A MITEL
PRODUCT
GUIDE

Unify OpenScape 4000 Assistant/Manager

Webmin Base Administration

Administratordokumentation
07/2024

A31003-H34B0-M129-02-00A9

Mitel

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.

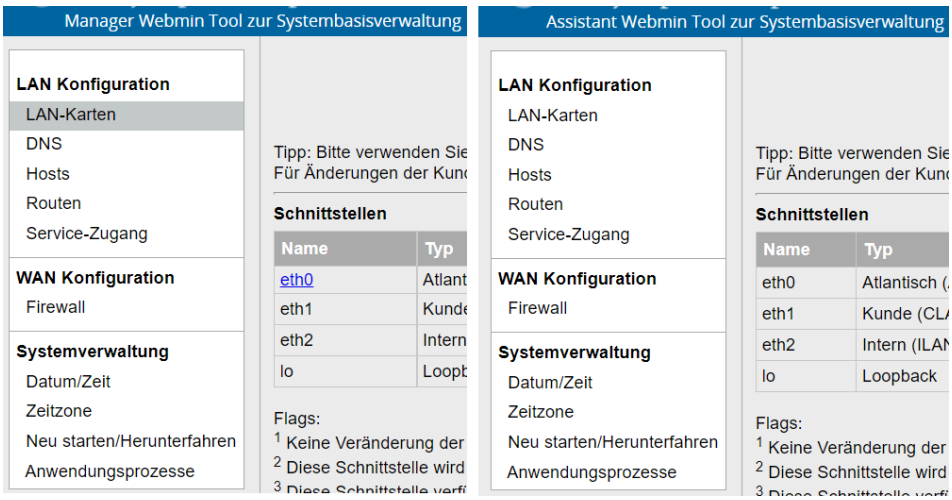
Inhalt

1 Übersicht

Webmin ist die Basis-Administrationsfunktion für die Konfiguration der Systemressourcen, des TCP-Netzwerks in Linux. Webmin wird auch für die Bedienung im laufenden Betrieb eingesetzt, beispielsweise für das Herunterfahren des Systems.

Webmin wird aus der OpenScape 4000 Manager/Assistant Startseite heraus über **Basis Administration** -> **Webmin** aufgerufen.

2 Startseite/linke Navigationsleiste



Funktionsübersicht

LAN Konfiguration

- LAN-Karten
- DNS
- Hosts
- Routen
- Service-Zugang

WAN Konfiguration (nur Assistant)

- Firewall

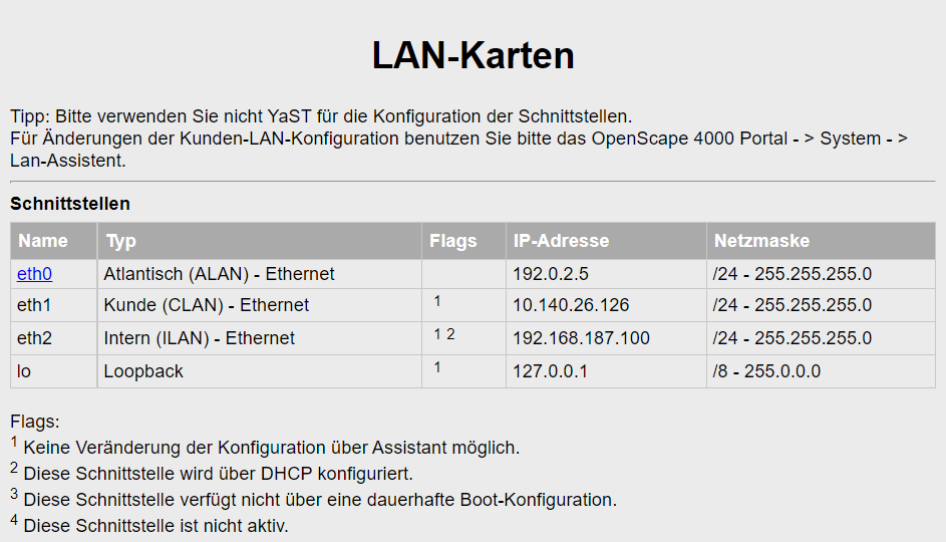
Systemverwaltung

- Datum/Zeit
- Zeitzone
- Neu starten/Herunterfahren
- Anwendungsprozesse

Andere Webmin-Funktionen

- Webmin-Protokoll

3 LAN-Karten



LAN-Karten

Tipp: Bitte verwenden Sie nicht YaST für die Konfiguration der Schnittstellen.
Für Änderungen der Kunden-LAN-Konfiguration benutzen Sie bitte das OpenScape 4000 Portal - > System - > Lan-Assistent.

Schnittstellen

Name	Typ	Flags	IP-Adresse	Netzmaske
eth0	Atlantisch (ALAN) - Ethernet		192.0.2.5	/24 - 255.255.255.0
eth1	Kunde (CLAN) - Ethernet	1	10.140.26.126	/24 - 255.255.255.0
eth2	Intern (ILAN) - Ethernet	1 2	192.168.187.100	/24 - 255.255.255.0
lo	Loopback	1	127.0.0.1	/8 - 255.0.0.0

Flags:
1 Keine Veränderung der Konfiguration über Assistant möglich.
2 Diese Schnittstelle wird über DHCP konfiguriert.
3 Diese Schnittstelle verfügt nicht über eine dauerhafte Boot-Konfiguration.
4 Diese Schnittstelle ist nicht aktiv.

Im **Assistant** kann die aktuelle Konfiguration der LAN-Karten lediglich angesehen werden.

In der Spalte **Typ** der Tabelle **Konfigurierte Schnittstellen** werden drei Netzwerktypen unterschieden:

- ALAN
- CLAN und
- ILAN.

Die kundenseitige LAN-Adresse für den Assistant muss jedoch per LAN-Wizard am OpenScape 4000-Portal konfiguriert werden. Im Assistant wird diese Adresse dann automatisch eingestellt. Während des Linux-Starts überprüft der Assistant ebenso die Kunden-LAN-Adresse im OpenScape 4000-Portal und konfiguriert sich eigenständig, falls eine Änderung über den LAN-Wizard erfolgte.

Anmerkung: OpenScape 4000 **Assistant**: Verwenden Sie **nicht** YaST zur Konfigurierung der LAN-Karte(n), da dies die Konfigurierungsdateien beschädigt.

Bei der Konfigurierung der LAN-Karte des Kunden am Manager müssen Sie eine Adresse innerhalb der Kunden-LANs spezifizieren, die vom Administrator des Kunden-LANs vergeben wird, sowie eine Netzmasken- und eine Broadcast-Adresse. Am Manager können mehrere LAN-Karten konfiguriert werden.

Die LAN-Karte wird gleichzeitig konfiguriert und aktiviert. Nach dem Neustart sind alle LAN-Karten automatisch aktiv.

Dieses Kapitel behandelt folgende Themen:

3.1 Parameter

- **Adresse**

  Jeder LAN-Karte muss eine eindeutige Adresse innerhalb des Kunden-LAN-Adressbereichs zugewiesen werden. Dieser Adressbereich ist vom LAN-Administrator des Kunden zu definieren.
- **Netzmaske**

  Die Netzmaske hängt von der Klasse der LAN-Karten-Adresse ab. So lautet beispielsweise die Netzmaske für eine Adresse der Klasse C 255.255.255.0. Die Netzmaske ist vom LAN-Administrator des Kunden zu definieren.
- **Broadcast**

  Die Broadcast-Adresse wird dazu benutzt, ein Datagramm-Paket durch das Netzwerk zu leiten, beispielsweise um die IP-Adresse eines Routers bekannt zu machen. Die Broadcast-Adresse hängt von der Adresse der LAN-Karte ab. So kann beispielsweise für die LAN-Karten-Adresse 218.100.200.204 die Broadcast-Adresse 218.100.200.255 lauten. Diese wird von der IP-Adresse der LAN-Karte und der Netzmaske abgeleitet.

3.2 Funktionen

Anmerkung: Wo nicht gesondert vermerkt, gilt der jeweilige Abschnitt sowohl für den Assistanten als auch für den Manager.

3.2.1 Eine neue LAN-Karte konfigurieren (nur Manager)

Um eine **neue** LAN-Karte zu konfigurieren, können Sie die Liste Nicht konfigurierter Schnittstellen benutzen.

- Wenn Sie den Namen der LAN-Karte (z.B. eth1) anklicken, erscheint die Seite **Schnittstelle erstellen** . Der Name der LAN-Karte ist bereits ausgefüllt.
  - Wenn die Karte, die Sie konfigurieren wollen, *nicht* in der Liste **Nicht konfigurierte Schnittstellen** eingetragen ist, können Sie auf **Eine neue Schnittstelle hinzufügen** klicken und den Kartennamen manuell angeben.

- Wenn Sie wollen, dass die Karte die IP-Adresse vom DHCP-Server erhält, dann wählen Sie bitte die Option **Von DHCP**.

- Wenn Sie eine statische IP-Adresse setzen wollen, wählen Sie bitte die Option **oder** und tragen Sie **IP-Adresse**, **Netzmaske** und **Broadcast** in die entsprechenden Felder ein.
- Klicken Sie auf der Schaltfläche **Erstellen**, wenn alle Einträge vollständig sind.

  Ihre Konfigurationen sind nun gespeichert, werden aber erst dann wirksam, wenn Sie die nachfolgende Dialogbox bestätigen.

  In dieser Dialogbox werden Sie gefragt, ob die Aktivierung der neuen Schnittstelle zusammen mit dem Neustart aller OpenScape 4000 Dienste erfolgen soll, damit die Dienste über die neue Schnittstelle arbeiten.

  – Klicken Sie auf **Ja**, um sofort die Schnittstelle zu aktivieren und um alle Dienste neu zu starten
  – Klicken Sie auf **Nein**, wenn Sie die Schnittstelle später aktivieren wollen. In diesem Fall würde die Aktivierung automatisch nach einem Neustart des Systems erfolgen.

3.2.2 Aktivieren einer LAN-Karte

Konfigurierte LAN-Karten, die momentan nicht aktiv sind, werden mit einem Stern markiert.

