosibirsk Qyzylorda Sakhalin Tbilisi Ulaanbaatar Yerevan Almaty Baghdad
Brunei Damascus Ho_Chi_Minh Jerusalem Kolkata Magadan Omsk Rangoon
Samarkand Tehran Ulan_Bator Amman Bahrain Calcutta Dhaka Hong_Kong
Kabul Krasnoyarsk Makassar Oral Riyadh Seoul Tel_Aviv Urumqi
Anadyr Baku Choibalsan Dili Hovd Kamchatka Kuala_Lumpur Manila
Phnom_Penh Riyadh87 Shanghai Thimbu Vientiane Aqtau Bangkok Chongqing
Dubai Irkutsk Karachi Kuching Muscat Pontianak Riyadh88 Singapore
Thimphu Vladivostok Aqtobe Beijing Chungking Dushanbe Istanbul Kashgar

Kuwait Nicosia Pyongyang Riyadh89 Taipei Tokyo Yakutsk Ashgabat
Beirut Colombo Gaza Jakarta Kathmandu Macao Novokuznetsk Qatar
Saigon Tashkent Ujung_Pandang Yekaterinburg
Atlantic/
Azores Bermuda Canary Cape_Verde Faeroe Faroe Jan_Mayen Madeira
Reykjavik South_Georgia
St_Helena Stanley
Australia/
ACT Brisbane Canberra Darwin Hobart Lindeman Melbourne North Queensland
Sydney
Victoria Yancowinna Adelaide Broken_Hill Currie Eucla LHI Lord_Howe NSW
Perth
South Tasmania West
Brazil/
Acre DeNoronha East West
Canada/
Atlantic Central East-Saskatchewan Eastern Mountain Newfoundland Pacific
Saskatchewan Yukon
Chile/
Continental EasterIsland
Etc/
GMT GMT+1 GMT+11 GMT+2 GMT+4 GMT+6 GMT+8 GMT-0 GMT-10
GMT-12 GMT-14 GMT-3 GMT-5 GMT-7
GMT-9 Greenwich UTC Zulu GMT+0 GMT+10 GMT+12 GMT+3 GMT+5 GMT
+7 GMT+9 GMT-1 GMT-11 GMT-13
GMT-2 GMT-4 GMT-6 GMT-8 GMT0 UCT Universal
Europe/
Amsterdam Belgrade Bucharest Dublin Isle_of_Man Kiev Luxembourg Minsk
Oslo
Riga Sarajevo Stockholm Uzhgorod Vilnius Zaporozhye Andorra Berlin
Budapest Gibraltar Istanbul Lisbon Madrid Monaco Paris Rome Simferopol
Tallinn Vaduz Volgograd Zurich Athens Bratislava Chisinau Guernsey Jersey
Ljubljana Malta Moscow Podgorica Samara Skopje Tirane Vatican Warsaw
Belfast Brussels Copenhagen Helsinki Kaliningrad London Mariehamn Nicosia
Prague San_Marino Sofia Tiraspol Vienna Zagreb
Indian/
Antananarivo Chagos Christmas Cocos Comoro Kerguelen Mahe Maldives
Mauritius Mayotte Reunion
Mexico/
BajaNorte BajaSur General
Mideast/
Riyadh87 Riyadh88 Riyadh89

Pacific/

Apia Chuuk Enderbury Funafuti Guadalcanal Johnston Kwajalein Midway
Norfolk Palau

Ponape Saipan Tarawa Wake Auckland Easter Fakaofu Galapagos Guam
Kiritimati Majuro Nauru Noumea Pitcairn Port_Moresby Samoa Tongatapu
Wallis Chatham Efate Fiji Gambier Honolulu Kosrae Marquesas Niue
Pago_Pago Pohnpei Rarotonga Tahiti Truk Yap

US/

Alaska Aleutian Arizona Central East-Indiana Eastern Hawaii Indiana-Starke
Michigan Mountain Pacific Pacific-New Samoa

11 Appendix C: Bond- und VLAN-Konfiguration

Bond- und VLAN-Konfiguration muss über `firstinst-netw.sh` und **die** Rekonfiguration über das `Recovery/Reconfiguration Tool` `recover-H4K.sh` (im Verzeichnis `/opt/soco-common`) ausgeführt werden. Es wird keine andere Methode, z. B. YaST unterstützt. Mehr Informationen über das `Recovery/Reconfiguration Tool` finden Sie im [Abschnitt 6.3, "Recovery/Reconfiguration Tool"](#).

Wichtig: Auf Grund des internen Designs von YaST, zeigt YaST nicht die komplette Bond-Konfiguration, dennoch gibt es kein Problem mit der Bind-Funktionalität. Die Bond-Konfiguration/der Bond-Status sollten deshalb mit typischen Linux-Kommandos überprüft werden, wie: `"cat /proc/net/bonding/bond0"` or `"ip addr show bond0"`. Außerdem beachten Sie bitte, wenn Sie Duplex oder Schnittstellengeschwindigkeiten für einen Bond setzen (z.B. über First Installation XML), müssen diese für jeden Bond eth Slave Port und nicht für den Bond selbst konfiguriert werden.

11.1 Bond-Konfiguration

Wichtig: Die LAN-Schnittstelle `eth0` sollte zu diesem Zeitpunkt nicht gelöscht werden, da Sie sonst nach dem Neustart nicht auf die OpenScape 4000 Plattform Administration (Portal)-Standardadresse (<https://192.168.0.3>) zugreifen können. `eth0` kann gelöscht und dem Kunden-Bond hinzugefügt werden, nachdem die Konfiguration des LAN-Assistenten in der OpenScape 4000 Plattform Administration (Portal) abgeschlossen ist.



