Unify OpenScape 4000 Manager V10

Smart Switch-Over

Smart Switch-Over

Administrator Documentation
05/2020

A31003-H34A0-M135-01-76A9

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.

Contents

1 Smart SwitchOver - Overview

The OpenScape 4000 Manager product range now includes Smart SwitchOver, a new High Availability Solution providing high data availability based on data synchronization between two servers.

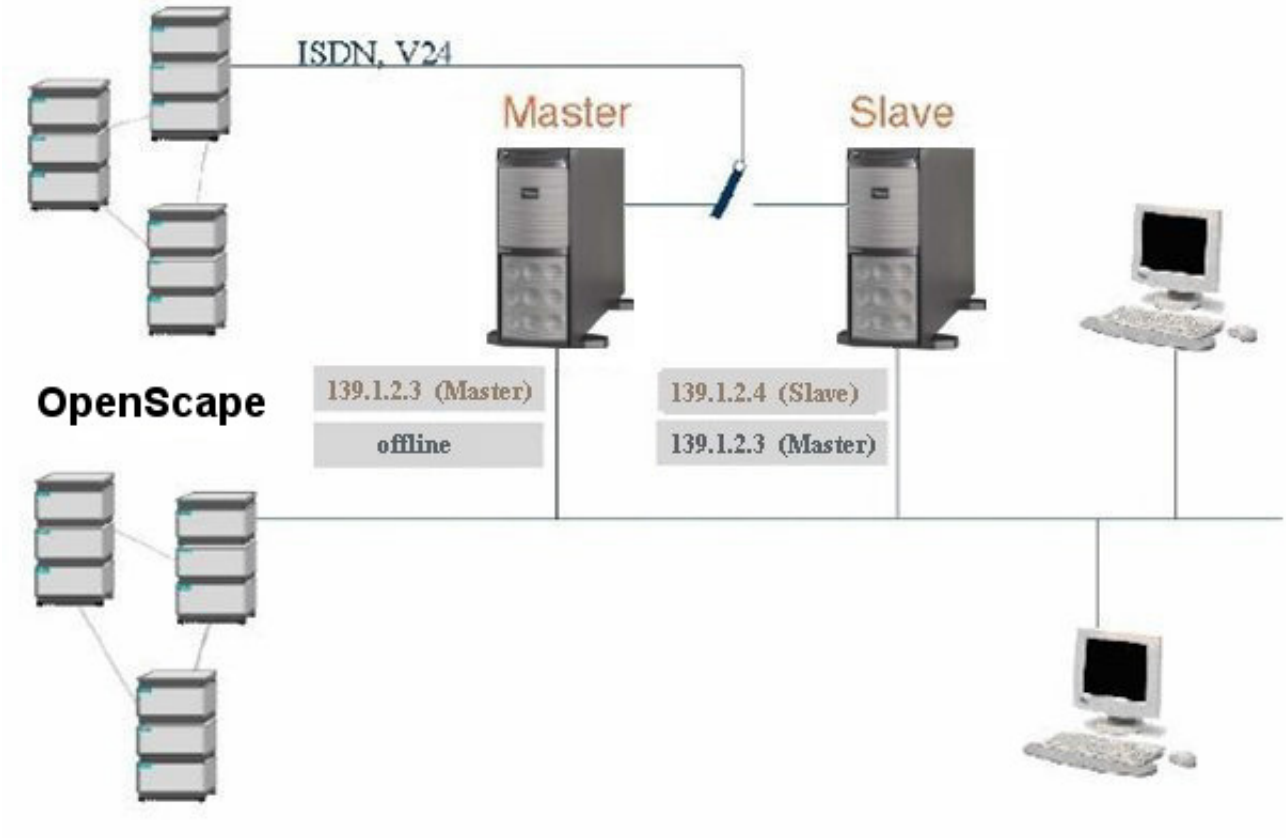
Smart SwitchOver requires two high-end OpenScape 4000 Manager servers arranged near one another in the same LAN segment of a network. The servers operate in a Master/Slave relationship, where only the Master server (i.e. Active node) is operating productively, while the Slave server (i.e. Standby node) is passive.

Data synchronization between the Master and Slave servers is implemented by replicating the data directly from the Master to the Slave, thereby eliminating the need for an FTP backup server. Data replication/synchronization is based on the Linux tools **LVM2** (Logical Volume Management) and **rsync** (file transfer program).

In order to implement the SSO solution, it is necessary to install the SuSe Linux Enterprise Server 11 (SLES 11) system with Logical Volume Manager (LVM) partitioning.

NOTE: For information regarding the installation of SLES11 with LVM partitioning, please refer to .Appendix A, “Appendix: Installation of SLES11 with LVM”.

Figure 1 Master/Slave Servers for “Smart Switchover”



NOTE: **Software Version Information**
Please also refer to the Release Notes, especially for SSO, for current information about the latest software version released.

1.1 Area of Application

1.1.1 New Solution: Smart SwitchOver on OpenScape 4000 Manager

In contrast to the older solution with Backup & Restore needing three servers (Master, Slave and FTP backup server), the SSO solution described here requires only two servers (a Master and a Slave server) by using the LVM technology and the rsync command to perform synchronization of the entire system.

SSO - Properties and Features Overview

- Data synchronization is performed using `rsync` command which is part of Linux system
- Minimum configuration effort required
- Usage of OpenScape 4000 Standard Tools
- Only one productive server (same as with previously used solutions)

1.1.1.1 Switching Over Between the Two Servers

In the event of a switchover between the two servers the following items need to be taken into account, and the following steps need to be performed:

- The connections to the clients are interrupted, and the clients need to log on again.
- A procedure must be invoked to "wake" the Slave (i.e., to configure it as Master and to start processes).

Related Topics

Switchover Process

1.1.2 Previously Used Solutions

Smart SwitchOver is used since HiPath 4000 Manager Version 2/OpenScape Manager Version 7.

1.2 Prerequisites and Restrictions

1.2.1 Prerequisites

The following prerequisites must be met in order for Smart Switchover to function properly:

- The Slave server requires its own license file (due to the MAC address). Master and Slave use different MAC addresses. Each has its own original MAC address. Upon switchover, only the IP address is exchanged between the Master and the Slave.
- 1Gb/s LAN segment is recommended in order to optimize data replication times.

NOTE: **Software Version Information**
Please also refer to the Release Notes, especially for SSO, for current information about the latest software version released.

1.2.2 Restrictions

The following restrictions apply to Smart SwitchOver (SSO):

a) The Master/Slave servers must be equipped with the same hardware.

   – Only Intel-based servers of the exact same type (e.g. Primergy TX300), certified and released for current version of OpenScape 4000 Manager, are to be used.

   – The expansion boards must also be identical, and it must be made certain that the PCI boards in both servers are connected to the same PCI bus and in the same PCI slot.

b) If case of upgrading OpenScape 4000 Manager V5 to a higher major version, replication must be disabled. See Section 2.7, “Upgrade Procedure for OpenScape 4000 Manager with SSO” for a detailed upgrade procedure.

c) Both OpenScape 4000 Manager servers must be located in the same LAN segment (i.e. the Slave must be reachable from Master via the LAN).

d) OpenScape Applications products in other LAN segments are not possible.

e) LVM must be used for partitioning.

f) During the OS installation in initial partitioning, **at least** half of the HDD's capacity must remain free. This applies regardless of the total amount of disk space on the HDD. If this precondition is not considered, SSO will not work properly.

g) It is mandatory to use the GRUB boot-loader. LILO is not supported.

h) The data replication from the master to the server comprises always the entire master data.

i) There is no GUI available for the SSO configuration. An ASCII menu is provided instead.

1.3 What SSO Does Not Support

The following tasks or conditions are not supported by Smart Switchover (SSO), so these must be handled using OpenScape Backup & Restore (HBR):

- SSO does not support Manager data migration.
- SSO does not support Manager logical backups for OpenScape 4000 Assistants and other OpenScape 4000 Managers.
- SSO does not check logical data consistency.
- SSO cannot replicate single applications or data sets.
- SSO does not run on Assistants.
- SSO does not support immediate (i.e. online) data replication. Data are replicated to the Slave at a specified point in time.

2 SSO - Installation and Configuration

2.1 Initial Startup

2.1.1 Installing and Activating the SSO Hardware

The basic procedure for installing the Smart Switchover hardware is as follows:

1. Install the two machines that will be the Master/Slave servers in the usual manner (refer to the corresponding sections earlier in this chapter). Pay special attention to the following:
   - Observe the prerequisites and restrictions in Section 1.2.1, “Prerequisites” and Section 1.2.2, “Restrictions”.
   - If an IP address is assigned during installation, it should be the address that will ultimately serve as the Master/Slave address (this prevents a situation where both servers have identical IP addresses following installation). Refer to Figure 1.
   - The Master and Slave servers must each have their own license.
2. Activate the Master server as follows:
   a) Log in using the `sso` account.
   b) Complete the SSO configuration file (Section 2.3.2, “Edit configuration file”).
   c) Configure the system as Master (Section 2.3.2, “Configure system as Master (Active Server)”).
3. Activate the Slave server as follows:
   a) Log in using the `sso` account.
   b) Complete the SSO configuration file (Section 2.3.2, “Edit configuration file”).
   c) Configure the system as Slave (Section 2.3.2, “Configure system as Slave (Standby Server)”).

2.2 Switchover Components

The basic components of involved in switchovers are **communication**, **data replication** using the Linux tools *LVM* (Logical Volume Manager) and *rsync*, and the **productive processes of OpenScape Management** (Configuration Management, Fault Management, and Data Collecting).

This section provides an overview of the role each component plays in a Smart Switchover configuration.

2.2.1 Data Replication

In a normal (non-SSO) OpenScape 4000 Manager setup, backup files can be saved on the same server or on a different server, as configured using the Backup function of OpenScape Backup & Restore.

NOTE: Please refer to the **OpenScape 4000 Manager Installation and Service Manual**, Section 5.6, “Backing Up/Restoring Data with OpenScape 4000 Manager” for more information.

The SSO solution, however, provides for a complete system replication on the Slave server. Under Linux, the **Logical Volume Manager (LVM)** makes it possible to take “snapshots” of disk partitions, which requires a minimal amount of system downtime (approx. 5 minutes). When the OpenScape 4000 Manager and Informix database are restarted, the data are replicated “online” to the Slave server by means of the file transfer program **rsync**. This tool ensures fast and secure data replication, while minimizing network traffic.

NOTE: After replication to the Slave server, it is possible to perform regular HBR logical backups on the Slave server.

2.2.2 Productive Processes of OpenScape Management

The relevant processes are the OpenScape 4000 Manager application processes (Configuration Management, Fault Management, Data Collecting). These must be deactivated on the Slave, so as not to initiate any activity on the network. These processes are automatically deactivated during the configuration as Slave (refer to Section 2.3.2, “Configure system as Slave (Standby Server)”), and activated during the switchover to Master (refer to Section 2.3.2, “Configure system as Master (Active Server)”).

2.2.3 Communication

LAN Configuration

The OpenScape 4000 Manager should be accessible via a single IP address - even after a switchover. Consequently, neither HICOMs nor Clients need to be changed over; rather, only the connection to the Manager is lost at the time of the failure. To switch over the IP address from the Master to the Slave, the following solutions are available:

- Two LAN Cards

  Each system is equipped with two LAN cards, and there are three real IP addresses available for these two systems. The Master and the Slave system each have their own IP address, while the third IP address is configured on the second LAN card of each system, acting as communication interface to the OpenScape partners. On the Slave, however, this second interface to the OpenScape IP address is deactivated.

  Switchover:
  A script is used to activate or deactivate this second interface, respectively.

- Two LAN Cards (Bonding interface)

  SSO with bonding enables the use of more than one network card on the specified machines; i.e. if one of the network lines fails, the manager can continue with the other network card installed on the systems. SSO automatically detects the network cards available on the system and allows the manager to select which network cards shall be used for LAN communication. The selected LAN card is automatically updated in the SSO configuration file.

