MiVoice 5000 Manager - Redundancy

12/2024

AMT/PTD/NMA/0046/12/4/EN

Warning
Although the information provided in this document is considered as pertinent, Mitel Networks Corporation (MITEL ®) cannot guarantee the accuracy thereof.
The information may be changed without notice and should not be interpreted in any way whatsoever as a commitment on the part of Mitel, its affiliated companies or subsidiaries.
Neither Mitel nor its affiliated companies or subsidiaries may be held liable for any errors or omissions made in this document. This document -may be reviewed or re-edited at any time in order to add new information.
No part of this document may be reproduced or transmitted in any form or by any means whatsoever - be it electronic or mechanical - no matter the purpose thereof, without the prior written consent of Mitel Networks Corporation.

CONTENTS

1 ABOUT THIS DOCUMENT

1.1 PURPOSE OF THIS DOCUMENT

This document describes how to install redundancy on MiVoice 5000 Manager. This mechanism prevents hardware failures on a MiVoice 5000 Manager platform.

1.2 SCOPE

As of R8.0, the operating system Rocky Linux must be installed in order to install the MiVoice 5000 Manager.

Rocky Linux can only be used for a first installation.

When upgrading to R8.x from a version below R8.0, it is necessary to perform an OS upgrade.

Documents referring to the installation of the OS, the application and the update:

- Rocky Linux and Double Attachment
- MiVoice 5000 Server/Manager- Upgrading to R8.0
- MiVoice 5000 Manager – Installation and Configuration
- MiVoice 5000 Manager - User Guide
- Updating OS Security Patch

2 PRINCIPLES OF AND RECOMMENDATIONS ON HOW TO IMPLEMENT REDUNDANCY

Redundancy is a functional security mode based on the use of two servers:

A main (Master) server for nominal operation,

A secondary (Slave) server for resuming the operation if the main server fails (resulting in a switchover from Master to Slave).

Only one virtual address must be defined while installing redundancy, which allows the connected devices to communicate with the active machine only.

The two servers are on the same network (LAN); the redundancy is LAN type redundancy.

The link to these servers' ETHERNET network can be set up either:

- Through **simple attachment**: only one interface is connected by a single cable. In this case, the physical "**eth**" interface of each server is used.
- Through **double attachment**: two interfaces are linked together by two separate cables. In this case, the virtual interface "**bondx**" (bonding mode) is used; this is the only network view which allows a switchover from one physical interface to the other if any of them fails.

Note: The name of these interfaces may vary according to server type (emx instead of ethx, for instance).

Configuration in double attachment is handled in the document "Rocky Linux and Double attachment".

To facilitate the procedure, it is advisable to set each server (main and secondary server) to double attachment. This is the default configuration (factory configuration) of the servers provided by Mitel.

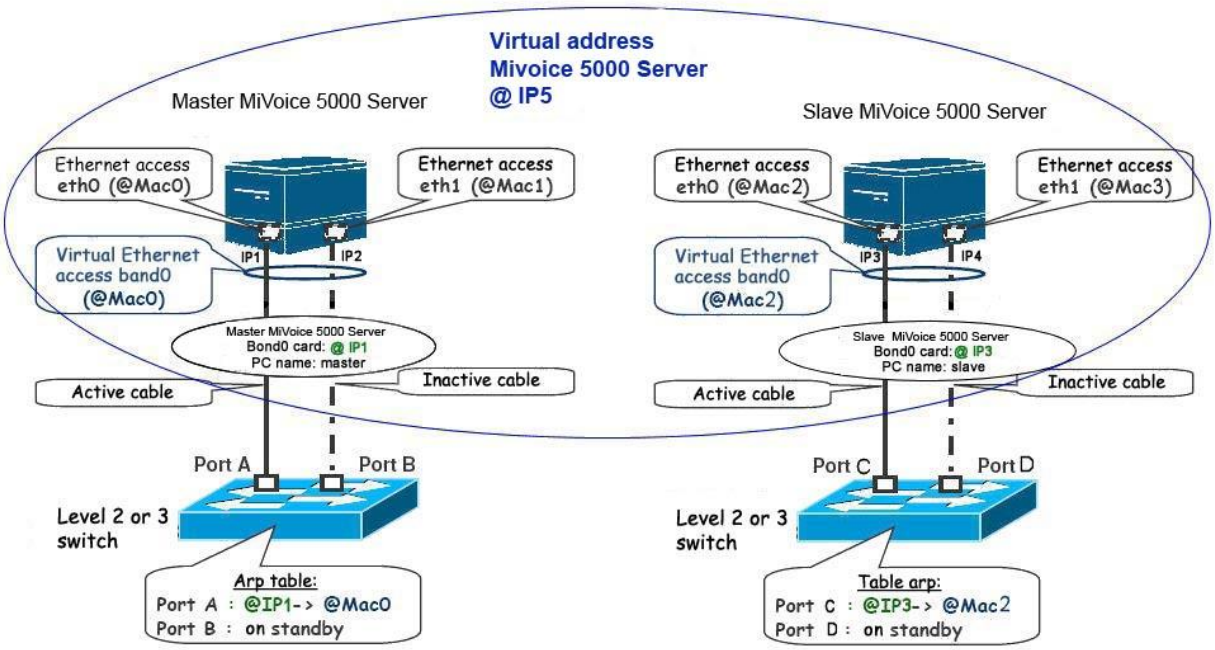
However, the user can work in simple attachment mode by deactivating the virtual interface **bond0** and reconfiguring the **eth0** interface on each server.

In summary, the rules for and order of implementation are:

- In all cases, start by installing the operating system on each server.
- In case of redundancy with double attachment:
  - Double attachment must always be configured first before implementing redundancy.
  - Redundancy must then be installed with the **bond0** interface on each server.
- In case of redundancy without double attachment:
  - Redundancy must be implemented with the **eth0** interface on each server.

Example of environment:

LAN redundancy with double attachment



3 INSTALLING REDUNDANCY

WARNING: Network interface names

In this chapter, the basic or standby Ethernet access will be called ethx. This name must be adapted to the type of server or working mode used:

- **emx for certain types of servers.**
- **bond0 in case of double attachment.**
- **eth0 should therefore be replaced with em1, bond0 or br0 if necessary.**
- **eth1 must be replaced with em2 where necessary.**

Disable boot in the Boot Options menu: Secure Boot > Disabled

In this document, the installation of redundancy will only be described with double attachment; Mitel recommends this configuration to facilitate the procedure.

This is the default configuration (factory configuration) of the servers provided by Mitel.

However, the user can work in simple attachment mode by deactivating the virtual interface **bond0** and reconfiguring the **eth0** interface on each server.