Abbildung 167: DSCXL2 Ethernet-Schnittstellen

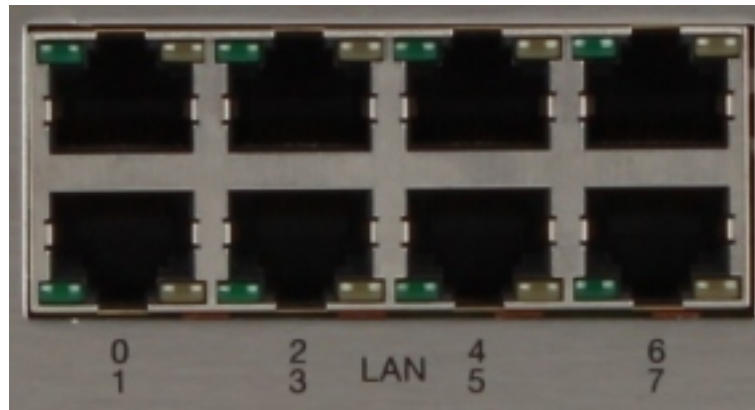


Abbildung 168: EcoServer Ethernet-Schnittstellen

Der Kreis um die Ethernet-Schnittstellen bei DSCXL2 (z. B. eth0 und eth1) gibt an, dass das Paar durch denselben Ethernet-Controller gesteuert wird. Um eine einzelne Fehlerstelle zu vermeiden, werden die Bond-Paare so gewählt, dass sie nicht durch denselben Controller gesteuert werden. Bonds werden diagonal von der obersten Zeile der Ports aus verwendet, damit die Kunden nach der Installation die Bindungen an freie Ports möglichst einfach konfigurieren können. Kunden ohne Bonds zum Beispiel belegen üblicherweise die erste Zeile der Ethernet-Ports.

Wenn LAN-Redundanz (Bonding) für die einzelnen Funktionen (Kunden-, IPDA-, Corosync-, Atlantik-LAN) erforderlich ist, werden pro Funktion zwei Schnittstellen verwendet. Die folgenden Einstellungen werden für DSCXL2-Hardware empfohlen:

- Kunden-LAN: **eth0 & eth3**
- IPDA-LAN: **eth2 & eth1**
- Corosync-LAN: **eth4 & eth7**
- Atlantik LAN: **eth6 & eth5**

Es gibt keine Empfehlung für die eth-Zuordnung für EcoServer-Hardware.

Hinweise:

- Bei **Duplex- und Separated Duplex-Bereitstellungen müssen die Bond-Namen** (z. B. bond0) **auf node1 und node2 übereinstimmen**. (Wenn z. B. für Kunden-LAN auf node1 der Name bond0 verwendet wurde, muss auch für Kunden-LAN auf node2 der Name bond0 verwendet werden.)
- Der verwendete Bond-Typ ist active-backup (Mode 1)

Dieser Modus versetzt eine Schnittstelle in einen Backup-Status und aktiviert sie nur dann, wenn der Link über die aktive Schnittstelle verloren geht. Nur ein Slave des Bonds ist aktiv. Ein anderer Slave wird nur dann aktiv, wenn der aktive Slave nicht mehr funktioniert. Dieser Modus bietet Fehlertoleranz.

11.2 Atlantik-Konfiguration

Es gibt zwei Möglichkeiten, die beiden Atlantik (ATLT) LAN-Schnittstellen zu konfigurieren:

- Lassen Sie die Schnittstellen überbrückt, wenn Sie ATLT-Zugriff von einem externen TAP/PC oder einer anderen Anwendung benötigen (Standardeinstellung).

Wichtig: In diesem Fall kann nur eine Schnittstelle für die CCA/CCB-Verbindung verwendet werden.

Anmerkung: Wenn beide Schnittstellen mit den entsprechenden zwei Schnittstellen auf der zweiten DSCXL2-Baugruppe/dem zweiten EcoServer oder alle Schnittstellen mit einem LAN-Switch verbunden sind, verfügen Sie über Netzwerkschleifen.

- Richten Sie einen Bond von den beiden ATLT-Schnittstellen ein, wenn Sie Redundanz bevorzugen, aber hier kein Standard-Port für die Verbindung zum ATLT verfügbar ist.

12 Anhang D: Wie Sie eine XML-Datei automatisch erstellen

Die XML-Datei mit den für das Erstinstallationsskript benötigten Konfigurationsdaten kann automatisch erstellt werden.

Führen Sie das Skript mit der Option `-w` aus:

```
#./var/opt/firstinstall/firstinst-netw.sh -w
```

oder

```
#cd /var/opt/firstinstall/
```

```
#./firstinst-netw.sh -w
```

Je nach der Bereitstellung werden die folgenden XML-Dateien im Verzeichnis **/var/opt/firstinstall** generiert:

- `firstinst-netw-Hostname-MAC-Adresse_von_eth0.xml` - wird für die Erstinstallation verwendet (z. B. `firstinst-netw-PCI06A-00-20-ce-f1-36-c8.xml`).
- `haipsetup.xml` - wird nur für das Debugging im Falle von Fehlern verwendet.
- **Nur im Falle von OpenScape 4000 V7 R1:** `initialcfg-Hostname-MAC-Adresse.xml` - wird für die OpenScape 4000 Softgate-Konfiguration verwendet (z. B. `initialcfg-SG18-00-30-ce-f2-96-c1.xml`).