  The user guide for configuring the bonding interface on SLES11 can be found under the following link:

  http://www.novell.com/communities/node/6626/bonding-multiple-network-interfaces-sles-10

- Script and Restart: Change the IP address and then restart the server (preferred solution).

  Only one LAN interface per server.

  In the event of a switchover, the operator reconfigures the IP address using a script, and restarts the server.

NOTE: Advanced Options of the network card driver (speed and duplex settings) are not handled by SSO. These settings are neither backed up nor restored. If connectivity problems occur after SSO restore, service technician may have to set the network driver options using the 'ifcfg' or 'YaST2' tool. Make also sure that the network switch is properly configured.

Manager servers at different locations can have different routing entries. The routing entries are not changed when data are replicated from the Master to the Slave. Therefore, the Master server can have a different default GW and different static routing entries than the ones used by the Slave.

The switchover configures the Master IP, Master default GW and Master static routes to the Slave when it is being configured as Master node. The static routes which had been configured on Slave node are dropped during the switchover procedure. For the node change from the Master to the Slave, only the Slave IP is configured, the default GW and static routes remain unchanged (i.e. they remain as configured when the node acted as the Master).

There is no explicit limit imposed by the OpenScape 4000 Manager on the RTT, so the maximum is defined by the TCP timeout.

Direct connections: Manual rerouting

This connection is not shown in the overview illustration (see Figure 1), nor is it a widely used connection type. Since this type of connection cannot be redirected via call forwarding, the only solution is to manually reroute the cable.

VPN configurations

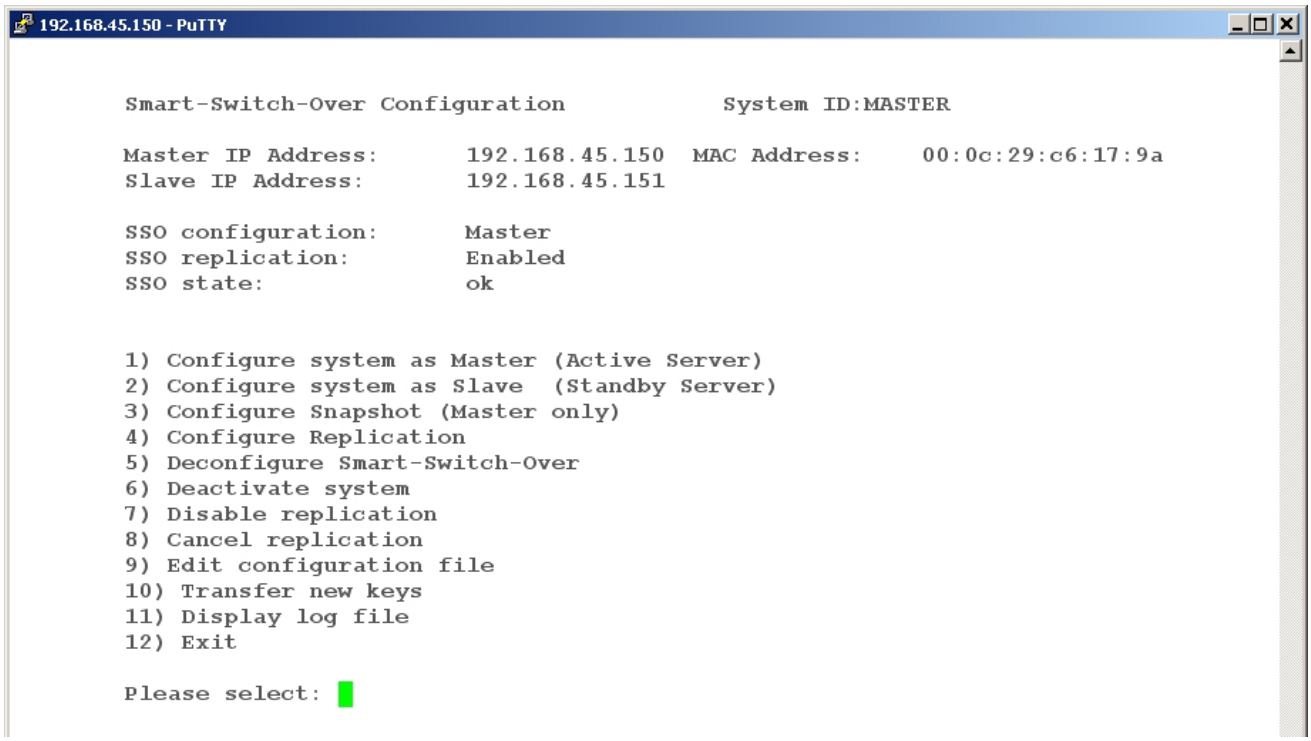
Due to the fact that VPN (virtual private network) connections evaluate the IP address and/or telephone number at the time of connection setup, communication via VPN continues to be possible following call forwarding and IP address change on the server.

2.3 Configuration

All SSO functionality is controlled via the user ID **sso**. There is no graphical user interface (GUI) for login. SSO-related data are configured in a manually edited ASCII file that is created for each server (Master/Slave). This file is accessed by selecting menu item **8) Edit configuration file** (see Figure 2). The file contains all SSO-relevant data, such as IP address, data for call forwarding, and so on. To see an example of a SSO configuration file, refer to Section 2.6, “Example of an SSO Configuration File”.

NOTE: Immediately following first installation, the password for the **sso** account is the same as for the **engr** account.

Figure 2 Smart Switchover Configuration Menu



2.3.1 The Smart Switchover Configuration Screen

The Smart Switchover Configuration screen (refer to Figure 2) displays the following information:

- Master IP Address:
- MAC Address:
- **Slave IP Address:**
- **SSO configuration:** indicates whether SSO is configured as Master or Slave (if SSO is not active, " - " is displayed)
- **SSO state:** indicates the status of SSO. The following values are possible:
  - **`Configuration running`**
    Configuration as Master/Slave is currently in progress.
  - **`Deconfiguration running`**
    Deconfiguration is currently in progress.
  - **`Replication running`**
    Data replication operation is currently in progress.
  - **`Configuration failed`**
    An error occurred during configuration. System may be inconsistent.
  - **`Deconfiguration failed`**
    An error occurred during deconfiguration. System may be inconsistent.
  - **`Replication failed`**
    An error occurred during data synchronization. System may be inconsistent. Next data replication will take place as scheduled.
  - **`OK`**
    Everything is in order. The OK message is displayed following successful configuration as Master/Slave, and following a successful data backup/ restore operation, for example.

2.3.2 Function of Individual Menu Items

The following contains a brief description of each of the menu items on the Smart Switchover Configuration screen (see Figure 2).

The actions described are performed automatically when the corresponding menu item is selected.

1. Configure system as Master (Active Server)

   This menu item is used to configure the server as Master. During the configuration of the system as Master, the root password will be required for connecting to the Slave machine.

   The following actions take place:

   - A check is performed to determine whether all required parameters were specified. If a value is missing, a corresponding error message is displayed, and the error can be corrected using menu item `Edit configuration file`.
   - Connect to the Slave server and transfer the rsa_key for communication during the replication process.
   - LAN configuration
   - Server reboot

   After the reboot, the following actions take place automatically:

   - Activation of the specified applications via **`procm`**
   - Call forwarding is enabled or disabled (generation of the necessary AMO batch, execution is handled via batch processing)

2. Configure system as Slave (Standby Server)

   This menu item is used to configure the server as Slave. The following actions take place:

   - A check is performed to determine whether all required parameters were specified. If a value is missing, a corresponding error message is displayed, and the error can be corrected using menu item `Edit configuration file`.
   - Creation of temporary Logical Volumes to ensure a successful replication process.
   - LAN configuration
   - Deactivation of the specified applications via **`procm`**
   - Creation of a RAM disk for the first replication on the server. During the restart, SSO replicates the original system to the temporary Logical Volumes.

- Server reboot

3. Configure Snapshot (Master only)

   This menu item is used to configure the snapshots which are used for the replication process. The maximum size for snapshots is the size of the corresponding partition. The minimum required size is 20% of the logical volume. The recommended size of the DBS snapshot is the size of the /DBS partition. The recommended size of the ASBackup snapshot is the size of the /.AS/BACKUP partition.

   Recommended Hard Disk Partitioning

NOTE: Please refer to the **OpenScape 4000 Manager Installation and Service Manual**.

   You can select which logical volumes will be backed up. Implicitly, all logical volumes are selected.

   It is necessary to allocate enough space for successful creation of snapshots. Snapshots will have the prefix “Snap”.

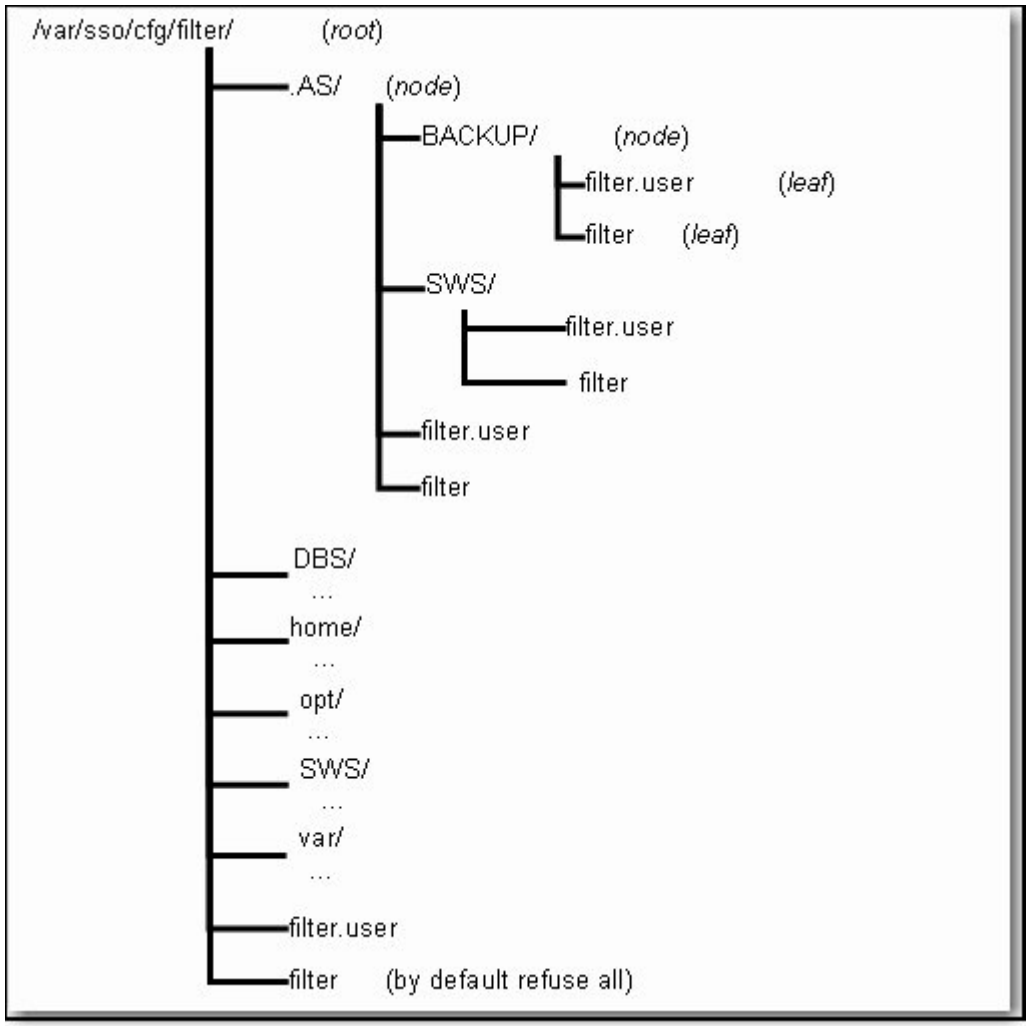
   The user can customize the snapshot sizes in the SSO menu.

4. Configure Replication

   This menu item is used to select which files and directories are to be replicated and which are not. Replication is configured using a special directory structure called the **configuration directory tree** (see Figure 3), which resides in the directory **/var/sso/cfg/filter**.