The following configuration is described in this chapter:

- The two MiVoice 5000 Manager PCs are located on the same LAN at the client's.
- Each MiVoice 5000 Manager PC has two Ethernet accesses.
- The virtual IP address used must be on the same subnet as the physical addresses of the two MiVoice 5000 Manager PCs.
- The physical and virtual IP addresses must be fixed.

3.1 PREREQUISITES

Prerequisites on the primary and secondary PCs:

- Configuring double attachment: refer to the document "Rocky Linux and Double Attachment".

3.2 INSTALLING AND CONFIGURING REDUNDANCY ON THE MASTER PC

3.2.1 NAME INPUT AND RESOLUTION ON THE MASTER PC

- Log in as **root** with the password **Mitel5000** on the master PC.
- Type in the command below to give a name to the master PC:

  hostnamectl set-hostname master-manager
- With this command the prompt is used to check the name, by typing in the **hostname** command:

  [root@**master-manager** ~]# hostname
  master-manager
- Go to the **etc.** directory, edit the **hosts** file, add to this file the IP addresses / name of the master and slave MiVoice 5000 as follows:

127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4
192.168.0.100 master-manager
192.168.0.101 slave-manager
::1 localhost localhost.localdomain localhost6 localhost6.localdomain6

Check that the resolution is actually working by typing in the command:

ping master-manager

3.2.2 COLLECTING INFORMATION ON THE MASTER PC

- Type in the **mount** command then check the device name of the partition to be made redundant (/opt/a5000) on the master MiVoice 5000 Server PC: **sda3** (this name may be different depending on the PC).

3.2.3 NAME INPUT AND RESOLUTION ON THE SLAVE PC

- Log in as **root** with the password **Mitel5000 on the slave PC.**
- Type in the command below to give a name to the slave PC: **hostnamectl set-hostname slave-manager**
- As a result of this command the prompt can be used to check the name, by typing in the hostname command:

  [root@**slave-manager** ~]# hostname
  slave-manager
- Go to the **etc.** directory, edit the **hosts** file, add to this file the IP addresses / name of the master and slave MiVoice 5000 as follows:

127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4
192.168.0.100 master-manager
192.168.0.101 slave-manager
::1 localhost localhost.localdomain localhost6 localhost6.localdomain6

Check that the resolution is actually working by typing in the command:

ping slave-manager

3.2.4 COLLECTING INFORMATION ON THE SLAVE PC

- Type in the **mount** command then check the device name of the partition to be made redundant (/opt/a5000) on the slave MiVoice 5000 Server PC: **sda3** (this name may be different depending on the PC).

WARNING: The size of the partition to be made redundant must be the same on the master and slave PCs.

WARNING: The name of the Ethernet interface must be the same on the master and slave PCs.

3.2.5 INSTALLING AND CONFIGURING REDUNDANCY ON THE MASTER PC

- Log in as root to the master PC using the password Mitel5000.
- Mount the application ISO image (see Section 6.1).

Once the iso image is mounted:

- Go to the directory **/mnt/iso/duplication**.
- Run the installation script with the command **./install_redondance.script**

Remove IP address

- PC Master(1) or Slave(0) ?:1
- Master IP address ?:192.168.0.100
- Master Hostname ?: am7450
- Slave IP address ?:192.168.0.101
- Slave Hostname ?:am7450-e
- Virtual IP Address ?:192.168.0.102
- Virtual IP netmask ?:255.255.255.0
- Redundancy: Lan(0) or WAN(1) ? : 0
- Master Ethernet board for redundancy ?:bond0
- Slave Ethernet board for redundancy ?:bond0
- Ethernet board for applications ?:bond0
- Do you want to ping an IP address: 1 (if there is a gateway IP address), or 0 (if there is no gateway IP address)
- IP address to ping: 192.168.0.254 (gateway IP address)
- Master Partition ?:sda4 (this name may be different depending on the PC)
- Slave Partition ?:sda4 (this name may be different depending on the PC)
- Heartbeat deadtime (in seconds)?: 10
- Failback auto = ON/OFF ?:OFF

- After checking the redundancy configuration settings, answer **1** to the question: **do you want to apply these settings: Yes(1) / No(0)**
- Check that the installation is working well:
  - Answer **yes** to the prompt To abort waiting enter ‘yes’.
- Check the synchronisation status on the server:

- Type in the command **drbdsetup setup**.
- The result below must appear:

cs:WFConnection st:Primary/Unknown ds:UpToDate/DUnknown

REDUNDANCY INSTALLATION AND CONFIGURATION ON THE MASTER PC HAS BEEN COMPLETED.

3.2.6 INSTALLING THE MIVOICE 5000 MANAGER APPLICATION ON THE MASTER SERVER

- Log in as root to the master PC using the password Mitel5000.
- Mount the application ISO image (see Section 6.1).
- Go to the root directory and type in the command:

  #./autorun
- Select the installation language according to location; **1** for French, **2** for English, **3** for Dutch, **4** for German and **5** for Italian.
- Go to the **CUSTOM_NAGIOS** directory.
- Type in the command **./install**.
- The installation of NAGIOS then starts.
- Wait till the end of the installation process.

- Remove the CD or DVD:

  #cd
  #umount /mnt/iso

3.2.7 INSTALLING AND CONFIGURING REDUNDANCY ON THE SLAVE PC

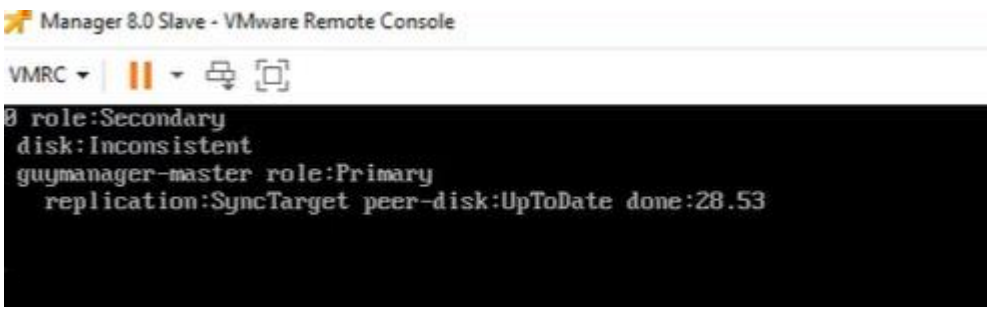
- Log in as root to the slave PC with the password Mitel5000.
- Mount the application ISO image (see Section 6.1).