- Sie können die LAN-Karte **aktivieren**, indem Sie auf den Kartennamen in der Tabelle Konfigurierte Schnittstellen klicken.

  Die Schnittstellenaktivierung wird wirksam, sobald Sie die Schnittstellenkonfiguration durch Klicken auf der Schaltfläche **Speichern** erneut sichern und anschliessend bestätigen, dass die Schnittstelle aktiviert und die Dienste neu gestartet werden sollen.

3.2.3 Löschen einer LAN-Karte (nur Manager)

- Sie können eine LAN-Kartenkonfiguration **löschen**, indem Sie auf den bestimmten LAN-Kartennamen in der Tabelle **Konfigurierte Schnittstellen** klicken und dann auf Löschen auf der Seite Schnittstelle aktualisieren.

  Das Löschen erfolgt sofort.

3.2.4 Ansicht und Ändern der LAN-Karteneigenschaften (nur Manager)

- Sie können die **Eigenschaften** der ausgewählten LAN-Karte ansehen und ändern, indem Sie auf den bestimmten LAN-Kartennamen in der Tabelle Konfigurierte Schnittstellen klicken.
- Dann können Sie die Konfigurationparameter der LAN-Karte auf der Seite **Schnittstelle aktualisieren** ändern. Klicken Sie auf der Schaltfläche **Speichern**, wenn die Einträge vollständig sind.

  Die Änderungen werden erst dann wirksam, wenn Sie die Dialog Box bestätigen, die nach Betätigung der Schaltfläche **Speichern** erscheint .

  In dieser Dialog Box werden Sie aufgefordert, die Konfigurationsänderungen und den Neustart aller Dienste zu bestätigen, damit die Dienste über die neue Schnittstelle arbeiten.

  – Klicken Sie auf **Ja**, um sofort die Schnittstelle zu aktivieren und um alle Dienste neu zu starten.
  – Klicken Sie auf **Nein**, wenn Sie die Schnittstelle nicht sofort aktivieren wollen. In diesem Fall würde die Aktivierung automatisch nach einem Neustart des Systems erfolgen.

    Wenn Sie die für Ihre aktuelle Verbindung verwendete IP-Adresse ändern, wird nach Bestätigung der zuvor erwähnten Dialog Box (zur Bestätigung der Konfigurationsänderungen und des Neustarts der Dienste), sofort das Browser-Fenster geschlossen.
  – Bestätigen Sie auch die Dialog Box zum Schliessen des Browser-Fensters und warten Sie eine Weile, bevor Sie eine neue Sitzung über die neu konfigurierte IP-Adresse beginnen. Der Server wird erst dann reagieren, wenn alle Dienste gestartet wurden.

Anmerkung: Wenn SSO läuft und diese LAN-Karte im SSO benutzt wird, kann diese nicht im DHCP-Modus konfiguriert werden.

3.2.5 Virtuelle LAN -Schnittstellen hinzufügen (nur Manager)

- Sie können Virtuelle LAN-Schnittstellen (nur Manager) zu einer bereits konfigurierten LAN-Karte hinzufügen, indem Sie auf **Virtuelle Schnittstelle hinzufügen** auf der Seite **Schnittstelle aktualisieren** klicken.
- Sobald die Seite **Schnittstelle erstellen** erscheint, tragen Sie **Name**, **IP-Adresse**, **Netzmaske** und **Broadcast** in die entsprechenden Felder ein.
- Klicken Sie auf **Erstellen**, wenn die Änderungen vollständig sind.

  Die neue virtuelle Schnittstelle wird sofort aktiviert. Sie werden gefragt, ob Sie alle Dienste sofort neu starten wollen, damit diese mit der neuen virtuellen Schnittstellen funktionieren.

  Eine oder mehrere virtuelle Schnittstellen können zu einer echten Schnittstelle hinzugefügt werden, indem Sie den Link **Virtuelle Schnittstelle hinzufügen** wiederholt benutzen.

3.3 Virtuelle LAN-Schnittstellen (nur Manager)

Falls Sie mehrere IP-Adressen einer LAN-Karte zuordnen wollen, können Sie virtuelle LAN-Schnittstellen dieser Karte hinzufügen (siehe Funktionen).

"Virtuell" heisst: physikalisch nicht vorhanden, aber auf eine existierende echte Schnittstelle beziehend.

3.4 Beispiel

Eine nicht konfigurierte LAN-Karte muss mit einer IP-Adresse konfiguriert werden, die innerhalb des Adressbereichs für das Kunden-LAN liegt.

Folgende Schritte sind auszuführen:

1) Beschaffen Sie eine IP-Adresse innerhalb des Adressbereichs des Kunden-LAN, beispielsweise 192.1.2.5.
2) Klicken Sie auf den betreffenden LAN-Kartennamen in der Tabelle **Konfigurierte Schnittstellen**.
3) Geben Sie die Angaben für die LAN-Kartenkonfiguration auf der Seite **Schnittstelle erstellen** wie folgt ein:

   IP-Adresse: 192.1.2.5

   Netzmaske: 255.255.255.0

   Broadcast: 192.1.2.255
4) Klicken Sie auf **Erstellen**.

4 DNS

Ist das System mit einem Kunden-LAN verbunden, in dem der DNS-Dienst (**D**omain **N**ame **S**ervice) benutzt wird, kann der Server als Client für die Nutzung dieses DNS-Dienstes konfiguriert werden.

Dieses Kapitel behandelt folgende Themen:

4.1 Parameter

- **Hostname**

  Der Hostname ist der Name dieser Maschine. Dieser Name wird von vielen der Netzwerkprogrammen benutzt, um die Maschine zu identifizieren.
- **Auflösungsreihenfolge**

  Neben dem DNS-Dienst (Domain Name Service) gibt es andere Namensdienste, wie der NIS-Dienst (Network Information Service), der für die Namensauflösung benutzt werden kann. Die Auflösungsreihenfolge bestimmt, welcher Dienst zuerst und welcher danach benutzt werden sollte. Die ersten zwei Dienste sind für Hosts und DNS bestimmt, und die drei restlichen können für NIS, NIS+ oder DB benutzt werden.
- **DNS-Server**

  Geben Sie die IP-Adresse(n) des/der DNS-Server(s) an. Sie erhalten diese vom Administrator des Kunden-LAN. Es können bis zu drei DNS-Server definiert werden. Um einen Hostnamen oder eine IP-Adresse aufzulösen, wird erst der erste DNS-Serverin der Reihenfolge aufgelöst, anschliessend der nächste und so weiter, bis kein DNS-Server mehr vorhanden ist. Um mit DNS arbeiten zu können, muss mindestens ein DNS-Server konfiguriert sein. Die beiden übrigen können konfiguriert werden. Werden keine IP-Adressen angegeben, wird das Linux-System ohne Nutzung von DNS konfiguriert.

  Am **Assistant** wird die Adresse des DNS-Servers des OpenScape 4000-Portals automatisch per DHCP eingestellt. *Ändern Sie diese Einstellung*

nicht, so lange keine Probleme mit der DNS-Auflösung in Erscheinung treten.

Wird eine der LAN-Karten so konfiguriert, dass DHCP (siehe Funktionen der LAN-Karte) benutzt wird, können **DNS-Server** und **Suchdomänen** von DHCP konfiguriert werden

- **Suchdomänen**

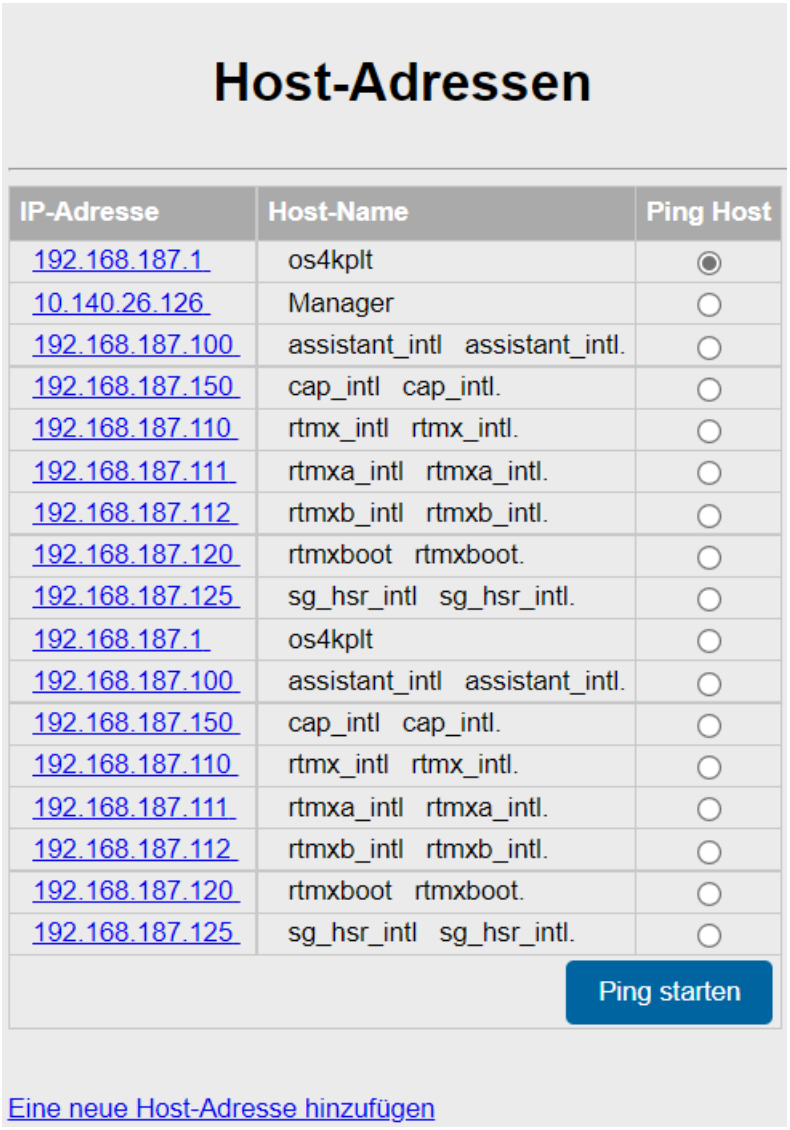
  Wird der Kurzname (ohne den Domänensuffix) des Hosts gesucht, fragt der Resolver den Namen bezüglich der Domänennamen in der Suchliste ab. Wenn die Option **Aufgelistet** ausgewählt und eine einzelne Domäne angegeben ist, so wird die lokale Domäne betrachtet. Falls Sie die Suchliste erweitern wollen, können Sie weitere Domänennamen im Feld **Suchdomänen** hinzufügen. Der Resolver wird jede Domäne in der Liste, bis eine Übereinstimmung gefunden wird, durchsuchen.