   The selection of files and directories that are to be synchronized (that is, transferred from Master to Slave) is based on filter rules contained in the files **filter.user** and **filter**, which are present in each directory of the configuration directory tree.

Figure 3 Configuration Directory Tree (for Replication)



The file **filter.user** contains filter rules for *rsync* set by user. This file is processed first.

The file **filter** contains default filter rules for *rsync*. This file is processed after the file **filter.user**.

The filter rules allow for flexible selection of which files to transfer (include) and which files to skip (exclude). In SSO the rules directly specify **include/ exclude patterns**.

Filter rules have the following syntax:

RULE [**PATTERN**_OR_**FILENAME**]

where **RULE** is either "**-**" (minus) for specifying an exclude pattern or "**+**" (plus) for specifying an include pattern.

The **PATTERN** or **FILENAME** that follows (when present) must come after either a single space or an underscore (_).

When rules are being read from a file, empty lines are ignored, as are comment lines that start with a "#".

The include/exclude rules each specify a pattern that is matched against the names of the files that are going to be transferred. These patterns can take several forms:

- If the pattern starts with a / then it is anchored to a particular spot in the hierarchy of files, otherwise it is matched against the end of the pathname. This is similar to a leading ^ in regular expressions. Thus "/foo" would match a file called "foo" at the "root of the transfer". An unqualified "foo" would match any file or directory named "foo" anywhere in the tree because the algorithm is applied recursively from the top down; it behaves as if each path component gets a turn at being the end of the file name. Even the unanchored "sub/foo" would match at any point in the hierarchy where a "foo" was found within a directory named "sub".
- If the pattern ends with a / then it will only match a directory, not a file, link, or device.
- If the pattern contains a wildcard character from the set *?[then expression matching is applied using the shell filename matching rules. Otherwise a simple string match is used.
- The double asterisk pattern "**" will match slashes while a single asterisk pattern "*" will stop at slashes.
- If the pattern contains a / (not counting a trailing /) or a "**" then it is matched against the full pathname, including any leading directories. If the pattern doesn't contain a / or a "**", then it is matched only against the final component of the filename. (Remember that the algorithm is applied recursively so "full filename" can actually be any portion of a path from the starting directory on down.)

NOTE: For a detailed description of the syntax and processing of filter rules used by **rsync**, see the manual pages for rsync, which can be found at **http://www.linuxcommand.org/man_pages/rsync1.html,** for example.

Examples of filter rules:

+ /home/	The user specifies that he wants to replicate the directory **`/home`**.
+ /home/engr/ + engr/*	The user specifies that the whole **`engr`** directory will be replicated
+ /home/other_user/ + other_user/file_trans	In directory **`other_user`** only the file **`file_trans`** will be copied.

```
- /home/engr/.ssh/known_hosts          This file is not to be replicated.
- /home/engr/.ssh/authorized_keys      This file is not to be replicated.
+ *                                    Alll other files will be copied.
```

5. Deconfigure Smart-Switch-Over

   This menu item is used to deactivate the SSO functionality. The following actions take place:

   - A check is performed to determine whether all required parameters were specified. If a value is missing, a corresponding error message is displayed, and the error can be corrected using menu item `Edit configuration file`.
   - Deconfiguration of Backup/Restore functionality in HBR.
   - Server reboot

NOTE: The current configurations of the LAN card and of call forwarding are not changed.

---

6. Deactivate System

   This menu item is used to deactivate the complete server.

   The following actions are performed on the server during this operation:

   - The server is shut down completely using the `init 0` command.
   - The system is configured so that does not start up automatically any more.

   You can use this menu item, for instance, to deactivate a defective Master server via remote access. At the same time, this configuration ensures that the server does not start up automatically any more, thus avoiding a situation with two active servers (Master and Slave) using the same IP address (at the same time).

   It is, however, possible to manually start up a deactivated system.

7. Disable Replication

   This menu item is used on the Master side to turn replication on/off. The configuration file need not be changed.

8. Cancel Replication

   This menu item will cancel a running replication at the nearest consistent point which might take several minutes.

9. Edit configuration file

This menu item is used to edit the SSO configuration file. When this item is selected, the "vim" text editor opens and displays the current contents of the configuration file. Upon exiting the vim editor, any changes made in the configuration file undergo a simple check for completeness (i.e., the minimum parameters required for a Master/Slave configuration must be present).

NOTE: See Section 2.6 on page 2-29 for an example of a configuration file.

NOTE: **Important**:
If changes are made in the configuration file, these are not automatically reflected in the system configuration. For these changes to become effective, another Master or Slave configuration must be carried out.

---

10. Transfer new keys

    In case that the communication between the Master and the Slave failed because of public keys, select this menu item to generate new keys used for the communication between the Master and the Slave.

11. Display log file

    With this menu item, the SSO log file can be viewed using "pg". This log file contains a record of all SSO actions.

12. Exit

    This menu item is used to exit the sso menu.

2.3.3 Required Configuration Parameters

The first time a system is configured as Master or Slave, all required parameters must be entered using the menu item **Edit configuration file** (refer to Figure 2).

If the server is to act as MASTER, the following parameters must be specified:

- IP address / Netmask / Broadcast for Master
- PCI bus/slot of LAN card, if the server has more than one LAN card
- If the LAN card is a TokenRing card, the speed must be specified
- Schedule/frequency of backups
- Specify whether replication is enabled or disabled.
- Change count of retries replication if fails and time between replications
- Indication whether call forwarding is necessary if the system is configured as Master

The following additional parameters are optional:

- Specification of applications to be started via **`procm`**

If the server is to act as SLAVE, the following parameters must be specified:

- IP address / Netmask / Broadcast for Master (if Slave becomes Master in the event of a failure)
- IP address / Netmask / Broadcast for Slave
- PCI bus/slot of LAN card, if the server has more than one LAN card
- If the LAN card is a TokenRing card, the speed must be specified
- Indication whether call forwarding is necessary if the system is configured as Master

The following additional parameters are optional:

- Specification of applications to be stopped via **`procm`**

2.4 How to Execute the Switchover

In general, LAN access must be guaranteed during the execution of a switchover, because if the SSH session on one server is lost and the status change has already been started on the other, there would be a conflicting IP situation.

NOTE: The admin sessions are dropped during switchover.

This section describes two ways of doing the switchover: one in which LAN access is guaranteed, and one where the work is done on-site at the console of one of the servers. The state of the servers can be viewed by logging on as special user sso; the state and name of the server are displayed (SSO_SERVER1 and SSO_SERVER2 in this example).

2.4.1 LAN access is guaranteed (switchover is done at the same time on both servers)

Because a server is not being taken out of the network, and to prevent an IP conflict situation, both servers must be switched over at the same time.

1. Open a SSH session to both servers at the same time and log in with the special user account sso.
2. Select "configure system as Master" on the Slave server (see Figure 5).
3. Select "configure system as Slave" on the Master server (see Figure 4).
4. Activate these functions at the "same" time.

NOTE: SSO automatically initiates a reboot of the servers to activate the status change.

---

5. Once the master is up, SSH to the MASTER, log in using special user sso and check the status. It should be MASTER and "ok".
6. Once the slave is up, SSH to the SLAVE, log in using special user sso and check the status. It should be SLAVE and "ok".

NOTE: The first action to be taken on the Manager is to start the delta uploads on all switches in order to synchronize the new MASTER with all changes that have occurred between the SSO backup and the switchover in the network. Once this is done, CM can be used. If this action cannot be done directly then the automatic nightly delta upload will do the synchronization.

2.4.2 LAN access is not guaranteed (switchover is done on-site one server at a time)

If LAN access cannot be guaranteed, then the intervention must be done onsite from the console of one of the servers. The remote server is switched over first, and then the local server. The switchover can be done from either site, as described below.

Onsite at the location of the MASTER server (status before switchover)

1. Change the status of the SLAVE server to MASTER (remote server)
   - Log on to the console using account `engr` and ssh to the SLAVE server using account `sso`.
   - Select "configure system as Master" (see Figure 5).

NOTE: The server you are connected to will reboot and then become active as MASTER.

---

2. Directly after this activation it is very important to remove the LAN cable from the server you are working at.
3. Change the status of the MASTER server to SLAVE (local server)
   - Log on to this server's console again, this time **using account `sso`**.
   - Select "configure system as Slave" on this server (see Figure 4).

NOTE: SSO automatically initiates a reboot of the servers to activate the status change.

---

4. After the reboot, reconnect the LAN cable at the interface. This server is now activated as SLAVE, and the switchover is complete.
5. Once the Slave is up, log in at the console using special user `sso` and check the status. It should be SLAVE and "ok".
6. Once the Master is up, log in at the console using account `engr`. SSH to the MASTER, log in using special user `sso` and check the status. It should be MASTER and "ok".

NOTE: The first action to be taken on the Manager is to start the delta uploads on all switches in order to synchronize the new MASTER with all changes that have occurred between the SSO backup and the switchover in the network. Once this is done, CM can be used. If this action cannot be done directly then the automatic nightly delta upload will do the synchronization

---

Onsite at the location of the SLAVE server (status before switchover)

1. Change the status of the MASTER server to SLAVE (remote server)
   - Log on to the console using account `engr` and SSH to the MASTER server using account `sso`.
   - Select "configure system as Slave" (see Figure 4).

NOTE: The server you are connected to will reboot and then become active as SLAVE.

---

2. Directly after this activation it is very important to remove the LAN cable from the server you are working at.
3. Change the status of the SLAVE server to MASTER (local server)
   - Log on to this server's console again, this time **using account `sso`**.
   - Select "configure system as Master" on this server (see Figure 5).

NOTE: SSO automatically initiates a reboot of the servers to activate the status change.

---

4. After the reboot, reconnect the LAN cable at the interface. This server is now activated as MASTER, and the switchover is complete.
5. Once the Master is up, log in at the console using special user `sso` and check the status. It should be MASTER and "ok".
6. Once the Slave is up, log in at the console using account `engr`. SSH to the SLAVE, log in using special user `sso` and check the status. It should be SLAVE and "ok".