Weitere Informationen zu den Befehlszeilenoptionen des Erstinstallationsskripts finden Sie in [Erstinstallationsskript - Befehlszeilenoptionen](#) > Aufruf mit der Option `-w` oder `-n` Option oder mit `-w hostname` oder `-n hostname`.

13 Anhang E: Häufig gestellte Fragen (FAQ)

13.1 Konnektivität und Installation

13.1.1 Konnektivität

- 1) Frage: USB 1 sieht wie ein Slave-USB-Controller aus. Wird er momentan unterstützt? Wie kann ich ihn verwenden?

Antwort: Dieser Controller ist für den Konsolenzugang (Terminalemulation) vorgesehen. Er wurde mit HiPath 4000 V6 R1.10.0 zu Installationszwecken bereitgestellt. Eine ausführlichere Beschreibung finden Sie in den Versionshinweisen.

- 2) Frage: Wird eine USB-Dockingstation mit Netzteil benötigt, oder liefert DSCXL2/EcoServer genügend Strom für die externe Festplatte über USB?

Antwort: Es wird empfohlen, Dockingstationen mit eigenem Netzteil zu verwenden. Dadurch sind wir unabhängiger und flexibler. Derzeit verwenden wir nur für DSCXL ein HDTR (Hard Disk Tray)-Gerät mit Anschlüssen für zwei SATA-Festplatten. Weitere Details finden Sie im Hardware-Abschnitt in der Dokumentation zu den Systemkomponenten.

- 3) Frage: Wird ein USB-Hub unterstützt?

Antwort: Ja, wenn die Leistungsaufnahme die Spezifikation des USB-Anschlusses nicht übersteigt. Es wird jedoch empfohlen, USB-Geräte mit eigener Stromversorgung zu verwenden, um Versorgungsengpässe zu vermeiden. Die Frontblende weist zwei USB-Anschlüsse auf (USB 2.0 Highspeed). Der USB-Controller ist im Chipsatz integriert. Die +5 V der beiden USB-Hostanschlüsse sind durch eine elektronische 1-A-Sicherung (Texas Instruments TPS2032) und als Ausfallschutz durch eine zweite, seriell geschaltete 2,5-A-Schmelzsicherung (Größe 0603) geschützt. Daher kann eine 2,5"-USB-Festplatte vollständig über den Bus versorgt werden, auch wenn sie etwas mehr Strom benötigt, als die USB-Spezifikation erlaubt. In diesem Fall sollte am anderen Anschluss weniger Strom aufgenommen werden.

- 4) Frage: Wie lässt sich das System so mit einer UPS (z. B. APC) integrieren, dass das richtige Shutdown-Skript bereitgestellt wird? Hierfür gibt es Standardverfahren über LAN, aber unter Linux darf nichts installiert werden.

Antwort: Für DSCXL2 wird nach wie vor die alte, von Unify bereitgestellte Batterielösung unterstützt. Außerdem kann für Server oder DSCXL2-Kunden jede standardmäßige USB USP-Hardwarelösung von APC verwendet werden. Mit HiPath 4000 V6 R2 wurde eine Software-Integrationslösung eingeführt. Weitere Informationen finden Sie in der OpenScape 4000 Platform Administration (Portal)-Dokumentation. Für eine Separated Duplex-Bereitstellung können mehrere UPS verwendet und für jeden Knoten als MASTER konfiguriert werden.

- 5) Frage: Es fällt auf, dass DSCXL2-Baugruppen mit unterschiedlichen Sachnummern, nämlich einer mit K und einer mit X bestellt werden können. Worin besteht der Unterschied?

Antwort: DSCXL2-Baugruppen mit einem K in der Sachnummer (z. B. S30122-K7732) weisen eine Festplatte auf, DSCXL-Baugruppen mit dem X in der Sachnummer (z. B. S30122-X8004) hingegen nicht.

- 6) Frage: Was bedeutet der Kreis um die eth-Schnittstellen der DSCXL2-Baugruppe?

Antwort: Der Kreis um die Ethernet-Schnittstellen (z. B. eth0 und eth1) gibt an, dass das Paar vom selben Ethernet-Controller gesteuert wird (siehe auch [Section 11.1, "Bond-Konfiguration"](#)).

- 7) Frage: Ich versuche, eine FTP-Verbindung zu OpenScape 4000 herzustellen, aber sie funktioniert nicht. Was haben Sie getan?

Antwort: Telnet und FTP sind in HiPath 4000 V6 (oder höher) aus Sicherheitsgründen nicht mehr enthalten. Diese Protokolle übertragen Passwörter im Klartext und stellen deshalb ein Sicherheitsproblem dar. Sie wurden durch die sicheren Verbindungsprotokolle SSH und SFTP ersetzt.

- 8) Frage: Der Kunde wünscht ein Separated Duplex-System. Können sich die einzelnen Systeme in unterschiedlichen Netzwerken befinden?

Antwort: Die Corosync-Adressen aller 3 Knoten sollten sich im selben Subnetz befinden. Dies ist ein redundantes L2-Cluster, bei dem alle 3 Knoten über einen Gigabit- oder Dark-Fiber-Switch verbunden sind.

- 9) Frage: Wir möchten ADP/OpenScape 4000 Assistant/CSTA zwingen, auf dem Partnerknoten zu laufen, und der aktive Knoten lässt sich offenbar nicht neu starten. Warum?