Anmerkung: Sie erhalten den Namen der lokalen Domäne vom Administrator des Kunden-LAN.

4.2 Funktionen

- Sie können **den Manager/Assistant als DNS-Client konfigurieren**, indem Sie die Option **Aufgelistet** auswählen und den/die Domänennamen in das Feld **Suchdomänen** eintragen.
  - Bitte tragen Sie die IP-Adresse(n) des (der) DNS-Server(s) in das Feld **DNS-Server** ein.
  - Sie können zusätzliche Namensdienste im Feld **Auflösungsreihenfolge** angeben.
  - Klicken Sie auf **Speichern**, um die Konfiguration abzuschliessen.
- **Löschen** Sie alle Domänen, indem Sie die Option **Keine** auswählen und auf **Speichern** klicken.
- Soll **DNS nicht mehr benutzt werden**, löschen Sie alle Server-Adressen und klicken Sie auf **Speichern**.
- Um eine **existierende DNS-Konfiguration zu modifizieren**, ändern Sie die betreffenden Felder und klicken Sie auf **Speichern**.

5 Hosts



Dieses Kapitel geht auf die Konfiguration von Hosts, wie Alias-Hosts, Firewalls, usw., ein. Zum Konfigurieren eines Hosts muss der IP-Adresse des betreffenden Hosts ein Name zugeordnet werden, beispielsweise Pluto zu 139.1.2.40. Danach kann der Host mit seinem Namen angesprochen werden. Netzwerk-Routinen verwenden diese Host-Konfigurationsdaten für die Umsetzung von Namen und IP-Adressen.

Dieses Kapitel behandelt folgende Themen:

- Parameter
- Funktionen
- Beispiel

5.1 Parameter

- **Host-Namen**

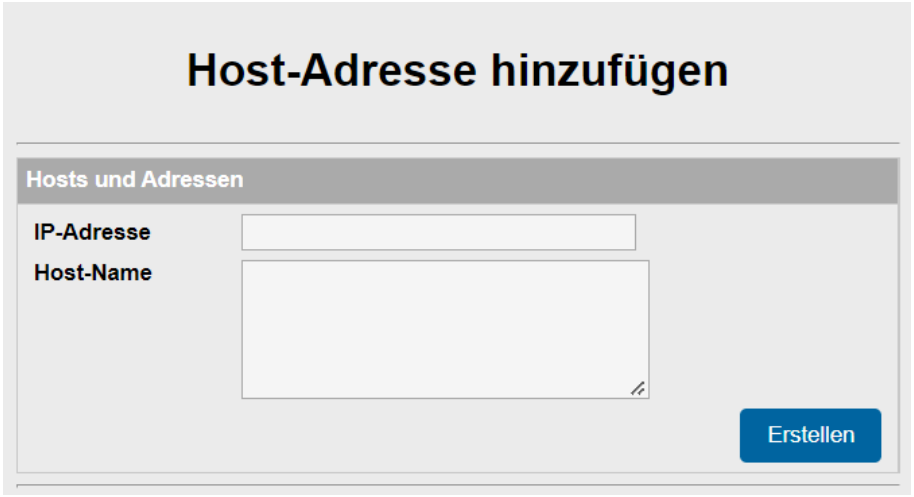
  Jeder Name muss eindeutig sein. Er umfasst maximal 50 Zeichen.
- **IP-Adresse**

  Bezeichnet die IP-Adresse des Hosts.

5.2 Funktionen

Einen Host hinzufügen

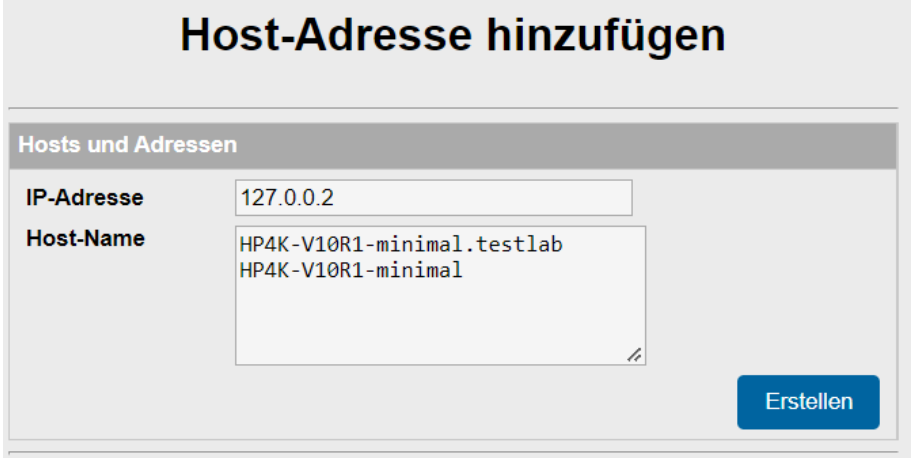
- Sie können einen Host **hinzufügen**, indem Sie auf Eine neue Hostadresse hinzufügen klicken.



- Klicken Sie auf **Erstellen**, wenn alle Einträge vollständig sind.

Einen Host löschen

- Sie können einen Host **löschen**, indem Sie seine IP-Adresse anklicken und anschliessend auf Löschen auf der Seite **Host-Adresse aktualisieren** klicken.



Anmerkung: Vorsicht! Am **Assistant** sind besondere Standard-Einträge für Hosts eingestellt, die nicht gelöscht

werden dürfen! Dies sind: ADP-RMX, WAML, ADP-UNIX, os4kplt, cap_intl.

- Sie können die **Host-Verbindung prüfen**, indem Sie den betreffenden Host auswählen und auf Ping starten klicken.

5.3 Beispiel

Für einen an das Kunden-LAN (beispielsweise Jupiter) angeschlossenen Host ist ein Host-Name zu konfigurieren.

Dazu müssen folgende Schritte ausgeführt werden:

1) Beschaffen Sie eine IP-Adresse innerhalb des Adressbereichsdes Kunden-LAN, beispielsweise 191.1.2.6.

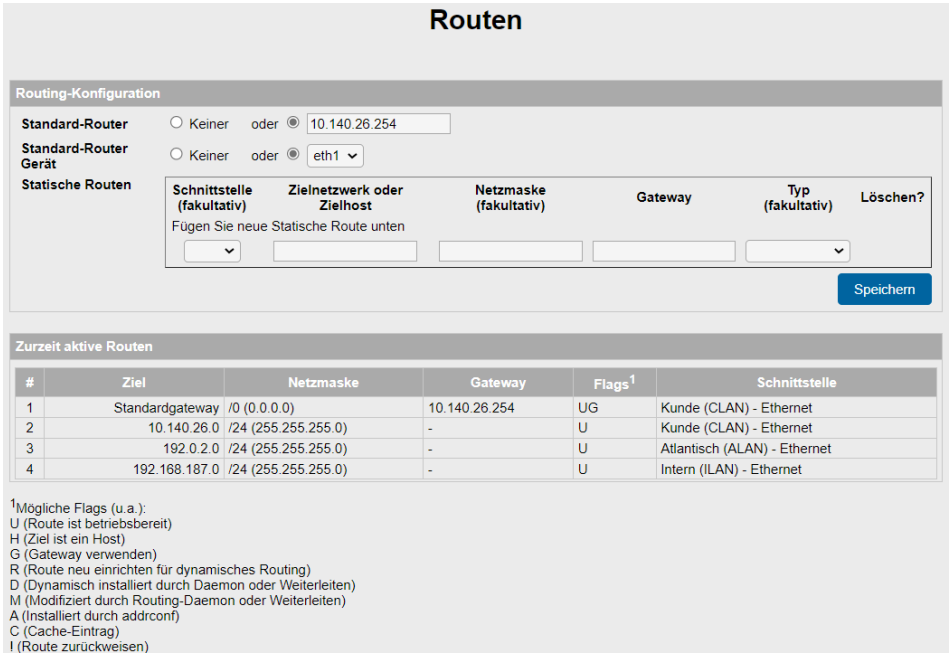
2) Fügen Sie einen Host-Namen mit folgenden Parameter hinzu:

Name: Jupiter

Adresse: 191.1.2.6

3) Klicken Sie auf **Erstellen**.

6 Routen



Dieser Abschnitt beschreibt die Konfiguration von Routen, die für den Austausch von Daten zwischen Hosts in verschiedenen Netzwerken benötigt werden. Für den Austausch von Routing-Informationen und die Weiterleitung von Daten von einem Netzwerk zu einem Ziel in einem andern sind bestimmte Hosts, so genannte "Gateways" verantwortlich.

Die Tabelle unter **Routing-Konfiguration** enthält ausschliesslich die statischen Routen unter Linux. Alle aktiven Routen, einschließlich der dynamisch konfigurierten (beispielsweise über DHCP), werden in der Tabelle unter **Zurzeit aktive Routen** angezeigt.

Es kann eine Standardroute konfiguriert werden, die benutzt wird, wenn keine andere Route zutrifft. Diese Standard-Route bestimmt das Standard-Gateway, an das die IP-Pakete weitergeleitet werden.

Vorsicht: Für den Assistant wird der Standard-Router über den LAN-Wizard am OpenSape 4000-Portal konfiguriert. Die Konfigurierung am Assistand wird anschließend automatisch durchgeführt. **Nehmen Sie Änderungen hier nur in außerordentlich begründeten Fällen vor.**

Auf Routen kann auch eine Netzmaske angewendet werden. Dieses Feld ist optional und sollte in den meisten Fällen leer bleiben. Bei komplexen Routing-Anforderungen kann es erforderlich sein, dass eine Netzmaske auf eine bestimmte Route angewendet wird. Dadurch ist es möglich, eine Route als Subnetz des Kundennetzes einzurichten.