Figure 4 Smart Switchover: Configuring the Current MASTER as SLAVE

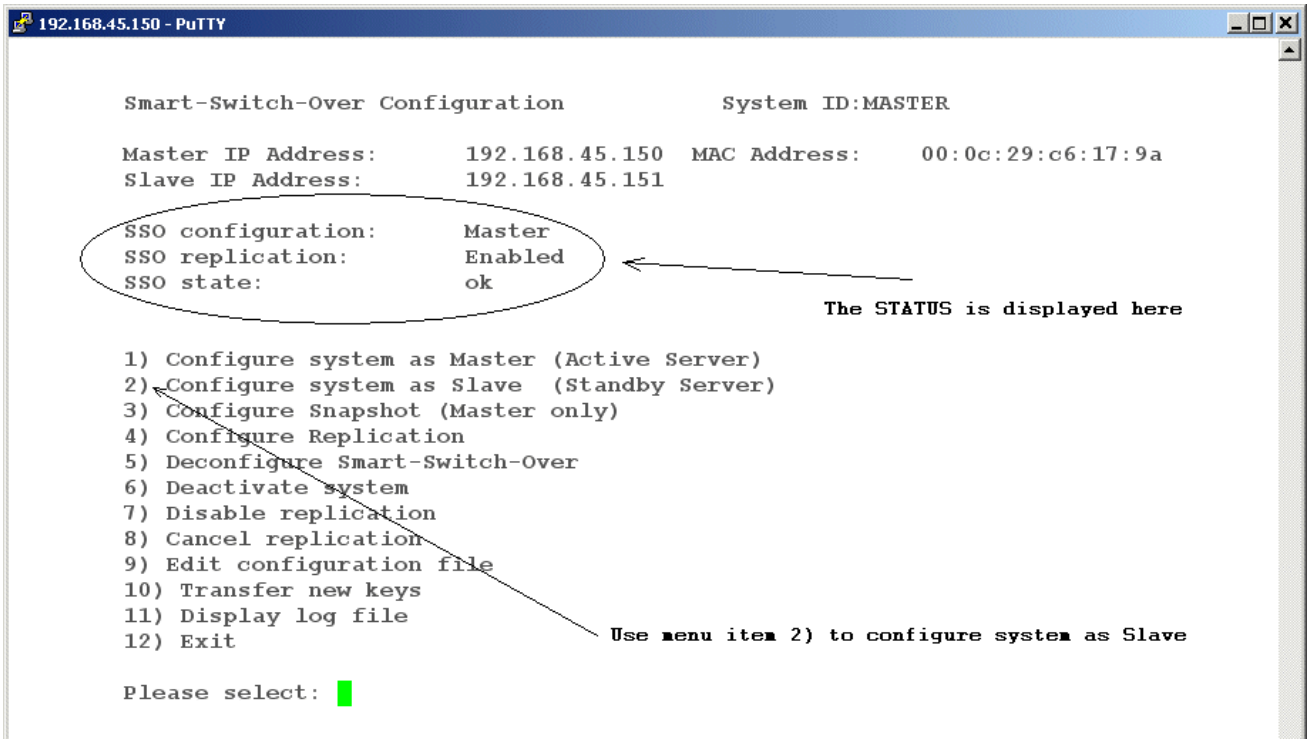
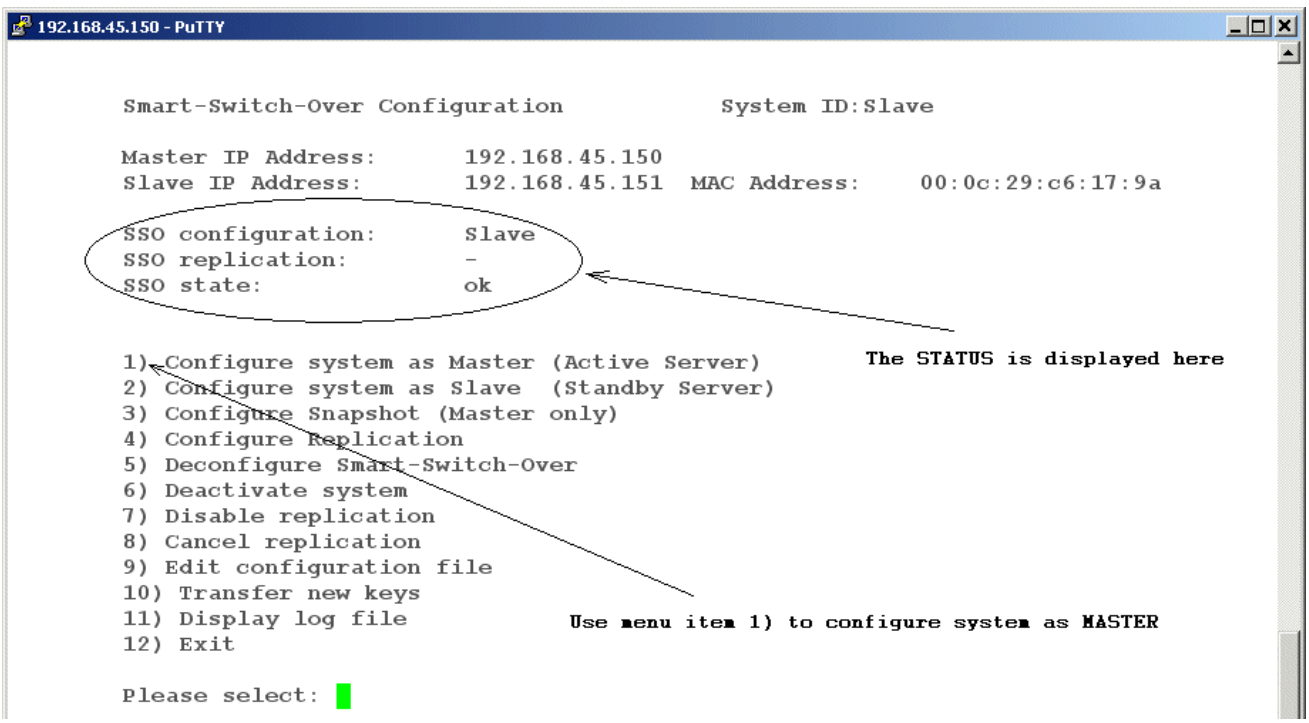


Figure 5 Smart Switchover: Configuring the Current SLAVE as MASTER



2.5 Updating an SSO System

Updates for an SSO system are performed the same way as for a normal OpenScape 4000 Manager system, via CD or SWT2/SWA2.

NOTE: Please refer to the **OpenScape 4000 Manager Installation and Service Manual**, Section 5.4, “Upgrade and Update Scenarios for OpenScape 4000 Manager” for more information.

The SSO configuration file is not modified during the update procedure.

Updates (Minor/Fix/Hotfix) must be applied on both Master and Slave systems.

After each update procedure (Minor/Fix/Hot Fix activation) it is recommended to initiate the Slave configuration again to ensure that the updates are replicated to the 'shadow' (temporary) Slave partition.

Make sure that no data restore operations take place in which the restored backup data are from a newer or older software version, i.e., during a Replication cycle, the Master and Slave must have exactly the same software status.

2.6 Example of an SSO Configuration File

```
#
# This file includes all necessary parameters for "Smart Switch
Over (SSO)"
#
#
# Do not remove or edit the following line !!!
VERSION=7.0


#################################################################
################
# Here you can specify an unique identifier for the system
# This identifier is displayed in sso-menu
# (The identifier will be truncated to max. 16 character)
SystemIdentifier=MASTER
#
#################################################################
################


#################################################################
################
#
# The following section specifies the LAN configuration of the
Server
# Attention: Both (Master and Slave) Addresses must be specified
#


# IP-Address if Server acts as Master
MasterIPAddress=158.226.25.189
MasterIPNetmask=255.255.255.0
MasterIPBroadcast=158.226.25.255


# IP-Address if Server acts as Slave
SlaveIPAddress=158.226.25.181
SlaveIPNetmask=255.255.255.0
SlaveIPBroadcast=158.226.25.255


# If Server has more than one LAN card the card name ethX and
MAC address of the card which
# connects Master/Slave must be specified
```

```
LanCardName=
LanCardMAC=


# If TokenRing is used for the specified LAN the Ring speed must
be selected
# Possible values are 4/16/100
TokenRingSpeed=


# VGName is used for specification VG Name which will be used
during SSO.
# It has to be specified. If one VG is used then it has to be
mentioned there
VGName=system
#
##################################################################
################


##################################################################
################
#
# The following section specifies the LAN configuration of a
second LAN card
# !!! These parameter are optional !!!
# If server has two LAN cards but nothing is specified here the
configuration
# will be restored from Master (only on a Slave System)
# if second LAN card parameter are specified both (Master and
Slave) Addresses
#  must be specified if system is configured as Slave


# IP-Configuration of second LAN card if Server acts as Master
SecMasterIPAddress=
SecMasterIPNetmask=
SecMasterIPBroadcast=


# IP-Configuration of second LAN card if Server acts as Slave
SecSlaveIPAddress=
SecSlaveIPNetmask=
SecSlaveIPBroadcast=


# Lan card name ethX and MAC address of the card must be
specified
```

```
SecLanCardName=
SecLanCardMAC=

# If TokenRing is used for the specified LAN the Ring speed must
be selected
# Possible values are 4/16/100
TokenRingSpeed=

# VGName is used for specification VG Name which will be used
during SSO.
# It has to be specified. If one VG is used then it has to be
mentioned there
VGName=system
#
##################################################################
################

##################################################################
################
# Specify how often a Backup is done if Server acts as Master
#
# specify Backup frequency
# possible values:
Monday,Tuesday,Wednesday,Thursday,Friday,Saturday,Sunday
#          or    : daily
# (two ore more values must be seperated with commas)
MasterBackupFrequency=daily

# specify start time of Backup
# Format: Hour(0-23):Minute(0-59)  e.g. 23:15
MasterBackupStartTime=10:00

##################################################################
################
#
# The following section specifies the Application handling

# Specify name of Applications (Group name within Procmgr) which
are
# stopped if system is configured as Slave and started if system
# is configured as Master
# (two ore more Applications must be seperated with commas)
```

```
SlaveDeactAppl=cm_subadm,FaultM,COL,Batch,MPCID,PM


# Specify name and path of scripts which shouldn't be executed
if system is
# configured as Slave
# e.g. openFT shouldn't be started during startup of system
# (two ore more scripts must be seperated with commas)
SlaveDeactScripts=/etc/init.d/openFT,/etc/init.d/snmpdm
#
#
################################################################
################


################################################################
################
#   This variable specifies if replication will be run on the
Master
#
# (Allowed values are: yes/no)
ReplicationEnable=yes



################################################################
################
#   This variable specifies how often replication will be run on
the SLAVE
#   if replication fails
#
ReplicationRetryCount=5



################################################################
################
#   This variable specifies when Master should try to continue
with replication
#   when previous replication fails
#   Value is in seconds
#
ReplicationRetryInterval=30
################################################################
################
# User which will be used for replication
```

```
#
# (Allowed accounts are: root/engr)
ReplicationAccount=root


################################################################
################
# The following section specifies the Call-Forward configuration
for
# connection interface via - Analogue/Digital Modems
# - PWS0, PWS2 or PWXV-2/4 boards
#
#
# Decide if Call-Forwarding must be configured if this system
acts as Master
# (Allowed values are: yes / no)
CallForwardNecessary=no



# Call-Forward configuration for analogue modems
# The following paramter must be specified if an analogue modem
is available:
# AModem=<SYSTEM-ID>/<Telephon-Number-1-From>-><Telephon-Number-
1-To>[/<Telephon-Number-2-From>-><Telephon-Number-2-To ...]
# (data for two ore more SYSTEMs must be seperated with commas)
#
# eg. AModem=abcd/12345->6789
AModem=



# Call-Forward configuration for digital modems
# The following paramter must be specified if a digital modem is
available:
# DModem=<SYSTEM-ID>/<Telephon-Number-1-From>-><Telephon-Number-
1-To>[/<Telephon-Number-2-From>-><Telephon-Number-2-To ...]
# (data for two ore more SYSTEMs must be seperated with commas)
#
# eg. DModem=abcd/12345->6789
DModem=TEST/12044->12045



# Call-Forward configuration for ISDN-S0 connection interface
(PWS0 board)
```

```
# The following paramter must be specified if PWS0 board is
available:
# PWS0=<SYSTEM-ID>/<Telephon-Number-From>-><Telephon-Number-To>
# (data for two ore more boards must be seperated with commas)
#
# eg. PWS0=abcd/12345->6789
PWS0=



# Call-Forward configuration for ISDN-S2 connection interface
(PWS2 board)
# The following paramter must be specified if PWS2 board is
available:
# PWS2=<SYSTEM-ID>/<Telephon-Number-From>-><Telephon-Number-To>
# (data for two ore more boards must be seperated with commas)
#
PWS2=



# Call-Forward configuration for MSV1 connection interface
(PWXV-2/4 board)
# The following paramter must be specified if PWXV board is
available:
# PWXV=<SYSTEM-ID>/<Telephon-Number-1-From>-><Telephon-Number-1-
To>[/<Telephon-Number-2-From>-><Telephon-Number-2-To ...]
# (max. 4 Telephon-Numbers for each PWXV board are allowed!!
# (data for two ore more boards must be seperated with commas)
#
PWXV=


################################################################
################
```

NOTE: The parameter `CallForwardNecessary` is particularly noteworthy. This parameter specifies whether call forwarding is to be enabled or disabled when the server is configured as Master.

2.7 Upgrade Procedure for OpenScape 4000 Manager with SSO

Current status:

SSO_Server_1= MASTER

SSO_Server_2 = SLAVE

DAY 1: Upgrade SSO_Server_2

NOTE: Times in parentheses (HH:MM) are included in order to provide an estimate of how long each step takes.