Once the iso image is mounted:

- Go to the directory **/mnt/iso/duplication**.
- Run the installation script with the command **./install_redondance.script**
  - PC Master(1) or Slave(0) ?:0
  - Master IP address ?:192.168.0.100
  - Master Hostname ?:master-manager
  - Slave IP address ?:192.168.0.101
  - Slave Hostname?:slave-manager
  - Virtual IP Address ?:192.168.0.102
  - Virtual IP netmask ?:255.255.255.0
  - Redundancy: Lan(0) or WAN(1) ? : 0
  - Master Ethernet board for redundancy ?:bond0
  - Slave Ethernet board for redundancy ?:bond0
  - Ethernet board for applications ?:bond0
  - Do you want to ping an IP address: 1 (if there is a gateway IP address), or 0 (if there is no gateway IP address)
  - IP address to ping: 192.168.0.254 (gateway IP address)
  - Master Partition ?:sda3 (this name may be different depending on the PC)
  - Slave Partition ?:sda3 (this name may be different depending on the PC)
  - Heartbeat deadtime (in seconds)?: 10
  - Failback auto = ON/OFF ?: OFF

- After checking the redundancy configuration settings, answer **1** to the question: **do you want to apply these settings: Yes(1) / No(0)**

- Check that the installation is working well:
- Check that the synchronisation operation is working well:



Finally,

```
r0 role:Secondary
  disk:UpToDate
  guymanager-master role:Primary
    peer-disk:UpToDate

Created symlink /etc/systemd/system/multi-user.target.wants/pacemaker.service → /usr/lib/syst

**********
Create symbolic links
**********

[root@guymanager-slave duplication]# _
```

- Check that synchronisation has been completed:
  - Type in the command **drbdsetup status**.
  - The result below must appear:

```
[root@guymanager-slave duplication]# drbdsetup status
r0 role:Secondary
  disk:UpToDate
  guymanager-master role:Primary
    peer-disk:UpToDate

[root@guymanager-slave duplication]#
```

~~cs:Connected st:Secondary/Primary ds:UpToDate/UpToDate~~

```
[root@guymanager-slave duplication]# drbdsetup status
r0 role:Primary
  disk:UpToDate
  guymanager-master role:Secondary
    peer-disk:UpToDate

[root@guymanager-slave duplication]# crm_
```

- Go to the **/ duplication** directory.
- Then run the switch script: **./switch_redondance_7450.script**

- Check that the switchover has been completed successfully:
  - Type in the command **drbdsetup status**.
  - The result below must appear: Secondary is primary

cs:Connected st: Primary/Secondary ds:UpToDate/UpToDate

THE "Primary/Secondary" STATUS IS MANDATORY TO CONTINUE

You can also use the "**crm_mon**" command to check that the switchover to the slave server is effective.

```
Cluster Summary:
  * Stack: corosync
  * Current DC: guymanager-master (version 2.1.0-8.el8-7c3f660707) - partition with quorum
  * Last updated: Tue Feb 15 16:33:30 2022
  * Last change:  Tue Feb 15 16:31:35 2022 by root via crm_resource on guymanager-slave
  * 2 nodes configured
  * 6 resource instances configured

Node List:
  * Online: [ guymanager-master guymanager-slave ]

Active Resources:
  * Clone Set: resource_drbd-clone [resource_drbd] (promotable):
    * Masters: [ guymanager-slave ]
    * Slaves: [ guymanager-master ]
  * Resource Group: group5000:
    * resource_fs       (ocf::heartbeat:Filesystem):     Started guymanager-slave
    * resource_ip       (ocf::heartbeat:IPaddr2):        Started guymanager-slave
  * Clone Set: ping-clone [ping]:
    * Started: [ guymanager-master guymanager-slave ]
```

3.2.8 INSTALLING THE MIVOICE 5000 MANAGER APPLICATION ON THE SLAVE SERVER

- Log in **to the slave PC** as **root** using the password **Mitel5000**.
- Mount the application ISO image (see Section 6.1).

Once the iso image is mounted:

- Go to the root directory and type in the command:

  #./autorun

- Select the installation language according to location; **1** for French, **2** for English, **3** for Dutch, **4** for German, **5** for Italian and **6** for Polish.

- At the end of the installation, press the "**q**" key upon prompt "**PRESS 'q' KEY TO EXIT**".

- Double-click the CD_7450 icon which appears on the desktop.

- Go to the **CUSTOM_NAGIOS** directory of the DVDROM.

  [root@ slave--manager CUSTOM_NAGIOS] #

- Type in the command **./install**.

- The installation of NAGIOS then starts.

- Wait till the end of the installation process.

- Remove the CD or DVD:

  #cd
  #umount /mnt/iso

3.2.9 STARTING MIVOICE 5000 MANAGER REDUNDANCY

3.2.9.1 Starting redundancy on the slave server

- Log in as **root** to the slave PC with the password **Mitel5000.**
- Mount the application ISO image (see Section 6.1).

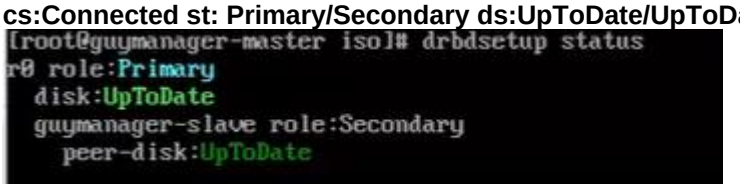
Once the iso image is mounted:

- Go to the directory **/mnt/iso/duplication**.
- Run the start script with the command**./start_redondance.script**

3.2.9.2 Starting redundancy on the master server

- Log in as **root** to the master PC with the password **Mitel5000.**
- Check that the switchover caused by the start of redundancy on the slave PC has been correctly executed:
  - Type in the command **drbdsetup status**.
  - The result below must appear:

cs:Connected st: Primary/Secondary ds:UpToDate/UpToDate



- Go to the **/duplication** directory.
- Run the start script with the command **./start_redondance.script**
- **The master has become Primary again.**

3.3 INSTALLING MIVOICE 5000 MANAGER CLIENT

Refer to the document MiVoice 5000 Manager - Installation and Configuration.

The installation of the redundant MiVoice 5000 Manager has been completed.

3.4 REDUNDANT MIVOICE 5000 MANAGER INSTALLATION TERMINAL

3.4.1 TESTING THE SWITCHES AND CHECKING THE NAGIOS INSTALLATION

- Restart the slave PC.
  Shutdown -r now
- Wait for the slave server to restart. Check that the switchover caused by the slave server restart has been correctly executed:

  On the master PC:

  - Type in the command **drbdsetup status**.
  - The result below must appear:

cs:Connected st: Primary/Secondary ds:UpToDate/UpToDate

- Restart the master PC.
  Shutdown -r now

- Wait for the master server to restart. Check that the switchover caused by the master server restart has been correctly executed:

  On the slave PC:

  - Type in the command **drbdsetup status**.
  - The result below must appear:

  cs:Connected st: Primary/Secondary ds:UpToDate/UpToDate

3.5 DECLARING LICENCES

3.5.1 CHECKING THE STATUS OF LICENCES ON THE MASTER MIVOICE 5000 MANAGER PC

The licence associated with this dongle is obtained from an installation code to be generated during first installation from MiVoice 5000 Manager, in **Menu Administration>Unlock functions**.