Dieses Kapitel behandelt folgende Themen:

6.1 Route-Parameter

- **Schnittstelle**

  Tragen Sie eine LAN-Schnittstelle in dieses Feld ein, um die Verbindung zwischen Route und der angegebenen LAN-Schnittstelle (z.B. eth0) zu erzwingen, sonst wird das Routing-Verfahren versuchen, das Gerät selbst zu bestimmen. In den meisten Netzen werden Sie dies nicht benötigen.
- **Netzwerk**

  Das Feld Netzwerk gibt den Ziel-Host oder das Netzwerk an. Für eine Host-Route muss die IP-Adresse des Hosts angegeben werden. Für eine Netzroute muss die Netzadresse angegeben werden.
- **Netzmaske**

  Dies muss ein Wert sein, der einen bestimmten Teil der IP-Adresse des Zielfeldes ausblendet und so eine Route zu einem Subnetz einrichtet, dass das angegebene Gateway verwendet wird. Das Feld muss mit einem Wert belegt sein, der bei Umsetzung in einen Binärwert einen Wert mit lauter Einsen gefolgt von **ausschliesslich** Nullen (d.h. nicht gemischt) ergibt. Der Abschnitt "Beispiele" enthält ein Beispiel hierfür (siehe Beispiele).
- **Gateway**

  Gibt die IP-Adresse des Gateway an. Das Gateway muss erreichbar sein.
- **Typ**

  Sie können den Route-Typ in diesem Feld eintragen.

  Die meist verwendeten Typen sind:

  – **Unerreichbar**

    Bewirkt, dass die Ziele unerreichbar werden. Pakete zu diesem Ziel werden verworfen und die Meldung "Host unerreichbar" wird erzeugt.
  – **Schwarzes Loch**

    Diese Ziele sind unerreichbar. Pakete werden ohne Rückmeldung verworfen.
  – **Lokal**

    Die Ziele werden diesem Host zugeordnet. Die Pakete werden gespiegelt und lokal ausgeliefert.
  – **Broadcast**

    Die Ziele sind Broadcast-Adressen. Die Pakete werden als Link-Broadcasts gesendet.

6.2 Funktionen

- Sie können einen **Standard-Router** manuell **einstellen**, indem Sie die Option "oder" für den Standard-Router auswählen. Tragen Sie die IP-Adresse des Standard-Gateway ein. Sie können auch den Namen des **Standard-Router Gerät**s eintragen, indem Sie die Option "oder" im Feld **Standard-Router Gerät** auswählen.
- Sie können diesen Host **als einen Router** für andere Systeme bestimmen, indem Sie die Option **Ja** auswählen.
- Sie können eine Route **hinzufügen**, indem Sie die Route-Parameter in der letzten Zeile der Tabelle eintragen. Klicken Sie auf **Speichern**, wenn

die Einträge vollständig sind. Die Seite wird neu geladen und Sie können weitere Routen hinzufügen.

- Sie können eine vorhandene Route **ändern**, indem Sie Felder ändern und danach auf **Speichern** klicken.
- Sie können eine Route löschen, indem Sie alle Felder einer Zeile in der Tabelle leeren und danach auf Speichern klicken.

  Ihre Konfigurationen sind nun gespeichert, werden aber erst dann wirksam, wenn Sie die nachfolgende Dialogbox bestätigen.

  In dieser Dialogbox werden Sie gefragt, ob die Änderungen zusammen mit dem Neustart aller OpenScape 4000-Dienste erfolgen sollen.

  – Klicken Sie auf **Ja**, um die Änderungen sofort zu aktivieren und um alle Dienste neu zu starten
  – Klicken Sie auf auf **Nein**, wenn Sie die Änderungen später aktivieren wollen. In diesem Fall würden die Aktivierungen automatisch nach einem Neustart des Systems erfolgen.

6.3 Beispiele

Beispiel - Eine Host-Route hinzufügen

Für einen an das Kunden-LAN verbunden ist (beispielsweise Jupiter) angeschlossenen Host ist eine Host-Route zu konfigurieren.

Dazu müssen folgende Schritte ausgeführt werden:

1) Beschaffen Sie eine IP-Adresse innerhalb des Adressbereichs des Kunden-LAN, beispielsweise 191.1.2.6 und die Gateway-Adresse 191.1.2.40.

2) Fügen Sie die Host-Route mit folgenden Parametern hinzu:

Ziel: 191.1.2.6

Gateway: 191.1.2.40

Beispiel - Verwenden einer Route mit einer Netzmaske

Wenn ein Kunde eine Route zu einem Subnetz des LANs (z.B. 138.223.236.z) benötigt, um ein anderes Gateway als das Standard-Gateway zu verwenden, würde beim Hinzufügen der Route 138.223.236.0 nur eine Route zu diesem bestimmten Host eingerichtet.

Um eine Netz-Route zum 138.223.236.z Subnetz-Adressbereich einzurichten, muss eine Netzmaske vom Typ 255.255.255.0 benutzt werden. Das Festlegen des richtigen Netzmaskenwerts erfordert eine genaue Kenntnis des Kundennetzes und sollte nur mit Unterstützung des LAN-Administrators des Kunden durchgeführt werden.

Der binäre Wert des Netzmaskenwert wird mit einer Zieladresse bitweise logisch UND verknüpft (z.B. 138.223.236.9). Dadurch wird der Netzteil der Adresse ermittelt - in unserem Fall ergibt sich bei Verknüpfung der Netzmaske 255.255.255.0 mit 138.223.236.9 der Wert 138.223.236.0.

Mit dem Ergebnis dieser Operation wird dann richtige Gateway-Adresse aus der Routing-Tabelle ermittelt, d.h. die Route zum Ziel 138.223.236.0, die über das Gateway 139.2.54.56 führt.

In diesem Fall sind folgende Schritte auszuführen:

1) Besorgen Sie sich beim LAN-Administrator des Kunden eine IP-Adresse, die im Subnetz-Bereich des Kundennetzes liegt (z.B. 138.223.236.0), die Gateway-Adresse (z.B. 139.2.54.56) und einen Netzmaskenwert (z.B. 255.255.255.0).
2) Fügen Sie die Host-Route mit folgenden Parametern hinzu:

   Ziel: 138.223.236.0

   Gateway: 139.2.54.56

   Netzmaske: 255.255.255.0

   Die hinzugefügte Route ermöglicht den Zugang zu einer beliebigen IP-Adresse im Bereich zwischen 138.223.236.0 und 138.223.236.255 über das Gateway 139.2.54.56 anstatt über das Standard-Gateway.

7 Service-Zugang

Das Linux-System kann durch den SIRA-Service-Zugang fern verwaltet werden. Im SIRA wird dem System eine individuelle IP-Adresse der Form 10.B.C.D zugeteilt. Die Felder B, C und D müssen diesem OpenScape 4000 Manager/ Assistant spezifisch durch einen Service-Vertreter zugewiesen werden und basieren auf der Anzahl der OpenScape 4000 Assistant Server.

Die SIRA-Adresse ist identisch mit der ehemaligen VPN-Adresse. Die VPN-Adressierungsstruktur wird durch das SPoA/NAT-Konzept ersetzt.

Dieses Kapitel behandelt folgende Themen:

7.1 Funktionen

- Sie können die SIRA-IP-Adresse **hinzufügen**, indem Sie die IP-Adresse eintragen und auf **Erstellen** klicken. Bitte bestätigen Sie das Erstellen der Service-Zugangskonfiguration, indem Sie auf **Service-Zugang-Konfiguration erstellen** klicken. Alle Dienste werden neu gestartet und alle Benutzer, einschliesslich Sie werden getrennt.
- Sie können eine bestehende SIRA-IP-Adresse **ändern**, indem Sie IP-Adressenfelder ändern und auf **Ändern** klicken. Bitte bestätigen Sie die Änderung der Service-Zugangskonfiguration, indem Sie auf **Service-Zugang-Konfiguration ändern** klicken. Alle Dienste werden neu gestartet und alle Benutzer, einschliesslich Sie werden getrennt.
- Sie können die SIRA-IP-Adresse **löschen**, indem Sie auf **Löschen** klicken. Bitte bestätigen Sie das Löschen der Service-Zugangskonfiguration, indem Sie auf **Service-Zugang-Konfiguration löschen** klicken. Alle Dienste werden neu gestartet und alle Benutzer, einschliesslich Sie werden getrennt.

7.2 Beispiel

Auf dem OpenScape 4000 Manager/Assistant, der direkt mit dem RSP (Remote Service-Plattform) verbunden ist, muss die SIRA-Adresse konfiguriert werden.

Zum Beispiel wird die folgende Adresse angegeben: 10.2.191.1

Es müssen folgende Schritte ausgeführt werden:

1) Die SIRA-IP-Adresse 10.2.191.1 in den Adressenfeldern eintragen.
2) Auf **Erstellen** klicken, um den Service-Zugang-Konfiguration zu erstellen.

3) Auf **Service-Zugang-Konfiguration erstellen** klicken.

8 Firewall

8.1 Firewall des Manager

Die Firewall-Seite des Manager hat hauptsächlich informellen Charakter:

Gesamtstatus

Sie können hier nur zwei Optionen ändern:

- SuSE Firewall
- Automatischer SuSE Firewall-Start

  Sie können diese Optionen mit der entsprechende Schaltfläche ein- oder ausschalten.