All day: frozen period (only display mode)

1. (10:00) Disconnect SSO_Server_2 from LAN (as soon as SSO restore is completed, can also be earlier)
2. (10:00 - 14:00) FULL backup of SSO_Server_2 to tape
3. (14:00) Configure SSO_Server_2 as MASTER
4. (14:00 - 17:30) Upgrade SSO_Server_2 with KVnnn + Patches
5. (17:30) Execute procedure **"Customer-specific adaptations"** (if applicable; refer to Section 2.7.1)
6. (18:00) Collect Call Details Records (CDR) from all systems to SSO_Server_1
7. (18:10) HIS reports pull PO's on SSO_Server_1
8. (18:20) Start Collect on OpenScape AM
9. (18:30) Deconfigure Smart-Switch-Over on SSO_Server_1
10. (18:40) Reconnect SSO_Server_2 to LAN
11. (18:50) Upload ALL for all systems on SSO_Server_2 (the new MASTER)
12. (19:30) Functional testing of SSO_Server_2

DAY 2: Backup SSO_Server_1

1. (7:00) Stop frozen period
2. (8:30) Disconnect SSO_Server_1 from LAN
3. (8:40) Configure SSO_Server_1 as MASTER
4. (8:45) Start full backup of SSO_Server_1 on tape
5. (13:00) End of full backup

DAY 3: Upgrade SSO_Server_1

1. (8:30) Upgrade SSO_Server_1
2. (10:00) Execute procedure **“drop pm table”** (refer to Section 2.7.2)
3. (10:15) Install patches
4. (11:45) Execute procedure **"Customer-specific adaptations"** (if applicable; refer to Section 2.7.1)
5. (12:00) Configure SSO_Server_1 as SLAVE and reboot
6. (12:30) Reconnect SSO_Server_1 to LAN; reboot NA
7. (13:00) Check functionality

DAY 4:

Check SSO backup/restore functionality

2.7.1 Customer-specific adaptations on the OpenScape 4000 Manager

NOTE: This section describes a general adaptation of CM and and is not specific to the SSO feature. The main point to keep in mind in the SSO scenario is that if these adaptations are made on the Master server, they must also be made on the Slave server.

NOTE: The following changes should be executed after each upgrade or patch upgrade.

1. Increase the number of extensions in the CM-station choice list.

Under the directory **/opt/cm/sad/VERIFY**

```
-r--r--r-- 1 sad unity 2813253 Apr 13 18:19 uxvporxx.txt
-r--r--r-- 1 sad unity 20386 Apr 13 18:22 uxvdecxx.txt
#
#
# grep 10000 uxvporxx.txt uxvdecxx.txt (10000 is the new value;
these are the patched files)
uxvporxx.txt: LIMIT: 10000
uxvdecxx.txt: CHOICELIST-DATA: 10000
#
```

```
1) file
/opt/cm/sad/VERIFY/uxvdecxx.txt
```

Search for "CHOICELIST-DATA" and change from

CHOICELIST-DATA: **1000**
to CHOICELIST-DATA: **10000**

2) file

/opt/cm/sad/VERIFY/uxvporxx.txt

Search for CHOICELIST_PORT_SELECT_EXTENSION_NET

```
CHOICELIST-SELECT:      CHOICELIST_PORT_SELECT_EXTENSION_NET

                IF:     $2 and
                        ( _22 or _23 )

                        APPLY:  SELECTS:
                                RULE_PORT_DIMSU_EXTENSION ,
                                RULE_PORT_CHECK_FCFW
                        RELATIONS:

RULE_PORT_EXISTING_TECHNICAL_EXTENSION_1 ,

RULE_PORT_EXISTING_TECHNICAL_EXTENSION_2 ,
RULE_PORT_S0BUS_ALLOWED_LOG_TLN_EXTEND_PTY_EXT
                        END;

                ACTION: SELECT $1 = pdn_8.station_no ,
                        pdn_8.reserved_pen : 2 ,
                        pdn_8.switch_name : 2,
                        { SQL } length ( pdn_8.station_no )
                        FROM priv_dial_number pdn_8

                        WITH CONDITIONS

                                C1 = (  pdn_8.switch_name =
                                                $2   ) ,
                                C2 = (  pdn_8.domain = $29  ) ,
                                C3 = (  pdn_8.type = "102" AND
                                  pdn_8.status = "002"
) ,
                                C7 = (  @CDB_ACTIVE_2 ( pdn_8 )
   )
```

```
                        ORDER BY 4,1;

                        LIMIT:  500
```

"Limit: **500**"

Change to"Limit: **10000**"

3) IMPORTANT !!! To activate the changes you need to restart the CM services:

#procadmin –t –g cm_subadm

#procadmin –s –g cm_subadm

2. Change port numbers as needed on the OpenScape Manager as well as on the switches

Logging Management port 5005 >> 5015

var/logm/tmp/ LoggingSessControl_port.conf

procadmin -t -g LogM

procadmin -s -g LogM

CORBA port 5010 >> 5400

/opt/sysm/bin/symService_port.conf

procadmin -t -g SysM

procadmin -s -g SysM

3. PM visualization of reports using MS Excel

MS Excel 2000 is required

Workaround: patch files

2.7.2 How to Drop and Recreate the PM Table on OpenScape 4000 Manager

1. Load the informix variables:

   ```
   # cd /home/engr/PM
   #. /opt/informix/*var
   ```

2. Create the dbschema of the pm table with the command:

   ```
   #dbschema -d cdb -t pm_cdrdatatbl 'pm.sql'
   ```

3. Default the file size is limited to 1 Gb, to unlimit this execute:

   ```
   #ulimit -f unlimited
   #ulimit -a
   ```

4. #dbaccess cdb

   ```
   select Query-language and type:
   unload to '/var/pm/pmdata.unl' select * from pm_cdrdatatbl;
   This will only work when the unload file is < 2 Gbyte. If not
   you can use the special unload script.
   ```

5. drop table pm_cdrdatatbl;

6. select Query-language/ Choose: select the pm sql command you made before and run it

7. PM data can be reloaded with the command:

   ```
   load from '/var/pm/pmdata.unl' insert into pm_cdrdatatbl
   ```

procadmin -t -g COL
procadmin -t -g PM
procadmin -t -g FaultM
procadmin -t -g cm_subadm
procadmin -t -g LogM
procadmin -t -g SysM

3 Switchover Check List for OpenScape 4000 Manager Server

NOTE: **Software Version Information**
Please also refer to the Release Notes, especially for SSO, for current information about the latest software version released.

NOTE: **Attention:**

To use the SSO feature, a completely new installation of Linux SLES11 and OpenScape 4000 Manager is **necessary** due to LVM requirements. Update from Manager 3.1 is not supported on SSO configurations.

In order to use SSO configuration, it is neccesary to install the SuSe Linux Enterprise Server 11 (SLES11) system with a Logical Volume Manager (LVM) partitioning as described in the **OpenScape 4000 Manager Installation and Service Manual**.

SSO has higher HDD requirements; it requires twice the HDD size compared to installations without SSO.

During initial partitioning (when SLES11 is installed) it is necessary that **at least** the half of the HDD's capacity is free. This applies regardless of the total amount of disk space on the HDD. If this precondition is not considered, the SSO functionality may not work properly.

It is mandatory to use the GRUB boot-loader. Otherwise SSO will not start.

3.1 Switching Over to the Emergency (Standby) Server

3.1.1 Activating the Emergency (Standby) Server

To switch over from the defective Master to the Emergency (Standby) Server you need to change the status of the Standby server from SLAVE to MASTER and to reboot the server in order to activate it as the new Master. For more details please refer to Failure of Master Server

3.1.1.1 Emergency Server Not Active?

Verify whether the Emergency Server is active.

Verifying the Power Supply

1. If the server is out of operation due to power failure, restart the server.

Verifying the LAN Cable

1. Is the LAN cable connected to the server?
2. Connect the LAN cable to the server, if necessary.

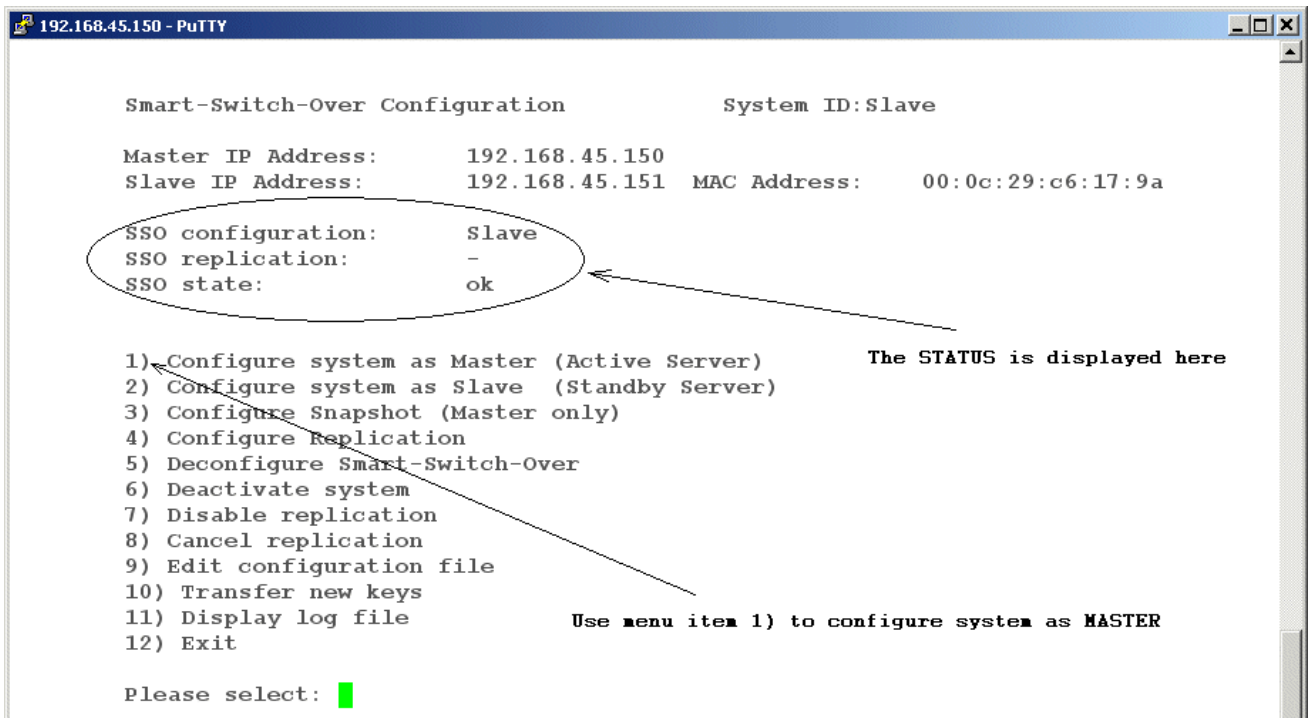
Verifying the LAN Link LED

1. Is the LAN Link LED inactive?
2. If the LAN Link LED is inactive -> Error is caused by LAN infrastructure -> Notify IT department.