This installation code is then used, while logging on to a dedicated server, to generate the actual licence, which will have to be entered in the key field of this same menu.

Note: It is better to use Internet Explorer to access the MiVoice 5000 Manager portal; this will make it easier to copy the values required to generate the licence. See Installation code below.

WARNING: In case of switchover to the slave MiVoice 5000 Manager PC, all the licences, including the redundancy licence, are seen as open on this PC, with a 30 days validity period displayed in the Validity column.

If the master MiVoice 5000 Manager PC is active, the Validity column does not appear on the table indicating the licences.

If the slave MiVoice 5000 Manager PC becomes active after a switchover, the licences are only valid for 30 days. As from D-7, a message is displayed daily in the operations log reminding the administrator that the licences will soon expire.

The message "Operation on secondary server" appears on the welcome page of the slave MiVoice 5000 Manager PC when this latter is active.

The detailed procedure is as follows:

In Menu **Administration>Configuration**, **Settings>General** tab:

- In the **IPv4** field, enter the MiVoice 5000 Manager virtual IP address.

From the master MiVoice 5000 Manager PC:

In Menu **Administration>Unlock functions**:

- Tick the **duplex** box.
- Click **Dongle** (master Key Field).
- In the **Configuration of a virtual dongle** window:
- Enter the Virtual dongle ID (provided by the MiVoice 5000 Manager, example 03FF01XXXXXXXXX).
- Enter the MiVoice 5000 Manager virtual IP address.

- Fill in the Reference ID field corresponding to the dongle ID of any of the iPBXs managed by MiVoice 5000 Manager.

WARNING: All these fields must be filled in.

- Click **Generate code**.
- Click **OK** to confirm the generation.
- The **Installation code** frame indicates the installation code value. Copy this code (to a .txt file for example).
- Click **OK** to close the window.

Switch over to the slave MiVoice 5000 Manager PC:

- On the master MiVoice 5000 Manager PC desktop, double-click the shortcut "**Change to slave"**.

In the menu **Administration>Unlock functions**:

- Click **Dongle** (duplication Key Field).

In the Configuration of a virtual dongle window:

- Enter the **Virtual dongle ID** (provided by the MiVoice 5000 Manager, example 03FF01XXXXXXXXX).
- Enter the MiVoice 5000 Manager **virtual IP address**.
- Fill in the **Reference ID field** corresponding to the dongle ID of any of the iPBXs managed by MiVoice 5000 Manager.

WARNING: All these fields must be filled in.

- Click **Generate code**.
- Click **OK** to confirm the generation.
- The **Installation code** frame indicates the installation code value. Copy this code (to a .txt file for example).
- Click **OK** to close the window.
- Log on to the licence server **https://support.mitel.fr/akop/external.php** then enter these two installation codes.

This server then generates the actual licence for the functions specified during the order and also the redundancy licence.

- Save these licences using the .**txt file export** link.
- Return to the **master** MiVoice 5000 Manager PC:

  On the **slave** MiVoice 5000 Manager PC desktop, double-click the shortcut "**change to master**".
- Return to the same menu **Administration>Unlock functions**.
- Enter the licences needed by the client in the **Master key** field of this same menu, then click **Validate**.

A new frame opens below, showing the unlocked functions.

- Enter the redundancy licence in the **Duplication key** field of this same menu, then click **Validate**.

A new frame opens below, showing the unlocked functions. The functions in question are then authorised, as well as the redundancy function.

It is advisable to store these two licences in a text file.

WARNING: The installation code is changed during each generation, even if no information has been changed (OS, MiVoice 5000 Manager, IP, dongle).

- If in future the characteristics of the IP address and IID number system are modified, the installation code must be regenerated.

Checking the validity of the logical dongle

The following settings are checked periodically:

- MiVoice 5000 Manager ID (dongle number)
- MiVoice 5000 Manager IP address
- MiVoice 5000 Manager MAC address
- Reference ID of an iPBX managed by MiVoice 5000 Manager.

Modifying any of these settings results in immediate expiration of the licence and closes all the functions.

- The Reference ID must correspond to a dongle ID of an (unlocked) iPBX generated by MiVoice 5000 Manager, or else the MiVoice 5000 Manager licence will expire 30 days after the wrong information is detected.
- If the reference ID corresponds but this iPBX is not accessible (off or disconnected from the network), the MiVoice 5000 Manager licence expires 30 days after the absence of the iPBX is detected.

Precautions for use:

- The installation code is unique, and the generated keycode can only work with an installation code.
- If an installation code is generated without obtaining a new keycode, the functions subject to a licence are closed within the next one hour.
- You can manage different cases requiring a change of installation code during the system's service life without first asking Mitel for an authorisation.
- After this change, you will no longer have the right to make any modification, you must contact Mitel to indicate your reasons for this change (user modification, physical replacement of the platform, network modification, etc.).
- After analysing your request, you will again be authorised to modify the installation code.
- During a consultation on the AKOP licence server ("search for a key"), the right to modify the installation code on the identification number concerned is indicated via the following information:
- Modification of installation code **allowed**
- Modification of installation code **not allowed**

- In Menu **Administration>Unlock functions**:
- Enter the new V3.x key associated with the master dongle ID to unlock the client functions, then click **Validate**.
- Enter the new V3.x key associated with the slave dongle ID to unlock the redundancy functions, then click **Validate**.

Note: MiVoice 5000 Manager is working on the master PC.

3.6 CHECKING THAT MIVOICE 5000 MANAGER IS WORKING CORRECTLY

Make the following checks (list not exhaustive):

- Site identification,

- TMA inventories.

3.7 SECURITY PATCHES ON THE MASTER AND SLAVE PCS

Refer to the document **Updating Rocky Linux Security Patches**.

3.8 MODIFYING THE GENERAL REDUNDANCY SETTINGS

If necessary, this procedure applies on an already operational redundant MiVoice 5000 Manager platform; modify one or more redundancy configurations.

This enables the following settings to:

- Change the **Failback** mode configuration
- Change the switchover timeout in case of failure (Heartbeat deadtime)
- Reconfigure redundancy if the IP address and/or name of both PCs changes
- Reconfigure redundancy if the name of the PCs changes
- Modify the virtual IP address and associated subnet mask.

WARNING: The modifications must be made on both machines. The final execution of the redundancy settings modification script on the active PC restarts the server (service interruption) possibly with a switchover to the other PC.

The procedure for this is described below, using as example a modification of **Failback** mode.

3.8.1 MODIFYING REDUNDANCY SETTINGS ON THE MASTER MANAGER PC

Before running the redundancy update script:

- Enter the command:

Run the modification script from the **/duplication**directory.