  Wichtiger hinweis: Es wird dringend empfohlen **beide Optionen immer eingeschaltet zu lassen!**

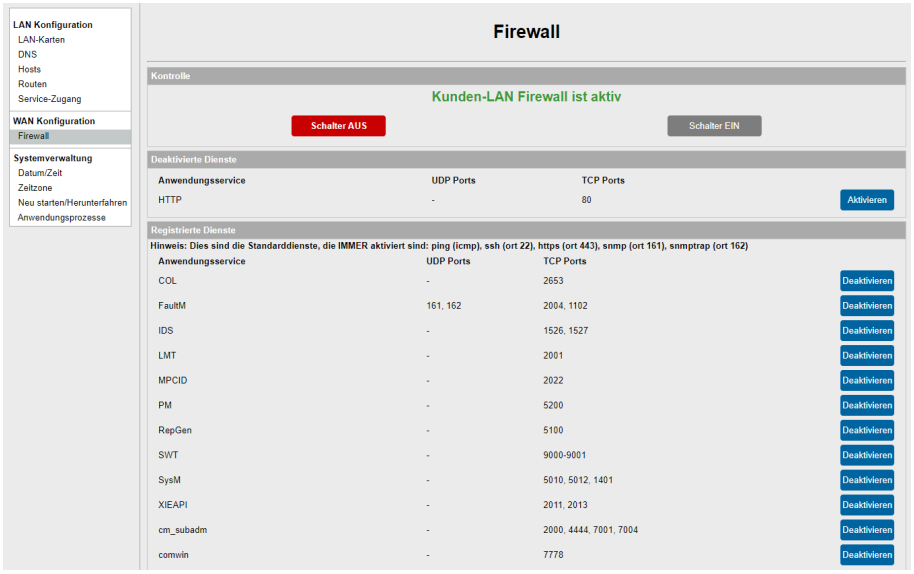
Warnung: Das Ausschalten der SuSE Firewall stellt ein Sicherheitsrisiko dar!

Firewall-Schnittstellen

Diese Teile zeigt an welche Schnittstellen für welche Zone erlaubt sind.

Registrierte Dienste für Externe Zone

Diese Teil zeigt an welche Dienste und Ports für diese Dienste für welche Zone erlaubt sind.



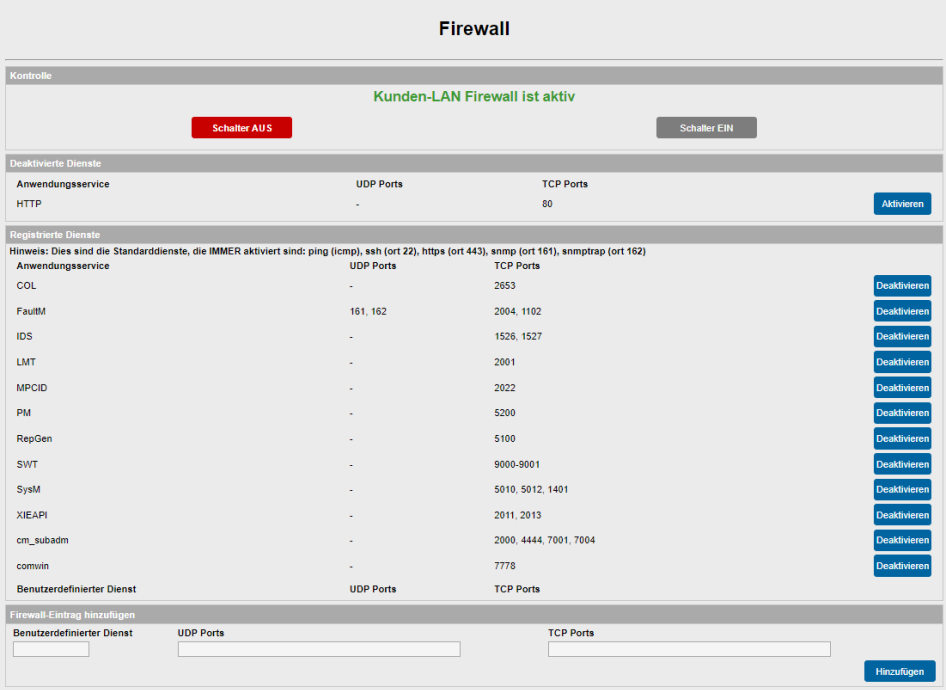
8.2 Firewall des Assistant

Die Firewall des Assistant besteht im allgemeinen aus der ALAN-Firewall (**A**tlantic **LAN**) und der CLAN-Firewall (**C**ustomer **LAN**).

ALAN-Firewall

Die ALAN-Firewall ist ein Adressfilter, der IP-Pakete weiterleitet, die vom CLAN-Host zum ALAN-Host oder ADP weitergeleitet werden. Nur die IP-Pakete vom CLAN-Host, die Zugriffsrechte besitzen, werden weitergeleitet. Alle anderen Pakete werden zurückgewiesen.

Wenn der 'Secure Mode' für ADP (in der Security Mode Konfiguration) eingeschaltet ist, sind ALAN- und ADP-Zugang komplett verboten. Alle Hosts, die in der Firewall erlaubt sind, sind geblockt und kein Host kann hinzugefügt oder gelöscht werden. Die Comwin-Funktionalität ist davon nicht betroffen, da sie im 'Secure Mode' einen anderen Weg beschreitet.



CLAN-Firewall

Die Tabelle **Dynamisch registrierte CLAN Dienste** geben eine Zusammenfassung der CLAN-Firewall.

Die CLAN-Firewall kann hier nicht konfiguriert werden. Es können jedoch gemäß den Einstellungen im 'Secure Mode' - für den Systemshell aus dem CLAN, Remote-ODBC/JDBC-Zugriff usw.- einige Ports geschlossen sein, auch wenn sie in der Tabelle erscheinen.

Benutzer können die Firewall jedoch ein- und ausschalten.

ACHTUNG: Ausschalten der Firewall birgt Sicherheitsrisiken!

Übersicht über die nachfolgenden Abschnitte:

8.2.1 Zugangsberechtigungen

Die folgenden Zugangsberechtigungen sind definiert:

- **ALAN**

  Der Einzelhost oder ein Host aus dem Netz, für das der Firewall-Eintrag definiert ist, erhält Zugang zu allen Hosts im ALAN, mit Ausnahme des OpenScape 4000 Assistant selbst.
- **ADP**

  Der Einzelhost oder ein Host aus dem Netz, für das der Firewall-Eintrag definiert ist, erhält Zugang zum RMX-ADP am OpenScape 4000 Assistant.

Es können eine oder mehrere Zugangsberechtigungen für einen Firewall-Eintrag vergeben werden. Die Obermenge dieser Zugangsberechtigungen bestimmt die erlaubten Kommunikationspfade.

8.2.2 Funktionen

- Um einen Firewall-Eintrag **hinzuzufügen**, geben Sie folgendes an:
  - CLAN Host / Netz:

    Geben Sie die gültige IP-Adresse des Hosts bzw. die Adresse des Netzes an, für den/das die Zugangsberechtigung erteilt werden soll.
  - Netzmaske:

    Aktiviere Sie **Zugang zum ADP (ComWin)**.
  - Klicken Sie auf die Schaltfläche **Hinzufügen**.
- Sie können einen Firewall-Eintrag **löschen**, indem Sie die auf Schaltfläche **Löschen** neben den entsprechenden Eintrag klicken.Sie können die CLAN Firewall **aus- oder einschalten**, indem Sie unter **Kontrolle** auf die Schaltfläche **Schalter AUS** oder **Schalter EIN** klicken.

  Beachten Sie, dassAussachalten der Firewall einSicherheitsrisiko darstellt!

  Schaltfläche **Schalter EIN** = Die CLAN Firewall ist eingeschaltet.
  Schaltfläche **Schalter AUS** = Die CLAN Firewall ist ausgeschaltet.

  Die ALAN-Firewall kann *niemals* ausgeschaltet sein.

8.2.3 Beispiel

Ein Host, z.B. mit dem Namen 'Jupiter', der mit dem Kunden-LAN verbunden ist, benötigt Zugang zum OpenScape 4000 (RMX-ADP) über LAN. Um die Kommunikation zwischen dem OpenScape 4000-Host und dem Host 'Jupiter' zu erlauben, muss ein Firewall-Eintrag für den Host 'Jupiter' erstellt werden.

Hierfür sind die folgenden Schritte notwendig:

1) Beschaffen Sie sich die IP-Adresse dieses Hosts im Kunden-LAN, z.B. 191.1.2.6.

2) Fügen Sie einen Firewall-Eintrag hinzu:

- Tragen Sie die IP-Adresse 191.1.2.6 ins Feld **CLAN Host / Netz** ein.
- Klicken Sie auf die Schaltfläche **Hinzufügen**.

9 Remote Service Platform

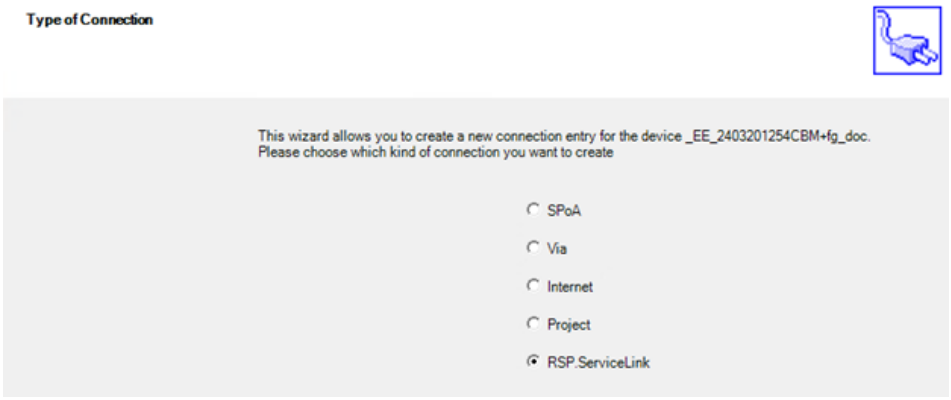
9.1 Überblick

Das RSP-Konzept (Remote Service Platform) erweitert das SIRA-Ökosystem um einen neuen Verbindungskanal, der vom Support für Fernverbindungen zu Kundensystemen verwendet wird. Wurde bisher ein Modem zum Aufbau einer SIRA-Verbindung verwendet, so wird nun ein OpenVPN-Tunnel, der vom Techniker auf Basis des SIRA-Profils konfiguriert werden kann, verwendet. Die einzige Anforderung ist eine Internetverbindung.