3.1.1.2 Switching Over the Emergency (Standby) Server to MASTER Status

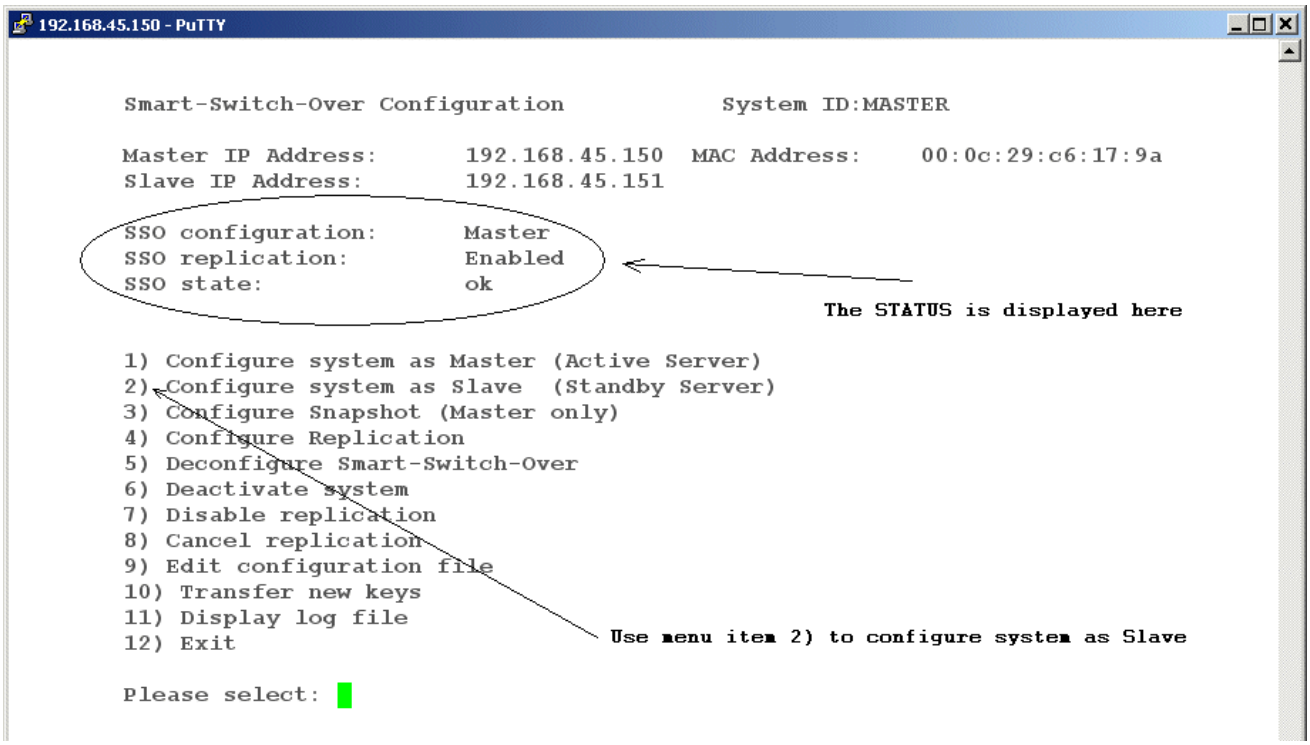
1. Log on to the Standby server using the **sso** user ID - see Login. After successful login the SSO main menu will be displayed; the **SSO configuration** status displays “Slave” (this is necessary in order to be able to switch the server to “Master” (Active Server) subsequently).

Figure 6 Switching Over the Emergency Server to MASTER Status



2. In the SSO menu, select item **1) Configure system as Master (Active Server)**, to configure the server as MASTER server.
3. When configuring the server as MASTER has finished, the system will be re-booted.
4. Next, verify the status of the server. To do this, please proceed as follows:
5. Log on to the Standby server using the **sso** user ID - see Login. After successful login the SSO main menu will be displayed; the **SSO configuration** status is now displaying “Master”.

Figure 7 Emergency Server switched to MASTER Status



The Standy Server is now configured as MASTER (Active Server).

3.1.2 Deactivating the Master Server

After activating the SSO Standby Server please shut down the defective Master server and apply the following note to it:

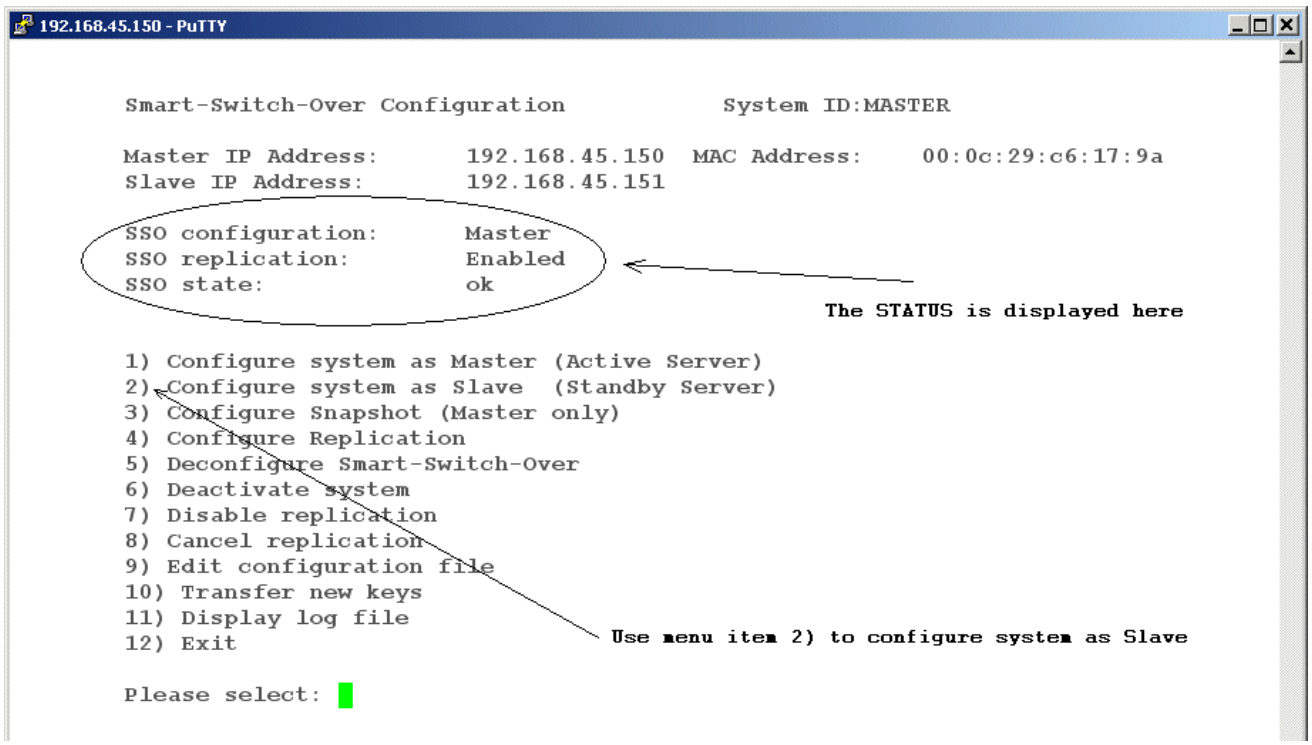
NOTE: **Attention:**
OpenScape 4000 Manager Server is defective! Do NOT turn on, since SSO Standby Server is active.

See also

- Failure of Master Server

In order to deactivate and turn off the defective Master, log on to the Master server using the **sso** user ID - see Login. After successful login the SSO main menu will be displayed; the **SSO configuration** status is now displaying “Master”.

Figure 8 Status Display of Master Server



Select **Deactivate System** from the main menu. The system shuts down and turns off.

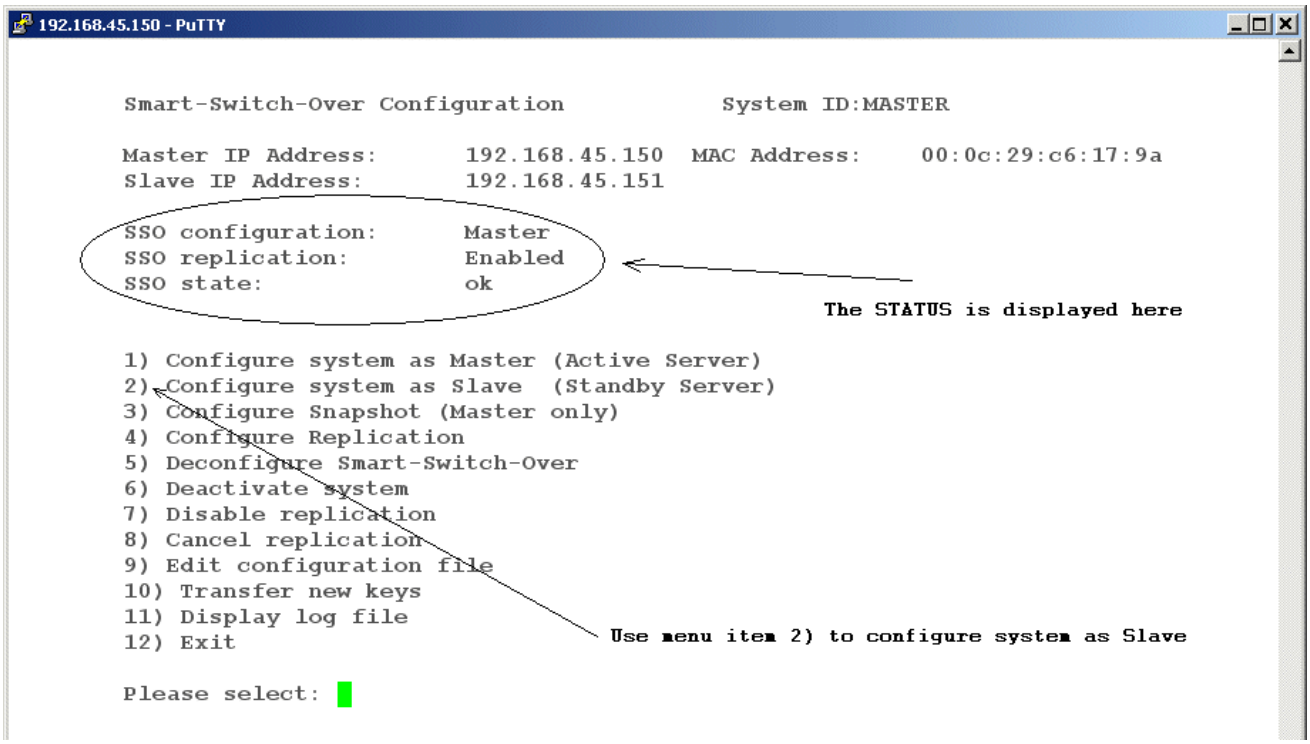
3.2 Switching Back to the Initial Master Server

In order to switch back the deactivated Master server from the SLAVE to the MASTER status and re-activate it as Master server, you need to perform the steps described below:

3.2.1 Switching Back the Emergency Standby Server to SLAVE Status

1. Log on to the Standby server using the **sso** user ID - see Login. After successful login the SSO main menu will be displayed; the **SSO configuration** status is displaying “Master”.

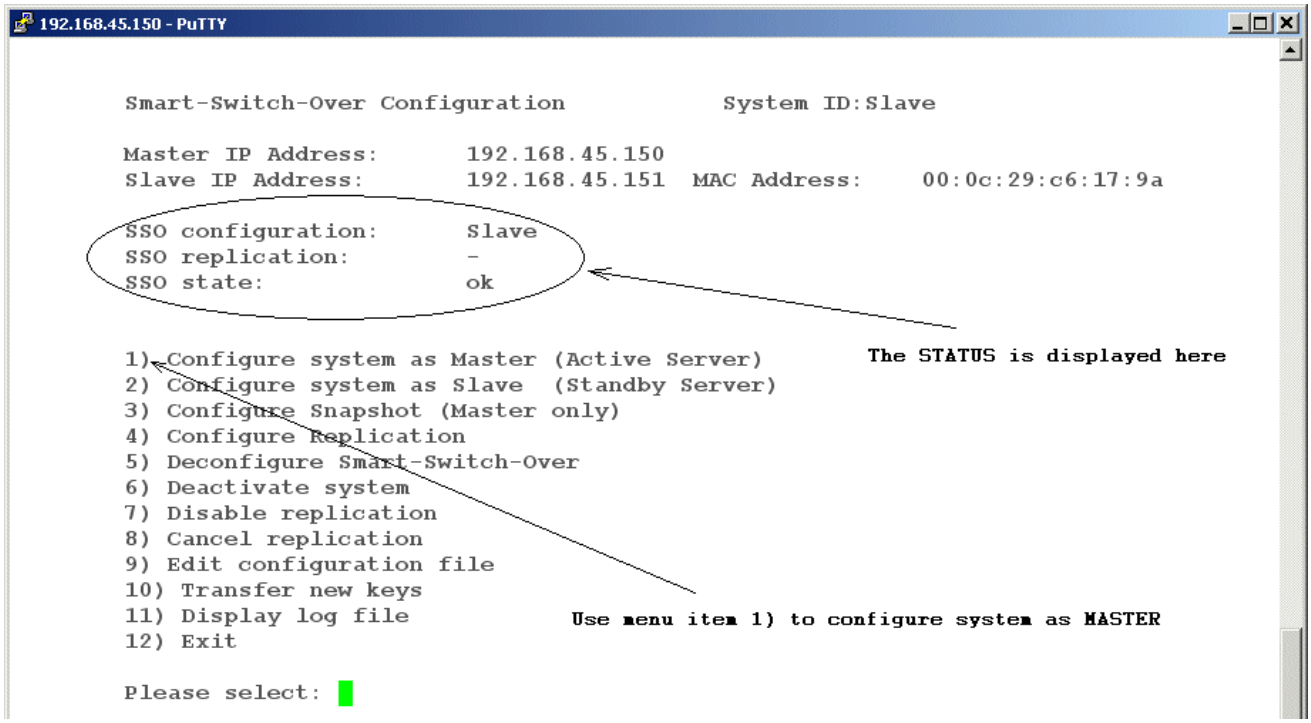
Figure 9 Status Display of Master Server



2. In the SSO menu, select item **2) Configure system as Slave (Standby Server)**, to configure the server as SLAVE server.
3. When configuring the system as SLAVE server has finished, the system is re-booted.
4. Next, verify the status of the server. To do this, please proceed as follows:

5. Log on to the Standby server using the **sso** user ID - see Login. After successful login the SSO main menu will be displayed; the **SSO configuration** status is displaying “Slave”.