- Go to the **/duplication** directory.
- Run the redundancy modification script:

  # ./update_redondance.script

The DRBD and Heartbeat software are stopped then restarted at the end of the script, which triggers an automatic return to the master MiVoice 5000 Manager PC if **Failback** mode is set to **ON**.

Each current setting is displayed gradually and can be modified by entering the new value for this setting. The value remains unchanged if the operator presses "Enter".

In the example below, **Failback** mode is set to **ON**.

```
************************
* Update configuration *
************************
Master PC (1) or Slave PC (0)? [1] :
Master IP Address? [10.102.43.123] :
Master Hostname [master] :
Slave IP Address? [10.102.43.124] :
Slave Hostname? [slave] :
Virtual IP address? [10.102.43.125] :
Virtual IP netmask? [24] :
```

WARNING: **Enter the prefix value of the mask. For example, the prefix 24 corresponds to Mask 255.255.255.0. See the section "Mask/prefix conversion" for the table of correspondence.**

```
Do you want a 2nd IP address?: Yes(1) or No(0) ? [0] :
Redundancy: LAN(0) or WAN(1)? [0] :
Master Ethernet board for redundancy? [eth0] :
Slave Ethernet board for redundancy? [eth0] :
Ethernet board for applications? [eth0] :
Do you want to ping an IP address: Yes(1) or No(0) ? [1] :
IP address to ping? [10.102.43.254] :
Master partition? [hda5] :
Slave partition? [hda5] :
Heartbeat deadtime (in seconds)? [10] :
Failback auto = ON/OFF? [OFF] :ON
Stop system log recorder:           [  OK  ]
Start system log recorder :       [  OK  ]
************************
* Stop Heartbeat       *
************************
Stopping High-Availability services: Done.
************************
* Starting DRBD        *
************************
Reloading DRBD configuration: .
************************
* Starting Heartbeat   *
************************
Starting High-Availability services: Done.
Please wait Heartbeat initialization ....
Configuring heartbeat / pacemaker ...
-> Edit CRM config
-> Edit all resources
-> Edit all constraints
```

Note: **Stopping the heartbeat service may take several minutes.**

3.8.2 MODIFYING REDUNDANCY SETTINGS ON THE SLAVE MIVOICE 5000 MANAGER PC

Run the modification script from the **/duplication** directory.

- Go to the **/duplication** directory.
- Run the redundancy modification script:

  # ./update_redondance.script

The software **DRBD** and **Heartbeat** are stopped then restarted at the end of the script, which triggers an automatic return to the master MiVoice 5000 Manager PC if **Failback** mode is set to **ON**.

Each current setting is displayed gradually and can be modified by entering the new value for this settinig. The value remains unchanged if the operator presses "**Enter**".

In the example below, **Failback** mode is set to **ON**.

```
************************
* Update configuration *
************************
Master PC (1) or Slave PC (0)? [0] :
Master IP Address? [10.102.43.123] :
Master Hostname [master] :
Slave IP Address? [10.102.43.124] :
Slave Hostname? [slave] :
Virtual IP address? [10.102.43.125] :
Virtual IP netmask? [24] :
```

WARNING: Enter the prefix value of the mask. For example, the prefix 24 corresponds to Mask 255.255.255.0. See the section “Mask/prefix conversion” for the table of correspondence.

```
Do you want a 2nd IP address?: Yes(1) or No(0) ? [0] :
Redundancy: LAN(0) or WAN(1)? [0] :
Master Ethernet board for redundancy? [eth0] :
Slave Ethernet board for redundancy? [eth0] :
Ethernet board for applications? [eth0] :
Do you want to ping an IP address: Yes(1) or No(0) ? [1] :
IP address to ping? [10.102.43.254] :
Master partition? [hda5] :
Slave partition? [hda5] :
Heartbeat deadtime (in seconds)? [10] :
Failback auto = ON/OFF? [OFF] :ON
Stop system log recorder:           [  OK  ]
Start system log recorder :       [  OK  ]
************************
* Stop Heartbeat       *
************************
Stopping High-Availability services: Done.
```

```
************************
* Starting DRBD        *
************************
Reloading DRBD configuration: .
************************
* Starting Heartbeat   *
************************
Starting High-Availability services: Done.
Please wait Heartbeat initialization ....
Configuring heartbeat / pacemaker ...
-> Edit CRM config
-> Edit all resources
-> Edit all constraints
```

3.8.3 CHECKING THE REDUNDANCY STATUS OF THE MASTER MIVOICE 5000 MANAGER PC

The following checks must be made on the **master** Manager PC:

- Check that **DRBD** synchronisation is up to date: run the command **drbdsetup status**.
- Check the status of the virtual address, using the **ifconfig** command. This latter must be activated.
- Check the mounting of the partition to be made redundant using the **mount** command, which must be implemented on the device **/dev/drbd0**.

3.8.4 REGENERATING THE INSTALLATION CODE AND LICENCE

This phase must be implemented for systems with a virtual (logical) dongle if the virtual IP address has been modified.

See Section 3.5.

3.9 MODIFYING THE PHYSICAL IP ADDRESSES OR HOST NAME OF MIVOICE 5000 MANAGER PCS

This procedure applies, if required, on an already working redundant MiVoice 5000 Manager platform; modify the physical IP addresses or host name of the PCs to adapt them to the client network configuration.

Concerning the modification of the virtual IP address, proceed as described in Section 4.7 - Modifying the general redundancy settings.

Note: To modify the virtual IP address, proceed as described in Section 3.8 Modifying the general redundancy settings.

Modifying the IP settings of the Ethernet access consists in modifying the network interface configuration text files, by entering:

- The IP address
- The Subnet mask
- The Gateway IP address.

The PC hostname is modified in the OS settings.

Before making any modification, first stop the MiVoice 5000 Manager resources (stop heartbeat).

For more information about these operations, see the corresponding section then continue this procedure.

Note: Redundancy stops working after the IP addresses are modified. However, the two PCs must see each other via a "ping".

Once modified, the following settings must be taken into account in the redundancy-settings update procedure described in Section 4.7 - Modifying the General redundancy settings:

- Master IP Address: new IP address of the master PC
- Master hostname: new host name of the master PC
- Slave IP Address: new IP address of the slave PC
- Slave hostname: new host name of the slave PC
- IP address to ping: new test IP address for testing the network status (if used)

If the IP address is modified, the **master** and **slave** licences must be regenerated.

See Section 3.5.

The procedure is now complete.

4 UPGRADING A REDUNDANT MIVOICE 5000 MANAGER

The different types of upgrades concerned in R8.x are:

- Upgrading a configuration from < R8.x to ≥ R8.x (with or without updating the patches)
- Upgrading a configuration from < R8.0 to R8.x (x ≥ 0). In this case, an upgrade is mandatory with full re-installation of the OS. Refer to the document “Rocky Linux and Double Attachment”.