INFO: Ursprünglich war SIRA für die Verwendung von IP-Adressen der Klasse 10.0.0.0/8 konzipiert. Dieser Bereich kann oft mit dem LAN-Subnetz des Kunden kollidieren, was zu Routing-Problemen führen kann. Für das neue RSP-Merkmal wird nun der Bereich 100.64.0.0/10 verwendet. Dieser Bereich ist global für Tunneling und ISP-Adressbereiche reserviert und sollte daher nicht mit den LAN-Subnetzen des Kunden kollidieren. Diese IP-Adressen sind außerhalb unseres RSP-Dienstes nicht sichtbar.

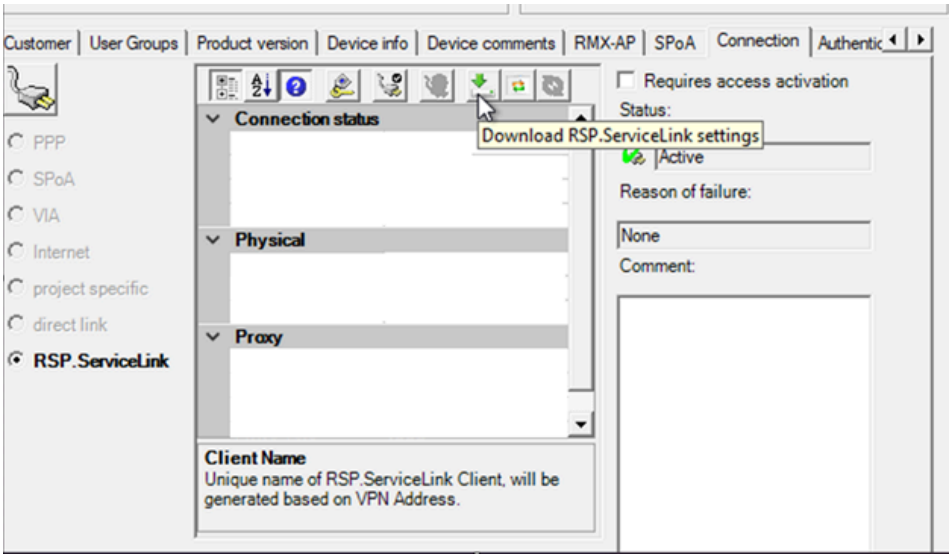
9.2 Konfiguration auf SIRA

Um die RSP-Option zu konfigurieren, muss auf SIRA mit V11 ein neues Profil definiert und für den Verbindungstyp RSP.ServiceLink ausgewählt werden.



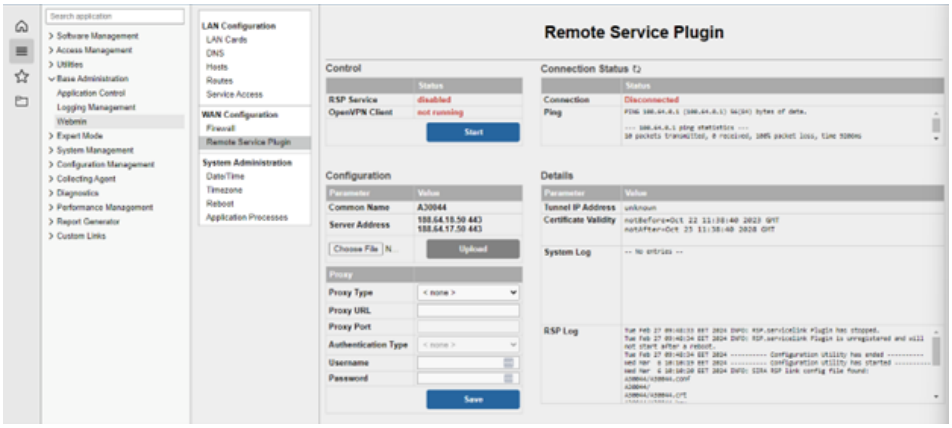
Am Ende des Konfigurationsassistenten muss die tar-Konfigurationsdatei gespeichert werden. Dies wird auf der Systemseite verwendet, um die Konfiguration für diesen Dienst abzuschließen.

Falls die tar-Konfigurationsdatei nicht gespeichert wurde, kann sie über den Eintrag Systemkonfiguration auf der Registerkarte **Verbindung** durch Auswahl der Schaltfläche **Herunterladen** heruntergeladen werden.

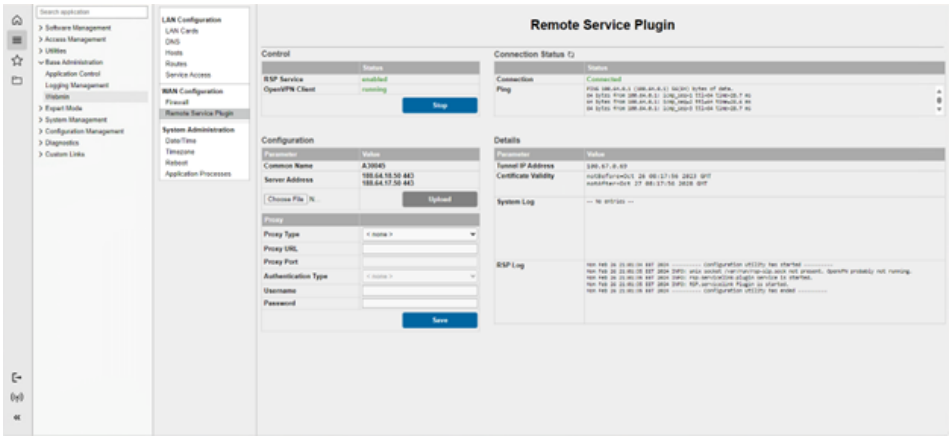


9.3 Konfiguration auf OpenScape 4000

Für diesen Dienst wurde auf der Webmin-Seite ein neuer Eintrag namens Remote Service Plugin hinzugefügt. Und um den Dienst zu konfigurieren, muss die von SIRA bereitgestellte tar-Datei über das Konfiguration-Kontextmenü hochgeladen werden. Sobald die tar-Konfigurationsdatei hochgeladen ist, kann der Dienst gestartet werden. Falls für die Internetverbindung ein Proxy erforderlich ist, müssen auch die entsprechenden Details bereitgestellt werden.



Sobald der Dienst gestartet und die Verbindung hergestellt ist, wird dies auf der Seite durch den entsprechenden Status und die Farbe angezeigt.



9.4 Die Konfigurationsdatei

Die Konfigurationsdatei enthält alle erforderlichen Zertifikate und Schlüssel für die OpenVPN-Verbindung, um den Tunnel zwischen Client und Server zu sichern. Daher müssen die Zertifikate auf beiden Seiten angebracht werden.

Auf der Client-Seite gespeicherte Zertifikate:

- client public crt
- client private key
- corporate CA chain

Auf der Serverseite gespeicherte Zertifikate (SIRA):

- server public crt
- server private key
- RSP-Client CA-Kette
- RSP certificate revocation list (CRL)

Wenn der OpenVPN-Client eine Verbindung zum RSP-Server herstellt, wird der Schlüsselaustausch durchgeführt. Beide Seiten prüfen die empfangenen Zertifikate gegen ihre lokal gespeicherte CA-Zertifikatskette. Wenn sie passen, bauen sie den Tunnel auf. Client-Zertifikate werden von der RSP-Client-Zertifizierungsstelle ausgestellt und signiert, während die Zertifikate des RSP-Servers von der Unternehmenszertifizierungsstelle (Unify) signiert werden. Jeder Client hat also eine Kopie der Unternehmenszertifikatskette, und jeder Server hat Zugriff auf die RSP-CA-Kette, gegen die das Client-Zertifikat geprüft werden soll.

Unify Server 2015 CA

Unify Server 2015 CA ist die derzeit verwendete Zwischen-CA für RSP-Client-Verbindungen, damit die Clients prüfen können, ob sie sich mit einem von Unify signierten OpenVPN-Server verbinden.

Die Zertifikate müssen alle 3 Jahre erneuert werden. Auf jedem Client sind CA-Zertifikatsketten, gegen die sie das Server-Zertifikat prüfen können, gespeichert.

RSP-Client CA

RSP-Client CA ist eine interne CA für die automatische Verwaltung von Client-Zertifikaten für RSP-Verbindungen. Zertifikate werden synchron mit dem Erstellen und Löschen von RSP-Geräteverbindungen signiert und

widerrufen. Bei jeder gelöschten Verbindung wird das Zertifikat an die RSP-Zertifizierungswiderrufsliste gesendet, um weitere Verbindungen zum RSP abzulehnen.

Registrar CA

Wird für den automatischen Registrar verwendet. Die automatische Selbstregistrierung ermöglicht die freie Konfiguration des Assistenten des Plugins nur mit SIRA-Tools.

NOTICE: Dieses Teilmerkmal wird später geliefert.

10 Datum/Zeit

Dieser Abschnitt beschreibt die Konfigurierung von Datum, Zeit, Taktquelle und Synchronisierungsintervall.

Das Vorgenhen bei der Konfigurierung von Datum und Zeit für den Manager bzw. für den Assistant unterscheidet sich:

- Datum/Zeit für den Manager
- Datum/Zeit für den Assistant

10.1 Datum/Zeit für den Manager

Dieser Abschnitt beschreibt die Konfigurierung von Datum, Zeit, Zeitquelle und Synchronisierungsintervall für den OpenScape 4000 Manager.

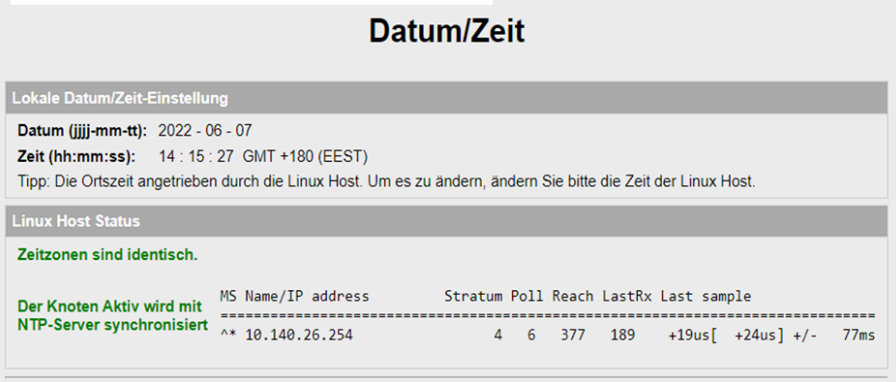
Allgemeine Informationen über Clock Source and Synchronization Status

- **Externer Zeit-Server - Periodische Synchronisierungen**

  Wenn die Uhrzeit im **EPS**-Modus (Externer Zeit-Server - Periodische Synchronisierungen) synchonisiert wird und ein Zeit-Server eingestellt ist, zeigt

  die Tabelle **Konfigurierter Zeit-Server** Einzelheiten über den letzten Versuch des Managers,

  die Zeit mit der externen Quelle zu synchronisieren.