Figure 10 Status Display of Slave Server



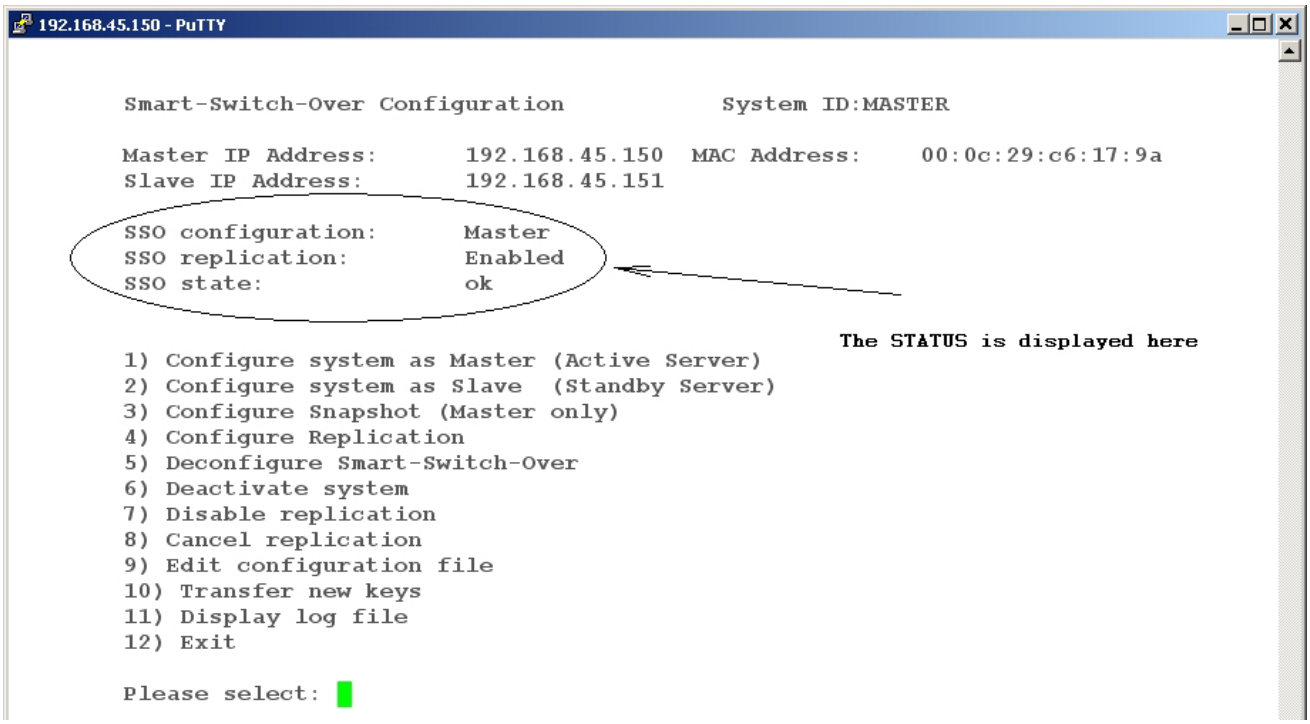
The Emergency Standby server is now configured as SLAVE server again.

3.2.2 Activating the Master Server and Verifying the MASTER Status

Since the Master server had been turned off, you need to access the Master locally and to configure and activate it as MASTER server again. See **Configure system as Master (Active Server)**, Switchback to the Original Master and Failure of Master Server.

1. Power the server up again.
2. Verify the server´s status as soon as the server run-up is completed. Log on to the Master server using the **sso** user ID - see Login. After successful login the SSO main menu will be displayed; the **SSO configuration** status is displaying “Master”.

Figure 11 Status Display of Master Server



The server is now configured as MASTER (Active server) again.

4 Using Smart Switch-Over

4.1 Installing the SSO Software

The ASsso software package contains all the necessary SSO functionality and is automatically installed on all OpenScape 4000 Manager servers.

NOTE: **Software Version Information**
Please also refer to the Release Notes, especially for SSO, for current information about the latest software version released.

NOTE:
Attention:

In order to use SSO, it is neccesary to have the SuSe Linux Enterprise Server 11 (SLES11) system installed with Logical Volume Manager (LVM) partitioning as described in the in the **OpenScape 4000 Manager Installation and Service Manual**.

SSO has higher HDD requirements; it requires twice the HDD size compared to installations without SSO.

During the OS installation in initial partitioning, at least half of the HDD's capacity must remain free. This applies regardless of the total amount of disk space on the HDD. If this precondition is not considered, SSO will not work properly.

It is mandatory to use the GRUB boot-loader. Otherwise SSO will not start.

4.2 Login

All SSO functionality is controlled via the **sso** user ID.

NOTE: **Attention:**
There is no graphical interface for SSO login, i.e. you log on to the server and start SSO by directly entering the **sso** account (user ID) and the corresponding password in the server´s command line (on ASCII level).

Starting the Application

To start the **SSO** application on a server, enter the **sso** account and the corresponding **password** into the command line (i.e. on ASCII level) on the server console.

Immediately following first installation, the password for the **sso** account is locked. Unlocking the account and setting the password is done via the Web access of the **cusa** administrator account. Please refer to **Access Management - System Account Management** for details.

Related Topics

User Interface

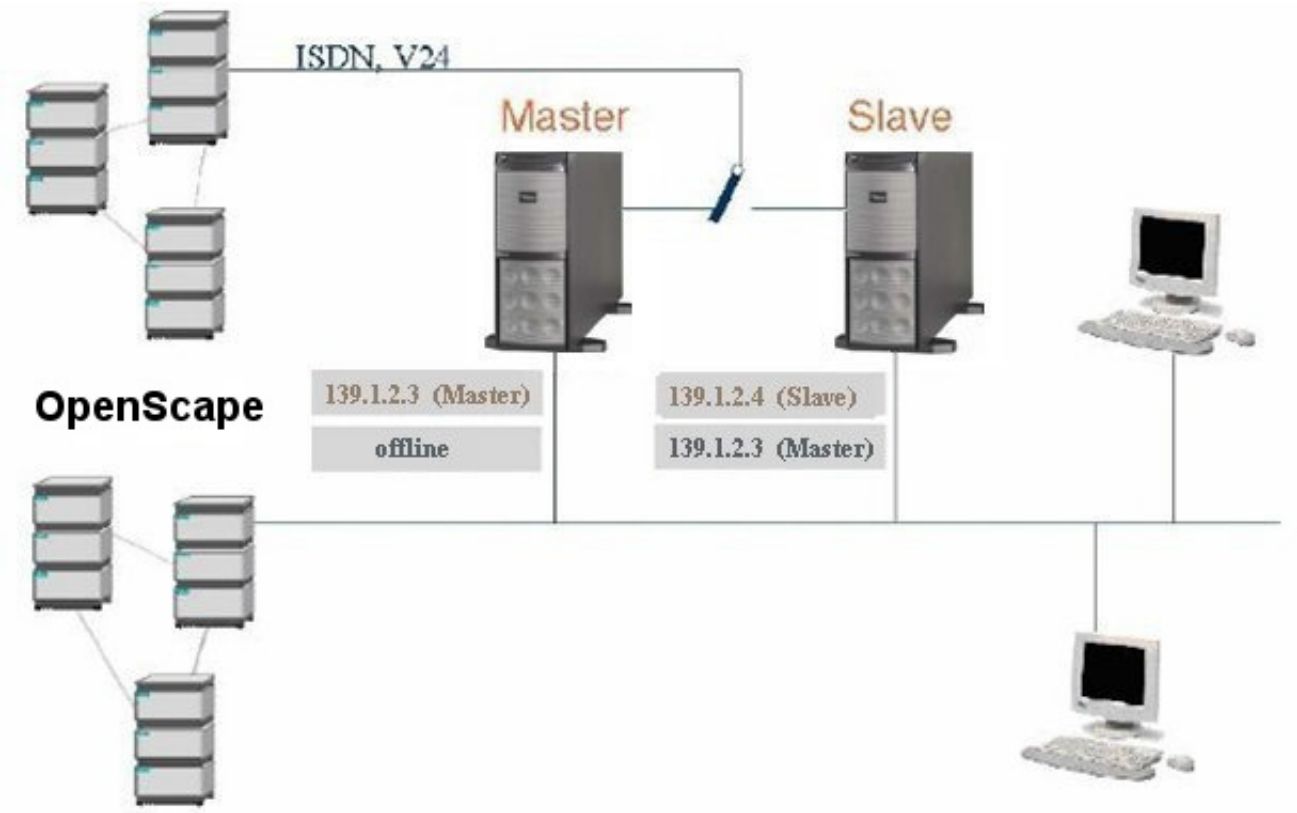
SSO Status

4.3 Arrangement of Servers

Both servers (Master and Slave) are included in the network, but the Slave is passive. Communication is handled by the Master. If the Master fails, the Slave needs to be activated manually, and the communication function is switched over to the Slave (further details in the sections that follow).

In these Master/Slave configurations, both Master and Slave must be Primergy machines.

Figure 12 Master/Slave Servers for “Smart Switchover”



NOTE: The Master and Slave servers must be equipped with the same hardware.
Only Intel-based servers of the exact same type (e.g. Primergy TX 300), certified and released for the current version of OpenScape 4000 Manager, are to be used.
The hardware must be certified and released for the current version of OpenScape 4000 Manager.

4.4 Switchover Process

4.4.1 Switchover Components

The basic components involved in switchovers are **communication**, **data replication**, and the **productive processes** of the OpenScape 4000 Manager (Configuration Management, Fault Management, and Collecting Agent).