4.1.1 CASE OF UPGRADE REQUIRING A REMOTE ACCESS

When the installer cannot intervene locally on the physical or virtual machines via the graphic interface, it is necessary to set up an SSH session with the master and slave machines.

Any command or execution must then be performed on command lines (Linux).

These are also indicated in the various procedures if necessary.

For a remote access, connection must be via the IP address of the physical machine, and not via the virtual IP address which remains inaccessible.

4.1 UPGRADING A CONFIGURATION FROM R8.X TO ≥ R8.X

This procedure applies, if necessary, on an already operational redundant MiVoice 5000 Manager R8.x platform; upgrade this latter with a new MiVoice 5000 Manager software release > R8.x containing some anomaly corrections or functional upgrades.

The application is upgraded while retaining the installed operating system.

Initial status

- Rocky Linux
- MiVoice 5000 Manager ≥ R8.0
- Active master server

Final status

- Operating system not changed
- MiVoice 5000 Manager R8.x new release in this same range
- Active master server

Security patches:

Depending on the case:

- Not installed in the initial state > Patches must be installed.
- Installed in the initial state but not up to date (a more recent release is available) > Patch upgrade is optional.
- Installed in the initial state and up to date compared to the most up-to-date release available > No patch update.

4.1.1 MAIN PHASES

- Back up the configuration on an external device.
- Check that DRBD synchronisation is working on the **master** PC (command: **drbdsetup status**).
- Check that the redundant partition is active on /dev/drbd0 on the **master** PC (command: **ifconfig** and **mount**.
- Upgrade the **master** MiVoice 5000 Manager PC software.
- Upgrade Nagios Extended Status Map on the **master** MiVoice 5000 Manager PC.
- Switch over to the **slave** MiVoice 5000 Manager PC.
- Check that DRBD synchronisation is working on the slave PC (command: **drbdsetup status**).
- Check that the redundant partition is active on /dev/drbd0 on the slave PC (command: **ifconfig** and **mount**.
- Upgrade the **slave** MiVoice 5000 Manager PC software.
- Upgrade Nagios Extended Status Map on the **slave** MiVoice 5000 Manager PC.
- Return to the **master** PC.
- Install MiVoice 5000 Manager Clients.
- Check the status of licences on the **master** MiVoice 5000 Manager PC.
- Check the status of licences on the **slave** MiVoice 5000 Manager PC.
- Upgrade the operating system security patches (if necessary).

Each phase is described in detail in the sections below.

4.1.2 BACKING UP THE DATA ON MIVOICE 5000 MANAGER SERVER

See in appendix, Section 6.2.

4.1.3 PRELIMINARY CHECKS ON THE MASTER PC (SYNCHRONISATION AND REDUNDANT PARTITION)

Before upgrading the software on the master MiVoice 5000 Manager PC, first perform the following checks:

Check that DRBD synchronisation is working: run the command **drbdsetup status**.

cs:Connected st: Primary/Secondary ds:UpToDate/UpToDate

Check the status of the virtual address, using the **ifconfig** and **mount** commands. This must be active, and the redundant partition moved to device **/dev/drbd0**.

Note: For certain server types, especially HP servers, the server needs to be restarted so the partition /dev/drbd0 on /opt/a5000 is mounted and so synchronisation becomes Primary/Unknown: command **drbdsetup status**.

4.1.4 UPGRADING THE MASTER MIVOICE 5000 MANAGER PC SOFTWARE

- Log in as root to the master PC using the password Mitel5000.
- Mount the application ISO image (see Section 6.1).
- Go to the root directory and type in the command:

  #./autorun
- Select the IP address to be used: **2** (choice corresponding to the virtual IP address).

Go to the **CUSTOM_NAGIOS** directory.

- Type in the following command:

  ./install
- Wait till the end of the installation process.
- Remove the CD or DVD:

  #cd
  #umount /mnt/iso

4.1.5 SWITCHING OVER TO THE SLAVE MIVOICE 5000 MANAGER PC

Before switching over to the slave manager PC, please wait for the supervision data initialisation messages in the operating log:

Waiting for the message "**Successful reset of supervision data**".

This operation consists in activating the virtual address on the slave MiVoice 5000 Manager PC and deactivating the virtual address on the master MiVoice 5000 Manager PC.

On the **master** PC desktop, double-click the shortcut "**Change to slave**".

In SSH Access mode:

On the **master** PC

Go to the **/opt/duplication/files/** tree structure

- Script **./hb_standby**

This operation also restarts the MC service on the **slave** MiVoice 5000 Manager PC if a new service is available.

4.1.6 PRELIMINARY CHECKS ON THE SLAVE PC (SYNCHRONISATION AND REDUNDANT PARTITION)

Before upgrading the software on the **slave** MiVoice 5000 Manager PC, first perform the following checks:

Check that **DRBD** synchronisation is working: run the command **drbdsetup status**

cs:Connected st: Primary/Secondary ds:UpToDate/UpToDate

Check the status of the virtual address, using the **ifconfig** and **mount** commands. This must be active, and the redundant partition moved to device **/dev/drbd0**.

Note: For certain server types, especially HP servers, the server needs to be restarted so the partition /dev/drbd0 on /opt/a5000 is mounted and so synchronisation becomes Primary/Unknown. Command: drbdsetup status.

4.1.7 UPGRADING THE SLAVE MIVOICE 5000 MANAGER PC SOFTWARE

- Log in **to the slave PC** as **root** using the password **Mitel5000**.
- Mount the application ISO image (see Section 6.1).

- Go to the root directory and type in the command:
  #./autorun

- Select the IP address to be used: **2** (choice corresponding to the virtual IP address).

Upgrade NAGIOS on the slave PC.

4.1.8 RETURNING TO THE MASTER PC

On the **master** PC

Go to the **/opt/duplication/files/** tree structure.

Run the script **./ hb_takeover**.

4.1.9 INSTALLING MIVOICE 5000 MANAGER CLIENTS

Refer to the document MiVoice 5000 Manager - Installation and Configuration (Version 11.2 minimum).

4.1.10 ENTERING LICENCES

The licence associated with this dongle is obtained from an installation code to be generated during first installation from MiVoice 5000 Manager, in **Menu Administration>Unlock functions**.

This installation code is then used, while logging on to a dedicated server, to generate the actual licence, which will have to be entered in the key field of this same menu.

Note: It is better to use Internet Explorer to access the MiVoice 5000 Manager portal; this will make it easier to copy the values required to generate the licence. See installation code below.

WARNING: **In case of switchover to the slave MiVoice 5000 Manager PC, all the licences, including the redundancy licence, are seen as open on this PC, with a 30 days validity period displayed in the Validity column.**

If the master MiVoice 5000 Manager PC is active, the Validity column does not appear on the table indicating the licences.

If the slave MiVoice 5000 Manager PC becomes active after a switchover, the licences are only valid for 30 days. As from D-7, a message is displayed daily in the operations log reminding the administrator that the licences will soon expire.