Antwort: Um sicherzustellen, dass die relevanten VMs nur auf einem Knoten ausgeführt werden, wird ab HiPath 4000 V6 R2 vor dem Initiieren einer Umschaltung ein Timer mit einer Laufzeit von 5 Minuten gestartet. Der Timer dient dazu, Probleme durch zwei gleichzeitig aktive Knoten (den so genannten Split-Brain-Betrieb) zu vermeiden.

- 10) Frage: Der Leistungsmerkmalbeschreibung entnehme ich, dass zwei der drei Knoten einer Separated Duplex-Bereitstellung einander immer "sehen" müssen, um den Betrieb zu gewährleisten. Gibt es irgendetwas, das ich tun kann, um sicherzustellen, dass die Telefonie funktioniert, sollten einmal zwei Knoten ausfallen?

Antwort: Die Sichtbarkeit zweier Knoten über das Corosync LAN ist notwendig, um eine "Split Brain"-Situationen zu vermeiden, in der sowohl Node1 als auch Node2 versucht, die Steuerung derselben Ressourcen zu übernehmen. Wenn einer der beiden Knoten verfügbar ist, kann natürlich automatisch ausgehandelt werden, welcher Knoten als Master fungiert. Wenn die Knoten einander nicht "sehen" können, kann ein Administrator mit dem Platform SSH-Befehl "standalone_operation enable" manuell einen Telefonie-Knoten starten. Sobald die Konnektivität der Knoten wiederhergestellt ist, muss der Standalone-Betrieb mit dem gegenteiligen Befehl "standalone_operation disable" ausdrücklich wieder deaktiviert werden.

13.1.2 Installation und Upgrades

- 1) Frage: Ist es möglich, 2 verschiedene Simplex-Systeme gleichzeitig in einer Kassette zu installieren, eine DSCXL2 in EBT 1/2 und die andere in

EBT 5/6? Die Prozessoren scheinen vollständig unabhängig voneinander zu sein, wenn sie nicht wie im Duplexbetrieb über LAN synchronisiert sind.

Antwort: Dieser Anwendungsfall wird nicht unterstützt und würde Probleme verursachen! Dieser Anwendungsfall muss in der Entwicklung und im Produktmanagement diskutiert werden. Zu diesem Zweck sollte der Service jedoch ein Service-KR ausstellen.

- 2) Frage: Gibt es eine Möglichkeit, das bereits installierte DSCXL2-/EcoServer-basierte System von Grund auf neu zu installieren, ohne einen USB-Stick oder eine Installations-CD zu verwenden?

Antwort: Es wird keine andere Möglichkeit der Reinstallation eines DSCXL2-/EcoServer-basierten Systems unterstützt. Außerdem hat die Verwendung eines USB-Sticks oder eines Installations-CD-Image den Vorteil, dass alles berücksichtigt und eine saubere Installation durchgeführt wird. Falls ein anderer Anwendungsfall vorliegt, sollte dieser auch via Service-KR an das Produktmanagement gemeldet werden.

- 3) Frage: Der AMO SIPCO-Parameter **BITRATE** wird in HiPath 4000 V6 R2 und späteren Versionen nicht mehr unterstützt. Wo und wie wird die benötigte LAN-Geschwindigkeit für die CCA/B LAN-Schnittstelle eingestellt?

Antwort: Dieser Parameter wurde in der Vergangenheit für HG3570 und CCA/B verwendet. Heute wirkt er sich nur noch auf HG3570 aus. Die Bitraten für CCA/B lassen sich nicht mehr konfigurieren, da diese Schnittstellen nicht physikalisch mit dem LAN-Netzwerk verbunden sind. Die Ports sind in Linux an eine logische Brücke angeschlossen und brauchen daher nicht mehr vom Administrator konfiguriert zu werden. Dies alles geschieht im Hintergrund bei der Einrichtung der CCA/B-VM. Ab HiPath 4000 V6 R2 können LAN-Schnittstellen offiziell nur noch mithilfe der XML-Erstinstallationsdatei konfiguriert/rekonfiguriert werden. Die XML-Datei wird während der erstmaligen Installation oder beim Aufrufen von *recovery.sh* verwendet (weitere Informationen hierzu siehe [Section 2.2.3, "Installation und Konfiguration von SLES und Konfiguration von OpenScape 4000"](#) oder [Section , "Ändern der Plattformkonfiguration"](#)). **TOSSIGNL** lässt sich für CCA/B jedoch nach wie vor in AMO konfigurieren.

- 4) Frage: Welche Funktion hat der AMO SIPCO-Parameter **VLAN** in OpenScape 4000, und wie und wo werden die benötigten VLAN-Informationen für die CCA/B LAN-Schnittstelle festgelegt?

Antwort: Dieser Parameter wurde in der Vergangenheit für HG3570 und CCA/B verwendet, aber heute wirkt er sich nur noch auf HG3570 aus. Um VLAN für CCA/CCB Ports zu konfigurieren, verwenden Sie bitte die XML-Datei mit den bekannten Erstinstallations-/Recovery-Methoden. **TOSSIGNL** lässt sich für CCA/B nach wie vor in AMO konfigurieren.

- 5) Frage: Auswahl des Tastaturtyps zu Beginn der USB-Installation erforderlich.

Antwort: Die Tastatur-Konfiguration erfolgt in der XML-Datei, indem man den entsprechenden Parameter hinzufügt (siehe [Section 10.3.2, "Mögliche Parameter und ihre Werte"](#) > customer-keyboard-layout).