4.4.2 Switchover Scenarios

This section describes the most common switchover scenarios:

Normal Operation

Failure of Master Server

Switchback to the Original Master

4.4.2.1 Normal Operation

Master

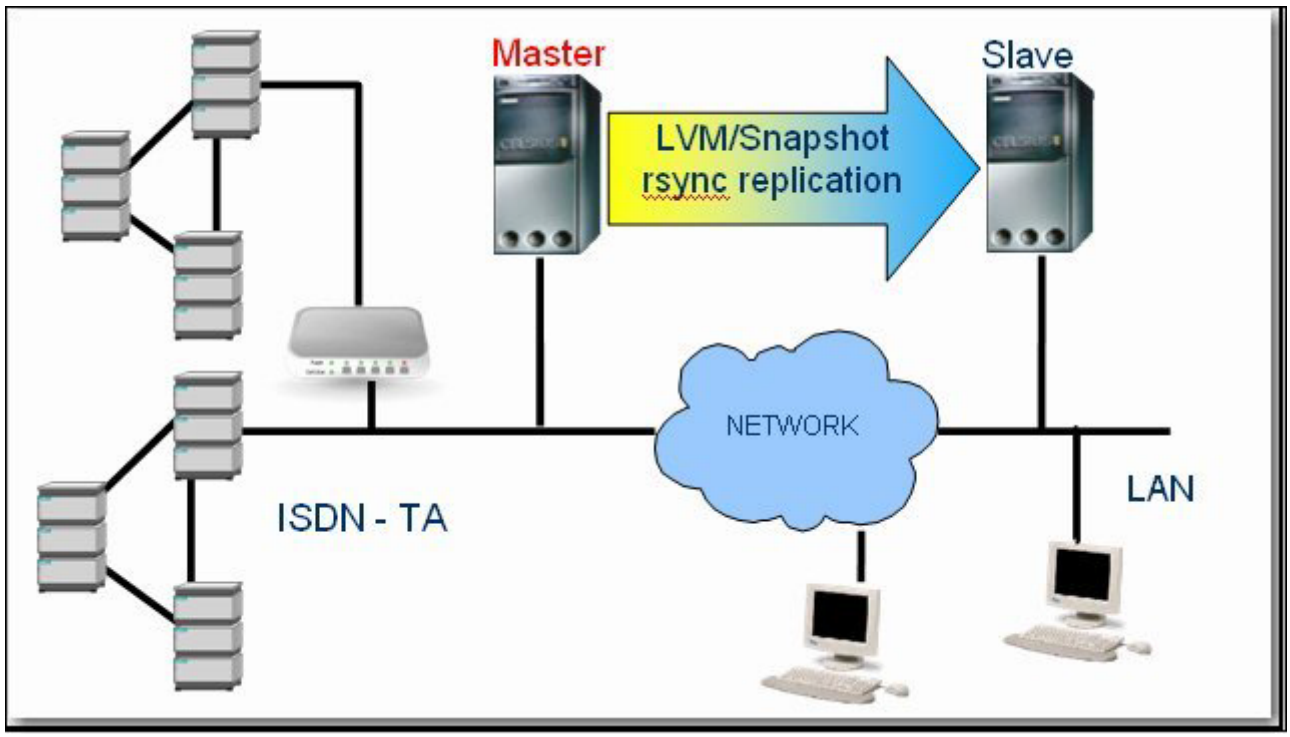
- The Master server is in productive operation on the network (see figure below).
- Communication is directed to the Master server.
- The Master server saves its data on the Slave server (according to the LVM/ Snapshot/rsync configuration).

Slave

- The processes for productive operation have been deactivated by the SSO Slave configuration.
- The rsync process imports current data from the Master server.
- Regular automatic restores are run on the Slave server.

NOTE: Other backup & restore operations are not allowed on the Slave server.

Figure 13 Normal Operation Master/Slave Servers



4.4.2.2 Failure of Master Server

The failure of the Master is not detected automatically. The operator needs to manually initiate the switchover process as soon as he/she finds out that the master has failed or is only partially operational:

1. Remove the Master server from the network, even if it is operational in part. (The steps necessary to identify and correct the cause of the failure can be initiated at a later time.)
2. Log in using **sso** account - see Login;
3. Complete/edit the SSO configuration file using the menu item **Edit configuration file**;

4. On the Slave server, select the SSO menu item **Configure system as Master (Active Server)**, thereby making this system the new Master.

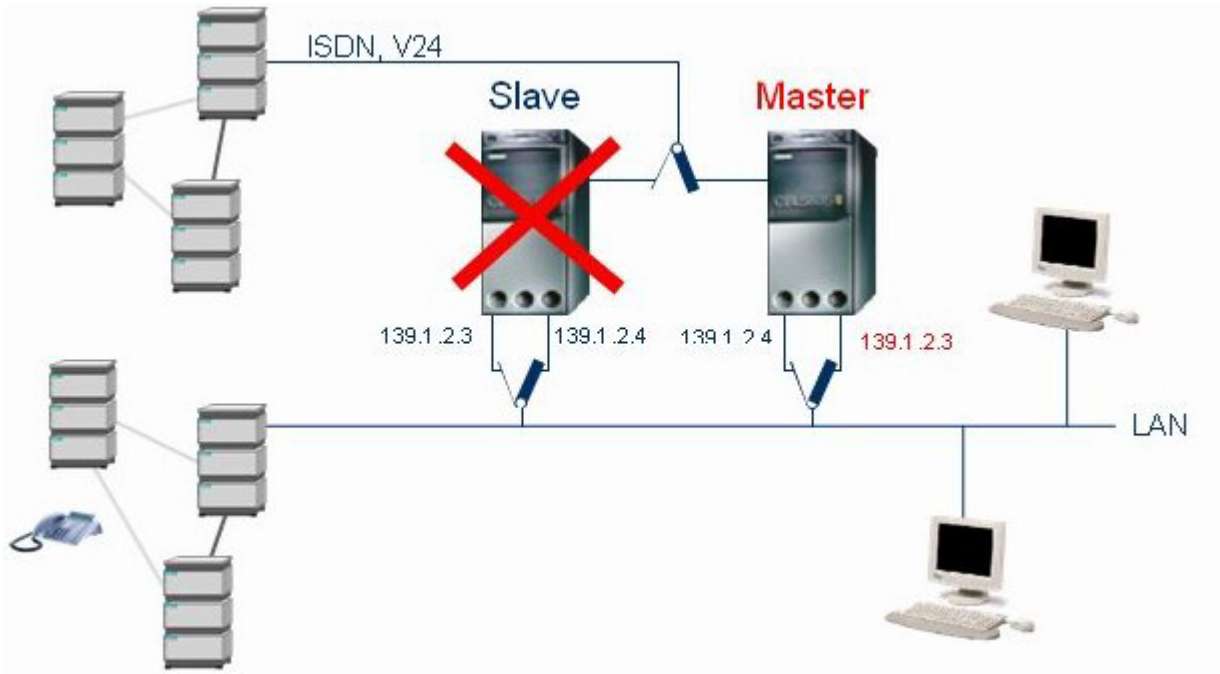
NOTE: Clients need to log on again, since their connections were interrupted when the Master server was removed from the network.

7

WARNING

After activating the SSO Slave Server (Standby Server) as the new Master Server please turn off the defective Master and apply the following note to it:
Warning: OpenScape 4000 Manager Server is defective. Do NOT turn on, since Standby server is active.

Figure 14 Failure of Slave Server



4.4.2.3 Switchback to the Original Master

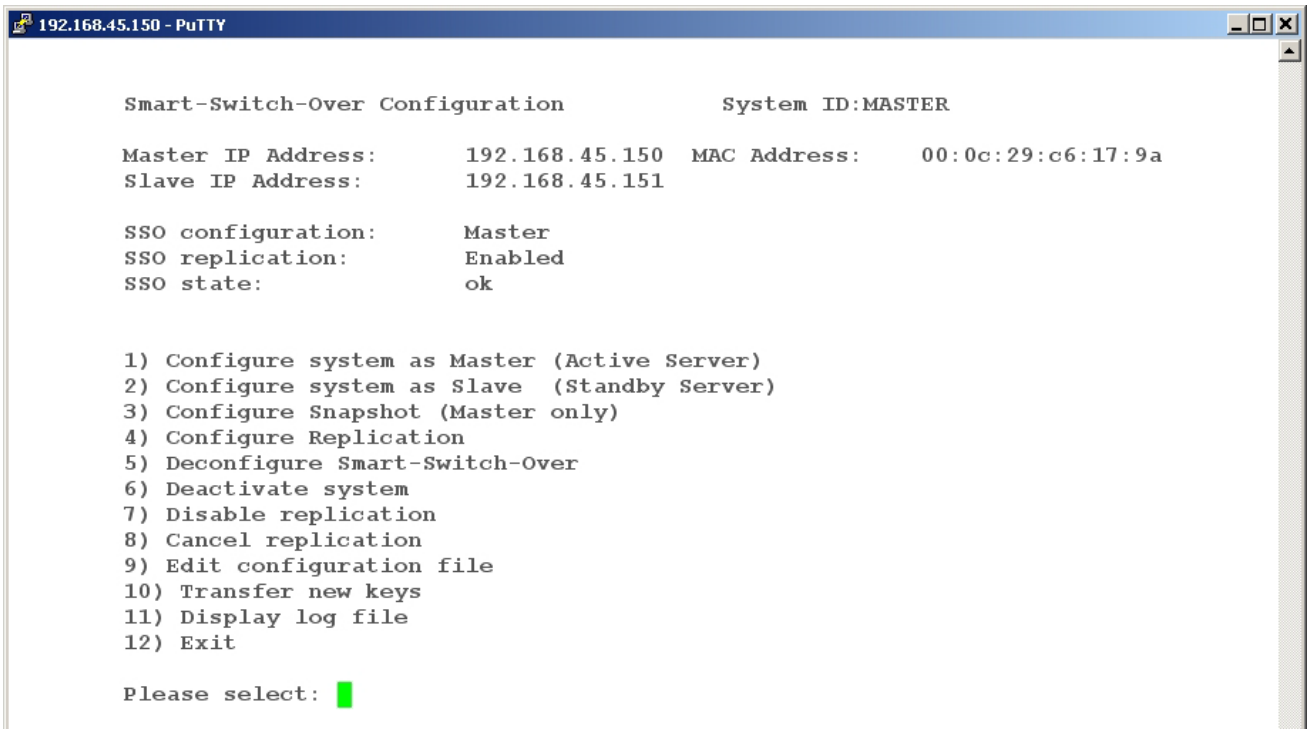
The procedure for switching back to the original Master server is similar to that described in Failure of Master Server. The server that was originally the Master must first be installed as the Slave, using the procedure for initial SSO installation.

1. Configure the former Master as **Slave** (same procedure as during initial installation).
   To do this, start SSO on the system and select **Configure system as Slave (Standby Server)**.
2. Start replication from the Master server to the Slave server.
3. Shut down the current defective Master and remove it from the network.
4. On the Slave server, select the SSO menu item **Configure system as Master (Active Server)**, thereby making this system again the new Master.
5. Configure the former Master as Slave by starting SSO and selecting **Configure system as Slave (Standby Server)**.
6. Remove the warning message referring to the defective Master.

4.5 User Interface

After successful login the following menu is displayed:

Figure 15 User Interface SSO Configuration



To select and open a menu item, enter the corresponding figure and press the **Return** key.

4.5.1 SSO Status

The status of SSO is displayed in the upper part of the SSO window:

SSO Configuration

Indicates whether SSO is configured as Master or Slave (if SSO is not active, " - " is displayed)

SSO Replication

Indicates whether the SSO replication is enabled or disabled.

SSO state

Indicates the status of SSO. The following values are possible:

Configuration running: Configuration as Master/Slave is currently in progress.

Deconfiguration running: Deconfiguration is currently in progress.

Replication running: Data replication operation is currently in progress.

Configuration failed: An error occurred during configuration. System may be inconsistent.

Deconfiguration failed: An error occurred during deconfiguration. System may be inconsistent.

Replication failed: An error occurred during data synchronization. System may be inconsistent. Next data replication will take place as scheduled.

ok: Everything is in order. The "OK" message is displayed following successful configuration as Master/Slave, and following a successful data backup/restore operation, for example.

A Appendix: Installation of SLES11 with LVM

SSO needs a special installation of Linux SLES11 (Enterprise Server 11). SLES11 has to be installed on a LVM (Logical Volume Manager) partition.

NOTE:
Attention:

SSO has higher HDD requirements; it requires twice the HDD size compared to installations without SSO.

During initial partitioning (when the operating system is installed) it is necessary that **at least** the half of the HDD's capacity is free. This applies regardless of the total amount of disk space on the HDD. If this precondition is not considered, the SSO functionality may not work properly.

It is mandatory to use the GRUB boot-loader. Otherwise SSO will not start.

SSO allows to use bonding interfaces. For more details please see Section 2.2.3, "Communication".

NOTE: Please follow the **OpenScape 4000 Manager Installation and Service Manual**, Section 3.6, "Operating System Installation".

Index