The message "Operation on secondary server" appears on the welcome page of the slave MiVoice 5000 Manager PC when this latter is active.

The detailed procedure is as follows:

From the master MiVoice 5000 Manager PC:

In Menu **Administration>Unlock functions**:

- Check that the **duplex** box has been ticked.
- Click **Dongle** (master Key Field).

In the **Configuration of a virtual dongle** window:

- Check the Virtual dongle ID (provided by MiVoice 5000 Manager, example 03FF01XXXXXXXXX).
- Check the MiVoice 5000 Manager virtual IP address.
- Fill in the reference ID field corresponding to the dongle ID of any of the iPBXs managed by MiVoice 5000 Manager.

WARNING: **All these fields must be filled in.**

- Click **Generate code**.
- Click **OK** to confirm the generation.
- The **Installation code** frame indicates the installation code value. Copy this code (to a .txt file for example).
- Click **OK** to close the window.

Switch over to the slave MiVoice 5000 Manager PC:

- On the **master** MiVoice 5000 Manager PC desktop, double-click the shortcut "**Change to slave"**.

In the menu **Administration>Unlock functions**:

- Click **Dongle** (duplication Key Field).
- Check the Virtual dongle ID (provided by MiVoice 5000 Manager, example 03FF01XXXXXXXXX).
- Check the MiVoice 5000 Manager virtual IP address.
- Fill in the reference ID field corresponding to the dongle ID of any of the iPBXs managed by MiVoice 5000 Manager.

WARNING: **All these fields must be filled in.**

- Click **Generate code**.
- Click **OK** to confirm the generation.
- The **Installation code** frame indicates the installation code value. Copy this code (to a .txt file for example).
- Click **OK** to close the window.

- Log on to the licence server **https://support.mitel.fr/akop/external.php** then enter these two installation codes.

This server then generates the actual licence for the functions specified during the order and also the redundancy licence.

- Save these licences using the .**txt file export** link.

Return to the **master** MiVoice 5000 Manager PC:

- On the **slave** MiVoice 5000 Manager PC desktop, double-click the shortcut "**Change to master**".
- Return to the same menu **Administration>Unlock functions**.
- Delete the previous licence in the **Master key** field.
- Enter the licences needed by the client in the **Master key** field of this same menu, then click **Validate**.

A new frame opens below, showing the unlocked functions.

- Delete the previous licence in the **Duplication key** field.
- Enter the redundancy licence in the **Duplication key** field of this same menu, then click **Validate**.

A new frame opens below, showing the unlocked functions. The functions in question are then authorised, as well as the redundancy function.

It is advisable to store these two licences in a text file.

WARNING: The installation code is changed during each generation, even if no information has been changed (OS, MiVoice 5000 Manager, IP, dongle).

- If in future the characteristics of the IP address and IID number system are modified, the installation code must be regenerated.

Checking the validity of the logical dongle

The following settings are checked periodically:

- MiVoice 5000 Manager ID (dongle number)
- MiVoice 5000 Manager IP address
- MiVoice 5000 Manager MAC address
- Reference ID of an iPBX managed by MiVoice 5000 Manager.

Modifying any of these settings results in immediate expiration of the licence and closes all the functions.

- The Reference ID must correspond to a dongle ID of an (unlocked) iPBX generated by MiVoice 5000 Manager, or else the MiVoice 5000 Manager licence will expire 30 days after the wrong information is detected.
- If the reference ID matches but this iPBX is not accessible (off or disconnected from the network), the MiVoice 5000 Manager licence expires 30 days after the absence of the iPBX is detected.

Precautions for use

- The installation code is unique, and the generated keycode can only work with an installation code.
- If an installation code is generated without obtaining a new keycode, the functions subject to a licence are closed within the next one hour.
- You can manage different cases requiring a change of installation code during the system's service life without first asking Mitel for an authorisation.
- After this change, you will no longer have the right to make any modification, you must contact Mitel to indicate your reasons for this change (user modification, physical replacement of the platform, network modification, etc.).
- After analysing your request, you will again be authorised to modify the installation code.

- During a consultation on the AKOP licence server ("search for a key"), the right to modify the installation code on the identification number concerned is indicated via the following information:
- Modification of installation code **allowed**
- Modification of installation code **not allowed**

4.1.11 UPDATING THE OPERATING SYSTEM SECURITY PATCHES

Depending on the case:

- Not installed in the initial status > Patches must be installed with the most recent version.
- Installed in the initial status but not up to date (a more recent release is available on MITEL Extranet) > Patch upgrade is optional.
- Installed in the initial status and up to date compared to the most up-to-date release available > No patch update.

If new patches have been provided on the Extranet, update the security patches, starting with the (active) master PC.

Refer to the document **Updating Rocky Linux Security Patches** for the range concerned.

The upgrade process has been completed:

5 REINSTALLING A REDUNDANT SYSTEM

5.1 REINSTALLING THE SLAVE SERVER

Back up the MiVoice 5000 Manager configuration data.

Disconnect the SLAVE server from the network.

Install the Rocky Linux OS.

Install MV5000 redundancy:

- ./install_redondance.script
- In master mode
- No ping

Install MV5000 Server.

Start redundancy:

- ./start_redondance.script

Update redundancy:

- ./update_redondance.script
- In this script, return to slave mode.
- Enable pinging if needed.

Stop redundancy:

- pcs cluster stop --force

Reset DRBD:

- drbdadm create-md r0
- drbdadm invalidate r0

Reconnect the network.

Start redundancy:

- pcs cluster start

Check the DRBD synchronisation with the command **drbdsetup status**.

Check that duplication is working, with crm_mon.

Finalisation

- Once synchronisation is completed, switch to the slave server.
- Generate the new installation code and enter the licence.
- Return to the master.

5.2 REINSTALLING THE MASTER SERVER

Back up the MiVoice 5000 Manager configuration data.

Disconnect the MASTER server from the network.

Install the Rocky Linux OS.

Install MV5000 redundancy:

- ./install_redondance.script
- No ping
- Install MV5000 Server.

Start redundancy:

- ./start_redondance.script

Update redundancy (optional):

- ./Update_redondance.script (to enable pinging if needed)

Stop redundancy:

- pcs cluster stop --force

Reset DRBD:

- drbdadm create-md r0
- drbdadm invalidate r0

Reconnect the network.

Start redundancy.

- pcs cluster start

Check the DRBD synchronisation with the command **drbdsetup status**.

Check that duplication is working, with crm_mon.

Finalisation

Once synchronisation is completed, switch to the master server:

On the **slave** PC, perform a **switchover to master:**

Go to the **/opt/duplication/files/** tree structure

Script **./hb_standby**

Generate the new installation code and enter the licence.

6 APPENDICES

6.1 MOUNTING AN ISO IMAGE

The mounting point must exist.