  Die Tabelle zeigt, wann der der letzte Synchronisierungsversuch gemacht wurde, über welchen von mehreren NTP-Zeitservern die Synchronisierung erfolgte und welche Aktion ausgeführt wurde. Außerdem wird eine Übersicht über den Gesamtstatus ausgegeben.

- **Externer Zeit-Server - NTP Server für andere Systeme**

  Im ENTP-Modus (Externer Zeit-Server - NTP Server für andere Systeme) zeigt die Tabelle, welche Server als Takt-Quellen eingestellt sind und welche Rolle sie im NTP-Synchronisierungsprozess sie einnehmen. Der

Manager wird nach dem Server synchronisiert, der unter Synchronisiert mit hervorgehoben ist.

Die folgenden Serverstatus sind möglich:

– Erreichbar

  Der Server ist erreichbar, aber es erfolgte noch keine Synchronisation, oder er ist kein "Kandidat" für die Synchronisation.
– Synchronisiert mit

  Das System wurde mit diesem Server synchronisiert.
– Unerreichbar

  Der Server ist kein NTP-Server oder kann nicht erreicht werden.
– Kandidat

  Mit diesem Server wird der der nächste Synchronisierungsversuch unternommen, wenn der Versuch mit dem ersten fehlschlägt.

Verwandete Themen

- Parameter
- Funktionen

Um die Zeitzone des Systems einzustellen, informieren Sie sich bitte im Abschnitt Zeitzone.

10.1.1 Parameter

- **Konfigurierte Taktquelle**

  Es gibt folgende Auswahlmöglichkeiten:

  – **HW Taktgenerator - Standalone** Wird diese Option gewählt:
    – kann der Benutzer die Zeit für dieses System einstellen.
    – kann kein anderes System dieses System als Zeit-Server verwenden.
    – versucht dieses System nicht, die Zeit mit einem anderen zu synchronisieren.
  – **HW Taktgenerator - NTP Server für andere Systeme** Wird diese Option gewählt:
    – kann der Benutzer die Zeit für dieses System einstellen.
    – können andere Systeme dieses System als Zeit-Server verwenden.
    – versucht dieses System nicht, die Zeit mit einem anderen zu synchronisieren.
  – **Externer Zeit-Server - Periodische Synchronisierungen** Wird diese Option gewählt:
    – kann der Benutzer die Zeit für dieses System nicht einstellen.
    – kann kein anderes System dieses System als Zeit-Server verwenden.
    – versucht dieses System, die Zeit mit einem konfigurierten Einzel-Zeit-Server-System zu synchronisieren. Der Versuch beginnt um Mitternacht und wird anschliessend gemäss dem

konfigurierten **Synchronisierungsintervall** fortgesetzt. Ein Synchronisierungsintervall von zwei Stunden sollte angemessen sein.

  - **Externer Zeit-Server - NTP Server für andere Systeme** Wird diese Option gewählt:
    - kann der Benutzer die Zeit für dieses System nicht einstellen.
    - können andere Systeme dieses System als Zeit-Server verwenden.
    - Versucht dieses System, die Zeit mit anderen konfigurierten Zeit-Servern über NTP (Network Time Protocol) zu synchronisieren.
- **Synchronisierungsintervall**

  Synchronisierungsintervall ist nur von Bedeutung, wenn die Taktquelle **Externer Zeit-Server - Periodische Synchronisierung** ist.
- **Datum (jjjj-mm-tt)**

  Das Datum wird im Format jjjj-mm-tt angegeben. Beispiel: 2010-01-22.
- **Zeit (hh:mm:ss)**

  Die Zeit wird im 24-Stunden-Format angegeben. Beispiel: 14:23:05.
- **Name oder Adresse des Zeit-Servers**

  Bitte geben Sie den Namen oder die IP-Adresse des externen Zeit-Server-Systems an.

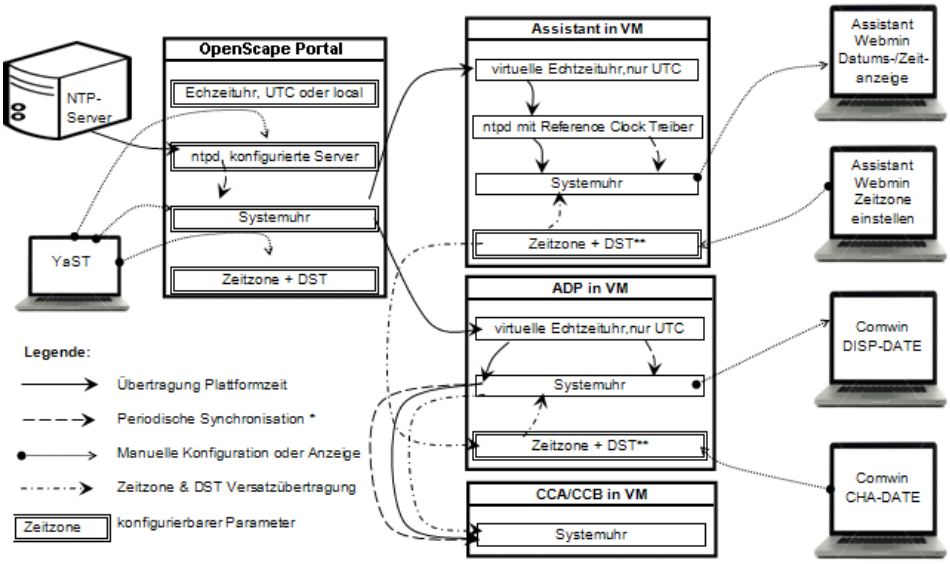
10.1.2 Funktionen

Für den Manager können folgende Funktionen zur Datums- und Zeiteinstellung vorgenommen werden:

- Datum/Zeit für den Assistant
- Datum/Zeit für den Assistant
- Synchronisierungsintervall ändern
- Neuen Zeit-Server hinzufügen
- Name oder IP-Adresse des Zeit-Servers ändern
- Zeit-Server löschen

10.2 Datum/Zeit für den Assistant

OpenScape 4000 Datum-/Zeitkonzept



* Das Synchronisierungsintervall für ADP und CCs beträgt 2 Minuten. Für den Assistant nimmt ntpd ständig fein abgestimmte Sychronisierungsintervalle vor. Wird am OpenSape 4000-Portal die Zeit vorgestellt, so erfolgt darauf die Synchronisierung am Assistant innerhalb von 3 Minuten.

** Wert für die Sommerzeitumstellung

Um am Assistant Datum und Zeit einzustellen sind folgende Schritte notwendig:

- Bevor der Assistant gestartet wird, muss die aktuelle Zeit und das aktuelle Datum mit dem 'YaST'-Datums-/Zeitmodul azf den OpenScape 4000-Portal eingestellt werden.

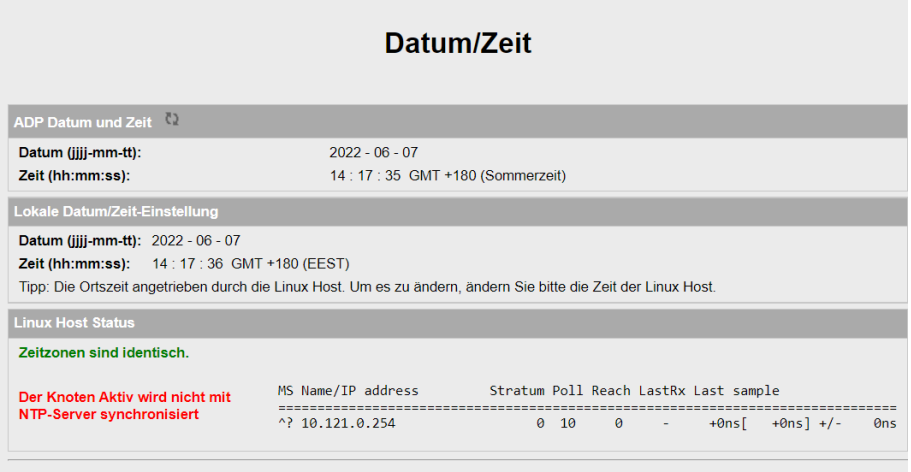
  Oder Sie stellen den Rechner so ein, dass er den NTP server als Zeitserver verwendet. In diesem Fall synchronisieren Sie das System mit dem `ntpdate`-Kommando - oder warten Sie, bis der NTP-Server das System synchronisiert.

  Hinweis: Wenn die Zeit auf dem Portal manuell *vorgestellt* wird, wird der Assistant in 3 Minuten synchronisiert. Bevor Sie die Zeit manuell *zurückstellen*, müssen Sie sicherstellen, dass die virtuellen Maschinen heruntergefahren wurden, da sonst die virtuelle Echtzeit-Uhr des Assistant hängt und das Ergebnis unvorhersehbar ist.

  Die Einstellung einer Zeitzone ist optional, sie hat keinen Einfluss auf die Zeitzone des Assistant.
- Starten Sie nun den Assistant.

  Die Anfangswerte für Zeit und Datum werden vom Portal geholt.

- Klicken Sie im Assistant auf den Link **Datum/Zeit** in der Navigationsleiste. Die aktuelle Einstellung für die Uhrzeit und das Datum werden im rechten Fensterausschnitt im 'read-only'-Modus angezeigt.