- 6) Frage: Gibt es eine Möglichkeit, das ADP ohne Betriebsunterbrechung von einem Prozessor auf einen anderen umzuschalten?

Antwort: Nein, starten Sie den Prozessor neu, auf dem der ADP ausgeführt wird.

Anmerkung: Nur ein Herunterfahren des Knotens auf dem ADP läuft, führt nach 5 Minuten zu einem Starten des ADP auf dem Partner-Knoten.

- 7) Frage: Kann ich ein System klonen und ein anderes mit diesem Klon installieren? Oder sollten wir jedes System einzeln vom Image installieren?

Antwort: Jede Installation sollte eine individuelle Installation sein.

- 8) Frage: Ist es bei einer OpenScape 4000 Separated Duplex-Konfiguration möglich, Hinzufügungen, Verschiebungen und Änderungen vorzunehmen, wenn die Verbindung zwischen den Servern ausgefallen und nur einer der DSCXL2-Server/EcoServer aktiv ist?

Antwort: Ja, das ist möglich. Der zweite Prozessor wird beim Starten mit dem aktiven Prozessor synchronisiert.

- 9) Frage: Wird Bonding in OpenScape 4000 unterstützt?

Antwort: Ja. Ab HiPath 4000 V6 R2 können LAN-Schnittstellen offiziell nur noch mithilfe der XML-Erstinstallationsdatei konfiguriert/rekonfiguriert werden. Die XML-Datei wird während der erstmaligen Installation oder beim Aufrufen von *recovery.sh* verwendet (weitere Informationen hierzu siehe [Chapter 11](#), "[Appendix C: Bond- und VLAN-Konfiguration](#)").

- 10) Frage: Wie wird RAID in OpenScape 4000 verwendet?

Antwort: Für DSCXL2 und EcoServer steht die RAID-Funktionalität nur auf dem Knoten 1 (CCA) des Systems zur Verfügung. Eine Notfall-HD kann nicht auf dem Knoten 2 (CCB) eines Duplex-Systems verwendet werden. Software RAID Synchronisation erfolgt zwischen sda und sdb von Knoten 1.

Die Information welche HD / SSD aus dem raid-Verbund entfernt werden kann, finden Sie auf dem LCD-Display des Systems (und auf dem virtuellen LCD in der OpenScape 4000 Plattform Administration (Portal)). Informationen über das DSCL2+ Display finden Sie in der Hardwarebeschreibung der DSCL2+ Baugruppe in **OpenScape 4000, Band 2: Systemkomponenten (Hardware, Software)**.

Daten-Replikation von Knoten 1 auf Knoten 2 erfolgt mit DRBD.

- 11) Frage: Wie kann die IP-Konfiguration geändert werden?

Antwort: Ab HiPath 4000 V6 R2 können LAN-Schnittstellen offiziell nur noch mithilfe der XML-Erstinstallationsdatei konfiguriert/rekonfiguriert werden. Die XML-Datei wird während der erstmaligen Installation oder beim Aufrufen von *recovery.sh* verwendet (weitere Informationen hierzu siehe [Section 2.2.3](#), "[Installation und Konfiguration von SLES und Konfiguration von OpenScape 4000](#)" oder [Chapter 6](#), "[Ändern der Plattformkonfiguration](#)").

- 12) Frage: Der Kunde möchte die Duplex-Knoten durch lange Leitungen trennen, ohne das Quorum zu verwenden - ist das möglich?

Antwort: Nein. Aktive OpenScape 4000 Duplex-Signale werden über die CPCI-Backplane signalisiert. Deshalb ist eine physische Trennung der Duplex-Knoten nur in einer Separated Duplex-Bereitstellung möglich.

- 13) Frage: Der Kunde möchte eine Separated Duplex-Bereitstellung auf den Servern von einer Minor Release R1 nach R2 migrieren. Kann der Standalone-Operation-Schalter verwendet werden, um die Ausfallzeit aufgrund des Upgrades zu minimieren?

Antwort: Der bekannte Schalter "standalone_operation enable" kann verwendet werden. Er wirkt sofort und sollte daher nicht auf einem Partner-Standby-Knoten ausgeführt werden. Für minimalen Telefonieverlust gehen Sie wie folgt vor:

- Aktivieren Sie RMX SWU auf Knoten 2 (CCB).
- Fahren Sie Knoten 1 (CCA) herunter - OpenScape 4000 Assistant, CSTA, ADP startet jetzt auf Knoten 2 (CCB, sofern nicht bereits aktiv).
- Aktivieren Sie den genannten Standalone Switch auf Knoten 2 (CCB).
- Fahren Sie den Quorum-Knoten (CCQ) herunter.
- Installieren Sie Knoten 1 und Quorum neu und achten Sie darauf, dass sie nicht über das Netzwerk mit Knoten 2 (CCB) verbunden sind.
- Nachdem der neue Knoten 1 und Quorum installiert sind, fahren Sie Knoten 2 herunter und ziehen Sie die zu Knoten 2 gehörenden Netzkabel ab.
- Schließen Sie IPDA-Kabel an den neuen Knoten 1 (CCA) an - RMX wird neu geladen.
- Installieren Sie nun Knoten 2 (CCB) neu und stecken Sie die Netzkabel wieder ein, um die Synchronisierung abzuschließen.

- 14) Frage: Spielt es eine Rolle, in welcher Reihenfolge Separated Duplex-Knoten installiert werden?