- Type in the following commands:

  mkdir /mnt/iso

- Copy iso to /tmp

  mount /tmp/CD** /mnt/iso**

6.2 BACKING UP THE DATA ON MIVOICE 5000 MANAGER SERVER

You must back up the following data:

- MiVoice 5000 Manager configuration data, including LDAP database configuration data
- The pictures.

Backing up the MiVoice 5000 Manager configuration

The different methods for creating the backup are:

- From the MiVoice 5000 Manager portal, use Choice **to start backing up the application. Click here** in Menu **Administration** (from a client terminal: https://@ipmanager).
- Use daily backup available in **/home/m7450/backup** (the most recent one).

The backups are stored in the directory **/home/m7450/backup** (see below for the content).

Backing up pictures

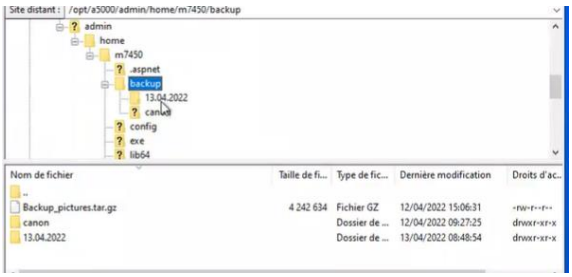
Run the script: **backupPictures.sh**.

The backups are stored in the directory **/home/m7450/backup** (see below for the content).

Then transfer this data to the (internal or external) location in question (e.g. USB).

Recommendation:

Group the backups in the same directory **(/home/m7450/backup**) to make it easier to restore the data later.



In the case of a backup on a USB key, at the end of the procedure, dismount the volume and remove the USB key from the active (master) machine.

Content of the backup directory

The last 31 backups are stored on MiVoice 5000 Manager Server, in the directory "**/home/m7450/backup**". Each backup is identified by its date.

By default, the backups are kept for 30 days. This period can be reduced if necessary by modifying the file **/home/m7450/portal.dll.config**.

- Modify the line

<add key="DELAI_SAVE_M7450" value="30"/> (the value must be between 3 and 30).

Recovering the backups

To recover the backups:

From the portal administration window, click the link proposed in the option "**To recover MiVoice 5000 Manager application backups, click here**".

For a given date, the backup files are:

config.tar.gz : configuration files -> directories /home/m7450/automate, /home/m7450/portal, var/www/M7450 and /var/www/webmanagement/data

m7450.out: application data (psql database)

repository1.tar.gz : Directory /home/m7450/repository/system

repository2.tar.gz: Directories /home/m7450/repository/pabxdata (excluding iPBX backup) and home/m7450/repository/Users

repository3.tar.gz: Directory /home/m7450/repository/pabxdata (excluding iPBX backup)

repository4.tar.gz: Directory /home/m7450/repository/pabxconfig (except alarms and Inventory)

repository5.tar.gz: Directory /home/m7450/repository/pabxdata (iPBX backup)

backup_conf_ldap.tar.gz & ldap_file.ldiff: AM7450 LDAP backup

backup_nagios.tar.gz: Nagios configuration file backup

selfadmin.tar.gz: User Portal application data backup

syncAd.tar.gz: External synchronisation backup

tma.tar.gz: TMA data backup

webdata.tar.gz: back up of links to Mitel applications

6.3 RESTORING THE DATA ON MIVOICE 5000 MANAGER SERVER

The data is restored by running the following scripts from the server (order to be respected):

- Script for LDAP database configuration
- Script for restoring the MiVoice 5000 Manager configuration (with or without iPBX backups)
- Script for restoring pictures.

Procedure:

- Log in as **root**.
- Select the directory **/home/scripts_m7450**.

To restore LDAP data

- Log in as **root** (otherwise the LDAP database will not be restored).
- Select the directory **/home/scripts_m7450**.
- In the terminal window, type in the command **restaure_ldap.sh**, followed by the setting **dd.mm.yyyy**, representing the date of the backup to be restored (input control). Example: "**#. /restaure_ldap.sh 24.06.2013**".

IMPORTANT : In a multi-site configuration with a directory replica, the replica must be recreated after the restore operation (refer to the MiVoice 5000 Manager User Guide).

To restore the MiVoice 5000 Manager configuration:

- Run the command **su - m7450**.

For standard restore without iPBX backups:

- In the terminal window, type in the command **restaure.sh**, followed by the setting **dd.mm.yyyy**, representing the date of the backup to be restored (input control).

Example: "**#. /restore.sh 24.12.2007**"

The duration of the restore process depends on the size of the configuration.

For a restore operation with iPBX backups:

- In the terminal window, type in the command **restore.sh -total** followed by the parameter **dd.mm.yyyy**, representing the date of the backup to be restored (input control). Example: "**#. /restaure.sh -total24.12.2007**".

The duration of the restore process depends on the size of the configuration.

Note : The restore script stops the portal automatically. During the operation, the script enumerates the files and data restored.

Restoring pictures:

- Log in as **root**.
- Select the directory **/home/scripts_m7450**.
- In the terminal window, enter the command: **#./restaurePictures.sh**
- Enter the backup directory name: **/home/m7450/backup**
- Enter the picture file name without extension: **pictures**.

After the restore operations, restart MiVoice 5000 Manager: # **service m7450 start**

6.4 DISABLING HEARTBEAT

It is necessary to first temporarily disable the MiVoice 5000 Manager resources. This will possibly move the resources to another PC.

Upon prompt, type in the following command:

 # pcs cluster stop

Note: Stopping the heartbeat service may take several minutes.

6.5 CONFIGURING THE FIREWALL

If the firewall is activated, the following ports must be open on each machine:

- TCP Port 7788: DRBD
- UDP Port 5405: Corosync

6.6 MASK/ADDRESS PREFIX CONVERSION

Netmask	Address Prefix Length
255.255.255.255	/32
255.255.255.254	/31
255.255.255.252	/30
255.255.255.248	/29
255.255.255.240	/28
255.255.255.224	/27
255.255.255.192	/26
255.255.255.128	/25
255.255.255.0	/24 (Class C)
255.255.254.0	/23
255.255.252.0	/22
255.255.248.0	/21
255.255.240.0	/20
255.255.224.0	/19
255.255.192.0	/18
255.255.128.0	/17
255.255.0.0	/16 (Class B)
255.254.0.0	/15
255.252.0.0	/14
255.248.0.0	/13
255.240.0.0	/12
255.224.0.0	/11
255.192.0.0	/10
255.128.0.0	/9
255.0.0.0	/8 (Class A)
254.0.0.0	/7
252.0.0.0	/6
248.0.0.0	/5
240.0.0.0	/4
224.0.0.0	/3
192.0.0.0	/2
128.0.0.0	/1
0.0.0.0	/0 (The Internet)