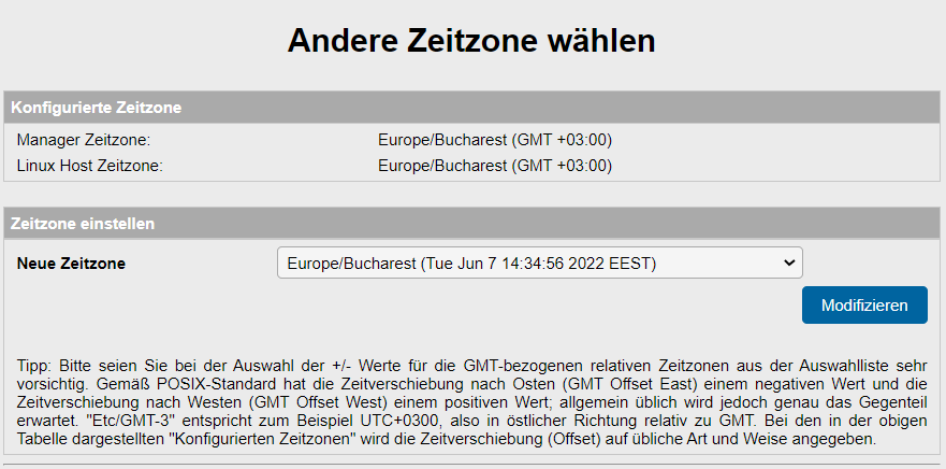
Während des Laufzeit des Assistant synchronisiert der ntp-Systemprozess mittels eines eigenen Referenzuhr-Treibers die Zeit jeweils nach einigen Minuten am Portal. Eine Konfigurierung ist nicht notwendig.

11 Zeitzone

In diesem Abschnitt wird die Konfiguration der Zeitzone beschrieben. Die Konfiguration der Zeitzone wird für den Manager und den Assistant unterschiedlich gehandhabt:

- Zeitzonenkonfiguration für den Manager
- Zeitzonenkonfiguration für den Assistant

11.1 Zeitzonenkonfiguration für den Manager



In diesem Abschnitt wird die Konfiguration der Zeitzone für den OpenScape 4000 Manager beschrieben.

- Sie können die Zeitzone **ändern**, indem Sie die gewünschte Zeitzone aus der Liste **Neue Zeitzone** wählen und anschließend auf die Schaltfläche **Ändern** klicken.

  Die Änderung der Zeitzone wird sofort wirksam.

  Anmerkung: Russland hat beschlossen, ab dem 26. Oktober 2014 auf permanente Standardzeit umzustellen. Daher werden zwei neue Zeitzonen erstellt. Weitere Einzelheiten finden Sie unter http://www.timeanddate.com/news/time/russia-abandons-permanent-summer-time.html.

  Damit der Manager mit diesen Änderungen konform bleibt, muss das neueste Zeitzonenpaket (Mindestversion timezone-2014g-0.5.1) mit entfernter Sommerzeit aus dem SuSE-Repository installiert werden. Die Zeitzone muss daher in Webmin Base Administration neu konfiguriert werden. Beachten Sie beim Ändern der Zeitzone bitte, dass die Zeitzone gemäß dem POSIX-Standard mit einem negativen Wert gekennzeichnet ist. Beispielsweise entspricht "Etc/GMT-3" UTC + 0300.

Verwandte Themen

Zeitzonenkonfiguration für den Assistant

11.2 Zeitzonenkonfiguration für den Assistant

In diesem Abschnitt wird die Konfiguration der Zeitzone für den OpenScape 4000 Assistant beschrieben. Der Assistant ist die zentrale Station für das Zeitzonenmanagement des gesamten OpenScape 4000-Systems, einschließlich ADP, CSTA und der Hostplattform.

In allen diesen Subsystemen sollte dieselbe Zeitzone angezeigt werden. Abweichende Einstellungen der Zeitzone können hier berichtigt werden.

- Sie können die Zeitzone **ändern**, indem Sie die gewünschte Zeitzone aus der Liste **Neue Zeitzone** wählen und anschließend auf die Schaltfläche **Ändern** klicken.

Nach der Änderung der Zeitzone wird die Änderung automatisch zu Hostplattform, CSTA und ADP übertragen.

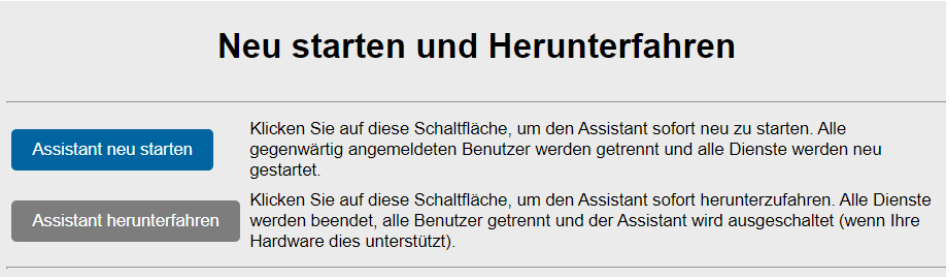
Für den ADP wird auch die Sommerzeitumstellung, die vom Assistant überwacht wird, automatisch übertragen. Der ADP überträgt jede Änderung der Zeitzone und der Sommerzeitumstellung sofort auf beide CCs.

Anmerkung: Die Zeitzone im ADP sollte nicht manuell über AMO CHA-DATE geändert werden!

Verwandte Themen

Zeitzonenkonfiguration für den Manager

12 Neu starten/Herunterfahren



Mit den folgenden Funktionen wird das System manuell neu gestartet oder der Manager heruntergefahren:

- Neu starten
- Herunterfahren (nur Manager)

12.1 Neu starten

Diese Funktion kann für eine Systemwiederherstellung genutzt werden, beispielsweise wenn sich das System in einem abnormalen Zustand befindet oder Konfigurationsänderungen wirksam gemacht werden sollen, z.B. beim Hinzufügen einer neuen Route.

- Sie können das System neu starten, indem Sie auf **System neu starten** klicken.

  Anschließend werden Sie zur Bestätigung des Neustarts aufgefordert.

  Das System wird dann heruntergefahren und neu gestartet

Bitte beachten Sie, dass während des Neustarts alle angemeldeten Benutzer getrennt und alle Dienste neu gestartet werden.

12.2 Herunterfahren (nur Manager)

- Sie können den Manager ganz herunterfahren, indem Sie auf **System herunterfahren** klicken.
- Bestätigen Sie nun auf der folgenden Seite, ob Sie das System wirklich herunterfahren wollen. Wenn Sie erneut auf **System herunterfahren** klicken, wird das System heruntergefahren und ausgeschaltet (falls die Hardware dies unterstützt).

Das System kann nur manuell wieder eingeschaltet werden. Bitte geben Sie acht, wenn Sie über einen **Fernanschluss** (remote) angemeldet sind. Nach dem Herunterfahren können Sie sich nicht mehr anmelden. Bitte beachten Sie, dass beim Herunterfahren alle angemeldeten Benutzer getrennt werden.

13 Anwendungsprozesse

Anwendungsprozesse

Name	Status	Zeit	Pid	Ext	Starten
Batch					
FM_FTserv	Active	Jun 4 16:33:47	44099		
FM_FTsucc	Active	Jun 4 16:33:47	44100		
COL					
col_cycliccheck	Active	Jun 4 16:33:51	44643		
col_dbproxy	Active	Jun 4 16:33:51	44649		
col_line	Active	Jun 4 16:33:49	44146		
col_receive	Active	Jun 4 16:33:53	44825		
col_schedule	Active	Jun 4 16:34:16	45774		
col_transform	Active	Jun 4 16:33:49	44147		
CORBA					
Naming_Service	Active	May 29 19:48:59	2973		
FM_AER					
FM_AER_Daemon	Active	Jun 4 16:33:47	44095		
FM_SNMP					
FM_DB_Server	Active	Jun 4 16:33:47	44092		
HG3550M					
Hg3550mAPIServer	Active	May 29 19:49:11	4575		
lwdaemon	Active	May 29 19:49:00	3100		
mekAdm	Active	May 29 19:48:59	3094		
IDS					
IDS_oninit	Active	May 29 19:49:02	1570	X	
Iptrace					
iptrace	Active	Jun 4 16:33:56	44919		
LMT					
LMT_Daemon	Active	Jun 4 16:33:53	44924		

Die Anwendungsprozesse, die im Hintergrund laufen, stellen verschiedene OpenScape 4000 Manager/Assistant Funktionen bereit. In der Tabelle können Sie sehen, welche Prozesse laufen (oder nicht) und welche Funktion daher verfügbar ist oder nicht verfügbar.

Die Prozesstabelle zeigt Grundinformationen über alle eingetragenen Prozesse an. Die Prozesse sind in verschiedene Gruppen aufgeteilt.

Folgende Spalten werden angezeigt:

- **Name**

  Der Name des Prozesses.
- **Zustand**

  Folgende Zustände sind möglich:

  – **Aktiv**

    Der Prozess wurde gestartet und läuft immer noch.

  – **Eingetragen**

    Der Prozess ist eingetragen, aber läuft nicht. Er wurde nie gestartet oder wurde nach der Anwendungsanforderung beendet. Sie können diesen

Prozess starten, in dem Sie diesen in der letzten Spalte markieren und auf die Schaltfläche **Ausgewählter Prozess starten** klicken.

– **Inaktiv**

Der Prozess läuft nicht. Dieser Prozess wurde zu oft neu gestartet (d.h. der maximale Neustart-Schwellwert wurde erreicht) und wurde durch die Prozessverwaltung nicht mehr neu gestartet.

– **Anlauf verschoben**

Der Prozessanlauf wird verschoben, wenn der Prozess von einem anderen Prozess, der noch nicht läuft, abhängig ist.

– **Anlauf zeitüberschritten**

Die Prozessanlaufzeit wurde überschritten.

- **Seit**

  Erstellungsdatum des Prozesses.
- **Pid**

  Prozess-Id (nur für aktive Prozesse).
- **Ext**

  Prozess ist extern. Er wird ausserhalb der Prozessverwaltung gestartet. Externe Prozesse können durch die Prozessverwatung nicht gestartet werden.
- **Start**

  Sie können den nicht laufenden Prozess starten, indem Sie diesen wählen und auf **die Schaltfläche** Ausgewählter Prozess starten klicken.

Index