Antwort: Seit HiPath 4000 V6 R2 ist es nicht mehr zwingend notwendig, zuerst den Quorum-Knoten zu installieren. Solange zwei beliebige Knoten verfügbar sind, ist nach der Inbetriebnahme eines Separated Duplex-Systems das "standalone_operation"-Flag nicht aktiviert.

Anmerkung: Der Tunnelbroker-Dienst startet erst, nachdem die Root-Passwörter der Plattform auf allen Knoten geändert wurden.

- 15) Frage: Ich habe das XML-Skript auf einem alten OpenScape 4000 SoftGate ausgeführt und die OpenScape 4000 Plattform Administration

(Portal)-IP-Adresse nicht erhalten. Dann habe ich die generierte XML-Datei verwendet, um das OpenScape 4000 SoftGate zu installieren.

Jetzt habe ich keine OpenScape 4000 Plattform Administration (Portal)-IP-Adresse. Wie kann ich auf OpenScape 4000 Plattform Administration (Portal) zugreifen, um das OpenScape 4000 SoftGate zu konfigurieren?

Antwort: Sie können unter der folgenden physikalischen Adresse auf die OpenScape 4000 Plattform Administration (Portal) zugreifen: `https://physical_ip_address/`

Schließen Sie die Installation des OpenScape 4000 SoftGate ab und klicken Sie auf **Submit** (Abschicken).

Von nun an können Sie unter der folgenden Adresse auf das vNCUI WBM zugreifen:

`https://vNCUI/`

Auf die OpenScape 4000 Plattform Administration (Portal) können Sie unter der folgenden Adresse zugreifen:

`https://vNCUI:8443/`

`https://physikalische_IP-Adresse:8443/`

16) Frage: Wie kann ich vor der Installation die MAC-Adresse des Rechners ermitteln?

Antwort: DSCXL2-Baugruppen weisen oberhalb der Ethernet-Schnittstellenbox einen Aufkleber mit der MAC-Adresse von eth0 auf.

Im Falle eines Servers können Sie Folgendes tun:

- Bereiten Sie den USB-Stick für die Installation wie üblich vor.
- Legen Sie im Ordner `/config` des USB-Sticks eine Datei namens "manual" an.
- Starten Sie den Server vom USB-Stick.
- Anstelle des üblichen Installationsdialogfelds wird eine Anmeldeaufforderung angezeigt.
- Melden Sie sich als **User** -> **root** mit dem **Passwort** -> **hicom** an.
- Nun können Sie mit dem Befehl `ifconfig eth0` die MAC-Adresse von eth0 abrufen.

17) Frage: Ich benötige eine unabhängige IP-Adresse für den OpenScape 4000 Plattform Administration (Portal)-Zugriff auf einem Standalone OpenScape 4000 SoftGate. Was kann ich tun?

Antwort: Fügen Sie Ihrer XML-Datei im Abschnitt **common** die folgende Zeile hinzu:

```
<entry="customer-portal.ip">10.13.68.36/21</entry>
```

Wichtig: Diese Adresse sollte mit der Kunden-IP-Adresse übereinstimmen, die Sie auf der Kunden-Schnittstelle im Abschnitt **node1** konfigurieren. Wenn Sie jedoch lieber eine separate IP-Adresse verwenden möchten, muss diese demselben Subnetz angehören wie die Kunden-IP-Adresse, die Sie auf der Kunden-Schnittstelle im Abschnitt **node1** konfigurieren.

- 18) Frage: Ich verwende eine Baugruppe eines anderen Kunden und mache mir Gedanken über die BIOS-Einstellungen. Wie kann ich sicherstellen, dass ich die richtigen Einstellungen verwende?

Antwort: Bei OpenScape 4000-Hardware sind die korrekten BIOS-Einstellungen werksseitig voreingestellt. Führen Sie auf Ihrer proprietären Hardware einfach einen "Reset To Default" durch.

13.2 Backup & Restore

- 1) Frage: Woher wissen wir, welche der beiden Festplatten bei einem physikalischen Festplattenfehler ausgetauscht werden muss? Ist "sda" immer ganz unten im Stapel?

Antwort: Diejenige, deren LED nicht blinkt. Eine andere Methode, dies festzustellen, gibt es nicht.

- 2) Frage: Welche Wiederherstellungsschritte sollten unternommen werden, wenn SLES 15 hochläuft, die OpenScape 4000 aber **NICHT** startet und OpenScape 4000 Platform Administration (Portal) nicht erreichbar ist?

Antwort: Sehen Sie in der Datei `/var/log/messages` nach. Geben Sie `crm_mon -l -f -A` ein, um die Ressourcen anzuzeigen.

- 3) Frage: Stehen irgendwelche Notfallwerkzeuge für die Fehlerbeseitigung zur Verfügung, wenn OpenScape 4000 Platform Administration (Portal) nicht erreichbar ist?

Antwort: Sehen Sie in der Datei `/var/log/messages` nach. Geben Sie `crm_mon -l -f -A` ein, um die Ressourcen anzuzeigen.

- 4) Frage: Welche Anforderungen hinsichtlich der Versionskompatibilität sind beim Zurückkopieren älterer VHD1/VHD2-Dateien in eine neuere Version zu beachten? Zum Beispiel mit HiPath 4000 V6 R1.10 erstellte VHD1/VHD2-Backupdateien, die wieder auf einen Backup-Server kopiert werden sollen, nachdem Hotfixes mit HiPath 4000 V6 R1.12 installiert wurden.

Antwort: Kein Problem, aber denken Sie daran, dass die RMX Hotfixes von HiPath 4000 V6 R1.12 reinstalliert werden müssen. Informationen zu möglichen Wechselwirkungen zwischen den verschiedenen Hotfixes finden Sie in den Versionshinweisen.

13.3 Hotfix-Installation

- 1) Frage: Reihenfolge der Hotfix-Installationen?

Antwort: Sofern in den Versionshinweisen nichts anderes angegeben ist, müssen die Hotfixes nicht in einer bestimmten Reihenfolge implementiert werden. Plattform-Hotfixes für den Duplexbetrieb setzen allerdings voraus, dass beide Prozessoren online sind, da die Aktivierung sonst fehlschlägt. Die Übertragung wird akzeptiert, aber in der SWA ist das PLT-HF ausgegraut.

- 2) Frage: Wird Hotfix in der SWA verfügbar, sobald der zweite Prozessor online geht?

Antwort: Ja.

- 3) Frage: Ist die Synchronisierung ein automatisierter Prozess und kann dieser angehalten oder manuell gestartet werden?

Antwort: Der Prozess ist automatisiert. Es ist nicht sinnvoll, ihn anzuhalten und neu zu starten, da keine Unterstützung für teilweise Upgrades implementiert ist.

13.4 Zeiteinstellung / Zeitsynchronisation

- 1) Frage: Bei aufgerüsteten Systemen ist die Uhr immer weniger genau als bei früheren Versionen, und ein paar Minuten pro Woche machen sich deutlich bemerkbar! Eine NTP-Lösung ist OK, aber viele unserer Kunden können von ihrem OpenScape 4000 Customer LAN aus auf keinen NTP-Server zugreifen. Gibt es für sie eine andere Lösung?

Antwort: Nein. NTP ist als Voraussetzung in den Versionshinweisen angegeben und in den Vorgehensweisen beschrieben. Wenn Sie eine genaue Uhr und eine einfache Möglichkeit zur Systemzeitkonfiguration benötigen, besteht die einzige Umgehungslösung darin, die Zeit per YAST von Hand zu ändern. Informationen zur manuellen Zeitumstellung finden Sie in der Dokumentation der Zeitsynchronisation. Lesen Sie die Anleitung und die Einschränkungen aufmerksam durch (siehe [Chapter 8, "Zeitsynchronisation"](#)).

- 2) Frage: In früheren Versionen konnte die Uhrzeit mühelos mit OpenScape 4000 Assistant geändert werden. Das ist jetzt nicht mehr möglich. Das Konzept der Zeiteinstellung im Host-Betriebssystem ist klar, aber jetzt müssen die Kunden SSH und YAST lernen. Um ihnen dies zu ermöglichen, muss ich ihnen Root-Zugriff auf das Linux gewähren. Das ist nicht an allen Fällen wünschenswert. Warum wird keine Möglichkeit zur Zeiteinstellung über OpenScape 4000 Assistant bereitgestellt?

Antwort: Es gibt keine andere Möglichkeit, die Zeit zu ändern, als durch eine NTP-Synchronisierung oder von Hand per YAST.

- 3) Frage: Wie werden die Telefone nach dem Ändern der Uhrzeit synchronisiert?

Antwort: Die Uhrzeit im Telefondisplay wird einmal täglich über Nacht synchronisiert. Bei aktivierter SPE ist NTP unbedingt erforderlich.

- 4) Frage: Welche Zeitquelle wird in OpenScape 4000 verwendet?

Antwort: Das neue Uhrzeitkonzept von HiPath 4000 V6 basiert auf NTP. Dies ist bei Servern das normale Standardkonzept. NTP-Server können sowohl auf Linux-Rechnern als auch auf Windows-Rechnern eingerichtet werden. Selbst einige Router verfügen über verlässliche Uhren. Sie können sogar NTP-Relays für Übergänge zwischen verschiedenen Subnetzen einrichten.

- 5) Frage: In Russland wird die Umstellung zwischen Sommer- und Winterzeit abgeschafft. Im März wird die Uhr zum letzten Mal auf Sommerzeit umgestellt, danach erfolgt keine Umstellung mehr. Wie lässt sich die Zeitumstellung in OpenScape 4000 deaktivieren?

Antwort: Stellen sie einfach auf dem OpenScape 4000-Host und in OpenScape 4000 Assistant die richtige Zeitzone ein (UTC+3:00 d. h. "ETC/GMT -3", für die keine Sommerzeit vorgesehen ist). Mehr ist nicht nötig, da die Zeitumstellung von OpenScape 4000 Assistant gesteuert wird.

- 6) Frage: Warum funktioniert die Synchronisierung mit dem Windows SNTP-Server nicht?

Antwort: Windows beinhaltet standardmäßig keinen NTP-Server. Es stellt die SNTP-Implementierung von Microsoft bereit, eine abgespeckte Version, der viele der in der vollständigen Implementierung enthaltenen Funktionen und Sicherheitsmaßnahmen fehlen. Die Version von Microsoft ist, abgesehen von den neuesten Releases, nicht mit dem SNTP-Standard RFC-2030 konform. Systeme mit SNTP sind nur dann als Server geeignet, wenn sie mit einem Hardware-Referenztaktgeber (zum Beispiel einem GPS-Taktempfänger) verbunden sind.

- 7) Frage: Im Internet ist zu lesen, dass Microsoft-Server für die Verwendung von NTP konfiguriert werden können. Ist diese Information korrekt und wird NTP tatsächlich unterstützt? Antwort: Jede beliebige stabile NTP-Quelle wird unterstützt. Microsoft stellt einen Knowledgebase-Artikel zur Konfiguration von Windows-Servern als autorisierende Zeitserver bereit (<https://support.microsoft.com/en-us/kb/816042>). Darüber hinaus muss der Wert des Parameters LocalClockDispersion unbedingt von 10 auf 0 geändert werden, damit die NTP-Synchronisation erfolgreich verlaufen kann (<https://technet.microsoft.com/en-us/library/cc782681%28v=ws.10%29.aspx?f=255&MSPPErr=-2147217396>)

13.5 Lizenzierung

- 1) Frage: CSTA-Lizenzinformationen?

Antwort: Es können maximal 4 Adapter konfiguriert werden. Pro Adapter können maximal 4 Applikationen konfiguriert werden. Für CAP-Lizenzen stehen drei Optionen zur Verfügung:

- a) Keine Lizenz

Bis zu 100 Monitor-Ports

Uneingeschränkte Lizenz

Lizenzen sind nicht für Unify-Applikationen, sondern nur für Applikationen anderer Hersteller erforderlich. Die Lizenz basiert auf der MAC-Adresse des OpenScape 4000-Systems (also nicht auf der MAC-Adresse der CSTA VM) und wird über OpenScape 4000 Assistant importiert.

Wichtig: Ab OpenScape 4000 V7 wird keine CSTA-Lizenz mehr benötigt.

- 2) Frage: Gibt es eine Möglichkeit, von der GUI aus (also nicht anhand von Protokollen) festzustellen, ob und welche Lizenz installiert ist bzw. verwendet wird?

Antwort: Diese Funktion ist geplant und soll mit einem kommenden HF/FR/MR in OpenScape 4000 implementiert werden.

Wichtig: Ab OpenScape 4000 V7 wird keine CSTA-Lizenz mehr benötigt.

- 3) Frage: Wird nach dem Austausch einer DSCXL2-Baugruppe / eines EcoServer / eines Servers eine neue Lizenz benötigt?

Antwort: Die neue Hardware weist eine andere MAC-Adresse auf. Deshalb ist eine neue Lizenzdatei erforderlich. Da die System-ID nicht geändert wird, kann die Lizenz mit der neuen MAC-Adresse wieder über den CLS/CLM-Account gehostet werden.

13.6 Hardwarefehler

- 1) Frage: Was ist, wenn meine Festplatten-Hardware ausfällt?

Antwort: Jeder Festplatten-Hardwarefehler muss an GVS gemeldet werden.

- 2) Frage: Wie gut ist SUSE SLES gegen Stromausfälle geschützt?

Antwort: So gut wie der ext3-Dateisystemmechanismus. Dieses Linux-Plattformsystem basiert auf einem ext3 Journaling-Dateisystem. Die Linux-Plattform verwendet die Journaling-Standardstufe „medium risk“ (mittelhohes Risiko).

- 3) Frage: Wenn die Festplatte im oberen EBT des HDTR ausfällt, muss die Festplatte vor dem Auswerfen des Datenträgers abgemeldet werden?

Antwort: In Platform Portal Maintenance ist eine Schaltfläche zum Entfernen zu sehen, wenn beide Festplatten synchronisiert sind. Klicken Sie nach Möglichkeit auf diese Schaltfläche, bevor Sie die Festplatte entfernen. Falls die Festplatte nicht in der Liste aufgeführt sein sollte, was nach einem Festplattenfehler vorkommen kann, lässt sie sich jedoch auch manuell entfernen.

14 Glossar

A

Aktiver/m Knoten

Der aktive Knoten ist der Knoten auf dem ADP, OpenScape 4000 Assistant und OpenScape 4000 CSTA laufen.

I

IP-Adressen des Hostsystem

IP-Adressen für die Backup-Konfiguration in OpenScape 4000 Assistant.

E

Einzelknoten-Deployment

Folgende Einzelknoten-Deployments sind möglich: Simplex, Simplex mit integriertem OpenScape 4000 SoftGate, Standalone OpenScape 4000 SoftGate, Survivable OpenScape 4000 SoftGate, OpenScape Access, Survivable OpenScape Access, RG 8350 a, APE

Index

B

Bond-Konfiguration [227](#)

E

Erstinstallation

Voraussetzungen [7](#)

Erstinstallations-Skript [195](#)

H

Häufig gestellte Fragen (FAQ) [231](#)

I

Infrastrukturplanungstabellen (leer) [193](#)

IP-Konfigurationsänderung mit dem Recover-/

Reconfiguration-Tool [175](#)

IP-Konfigurationsänderung über OpenScape 4000 Plattform

Administration (Portal) [160](#)

K

Konfiguration ändern [159](#)

L

Lizenzierung [178](#)

M

Migration [120](#)

logisches Backup speichern [123](#)

Reinstallation/Aktualisierung der Remote-Appliance
(RAR) [121](#)

O

OpenScape 4000 Appliance-Software-Lizenz JeOS [181](#)

R

Reinstallation/Aktualisierung der Remote-Appliance (RAR)
[121](#)

V

VLAN-Konfiguration [227](#)

X

XML-Konfigurationsdatei [195](#)

Format [203](#)

Name [203](#)

Netzmaske [223](#)

Parameter [205](#)

Präfixlänge [223](#)

Regeln [218](#)

Verzeichnis [203](#)

Zeitzonewerte [223](#)

