



A MITEL
PRODUCT
GUIDE

MiVoice MX-ONE

Upgrade Process Minimizing System Downtime

Release 7.6

165/1531-ANF 901 14 Uen F 2023-12-21

December 2023

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by **Mitel Networks Corporation (MITEL®)**. 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), its affiliates, parents, or subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: <http://www.mitel.com/trademarks>.

®,™ Trademark of Mitel Networks Corporation

© Copyright 2023, Mitel Networks Corporation

All rights reserved

Contents

1 Introduction.....	1
2 Benefits.....	2
3 Requirements.....	3
3.1 MX-ONE Running On Virtualized Environment.....	3
3.2 MX-ONE Running On Standard (Bare Metal) Environment.....	4
3.3 Network Definitions.....	4
4 Setup.....	6
4.1 Virtualized.....	6
4.1.1 Setting up a Network Using VMware.....	6
4.1.2 Deploy MiVoice MX-ONE OVA.....	9
4.1.3 Setting up Microsoft Hyper-V® for MiVoice MX-ONE.....	14
4.2 Standard Infrastructure.....	22
4.2.1 Network Setup.....	22
4.2.2 Deploy MiVoice MX-ONE.....	22
4.3 PC-Regen.....	23
4.3.1 Collecting the Current Data.....	23
4.3.2 Send the Data to the New System.....	24
4.3.3 Media Gateway and Media Server Setup.....	25
4.4 Migrating Provisioning Manager and Service Node Manager.....	26
4.4.1 Backup Service Node Manager (Manager Telephony Server in MX-one 5.0).....	26
4.4.2 Backup Provisioning Manager (Manager Provisioning in MX-ONE 5.0).....	27
4.4.3 Restore Service Node Manager.....	28
4.4.4 Restore Provisioning Manager.....	28
4.4.5 Verify Provisioning Manager and Service Node Manager setup.....	30
4.5 Migration Process.....	42
4.5.1 Migration Part 1.....	43
4.5.2 Migration Part 2.....	44
4.6 Final Verification.....	47

MiVoice MX-ONE (MX-ONE) is a communication system that runs on Linux operating system.

MX-ONE is composed by Service Node (a Communication Server) and Media Gateways or Media Server.

The main component of MX-ONE is Service Node, which runs on a Linux distribution called SUSE Linux Enterprise Server (SLES).

Operating System is often updated to add new functionality, fix faults, and security vulnerabilities.

Mitel is committed to deliver package updates with new Operating System version to MX-ONE as soon as they are available in the market.

Because of the technology evolution, the market is often introduced with a new operating system and requires a new installation process for that. For example, moving from 32 to 64 bits machines. Sometimes, the new operating system contains different types of kernel structures that requires a new installation to get benefit from the new improvements that kernel provides/requires. So, this is a challenge that an open platform as Linux adds to the overall system solution.

Additionally, the MX-ONE software is often updated which also requires upgrade. Sometimes the upgrade takes more time and customers cannot afford to have downtime for more than a couple of minutes due to critical service offered by MX-ONE. Likely, there are technologies available in the market that helps a partner/customer to make upgrade faster and more frequent.

The primary aim of this document is to explain how an upgrade/new installation of a MX-ONE system can be done via VMware (virtualized systems) or Hardware Simulator (standard physical servers, sometimes called Bare Metal).

In summary, the goal of the document is mentioned as follows:

- Explaining the straight forward procedure for existing customers with an MX-ONE 5.x or 6.x virtualized system migrate to MX-ONE 7.X with significantly reduced the downtime.
- Explaining about the same procedure that could also be a way to move an existing MX-ONE 5.x or 6.x customer system from a “bare metal” server environment to a new hardware (bare metal) or virtualized environment with MX-ONE 7.X.
- Explaining about the same procedure that could also be used by large systems running MX-ONE 7.X to upgrade the system to a recent MX-ONE 7.X version.

The process described in this document has the following benefits for a partner/customer.

Re-use of the existing virtualization data center environment tools.

- Virtually the same process for migration from a standard physical server environment to a Private cloud (virtualized) environment.
- Prepare the “time intensive” parts (Installation, configuration) offline during normal office hours.
- Pre-test features in new system in the “migration” network environment without affecting live traffic.
- Actual “cut-over” downtime reduced to an hour of less in most cases.
- Can be done by your Channel partner or through Mitel Professional services.

This chapter contains the following sections:

- [MX-ONE Running On Virtualized Environment](#)
- [MX-ONE Running On Standard \(Bare Metal\) Environment](#)
- [Network Definitions](#)

MX-ONE should run a previous version, for example, MX-ONE 5.0 SP1 or MX-ONE 6.X.

The MiVoice MX-ONE system is composed by the following main components:

- Service Node
- Media Gateway Unit (MGU) / Media Server
- Service Node Manager
- Provisioning Manager

The minimum requirements are:

From that system, all information needs to be collected and backup.

- Backup of all systems (Service Node, Provisioning Manager, Service Node Manager, Media Server, MGUs, and so on)
- PC-Regen of the system

New software available (Service Node, Provisioning Manager, Service Node Manager, Media Server, MGUs, and so on).

- VMware infrastructure for virtualized systems
- Extra Hardware for the standard systems
- Licenses

3.1 MX-ONE Running On Virtualized Environment

MiVoice MX-ONE is validated to work in VMware environment. To prepare the new MX-ONE system, the following material VMware software is required.

- vSphere 8.0 infrastructure with vCenter, vMotion, and VMware tools
- Minimum 3 networks in the virtualized environment
- Enough capacity to create additional Virtual Machines
- PC or a PC VM to be used to collect the PC-Regen data as well as access the system

For more information regarding MX-ONE virtualized, check the *MX-ONE CPI* documentation.

3.2 MX-ONE Running On Standard (Bare Metal) Environment

A system running in a standard physical server can also be updated following the procedure that is described in the next chapters; however, the requirements are different. The following are required:

Servers or a MX-ONE hardware chassis with ASU-II cards

Switch/switches

PC to be used to collect the PC-Regen data as well as access the system

For more information regarding MX-ONE standard, check the *MX-ONE CPI* documentation.

3.3 Network Definitions

The VMware environment will require 3 networks to create the new system.

The standard physical server environment requires 2 or 3 network segments and VLANs can be used to achieve it.

The networks definitions are:

- Network 1 (Production), the existing Production network where the current MX-ONE system is running and it is connected to the rest of customer network.

Note:

This could be an existing bare metal centralized system that should be on its own “subnet” connected to the rest of the customer network.

- Network 2 (Migration), the migration is the network used to create the new MX-ONE that needs to provide the same characteristics as the Production (same IP addresses, Default Gateway, etc.). However, this network needs to be completely isolated during the preparation/test phase.
- After migration, this essentially replaces the existing Production network. If the current Production Network has several subnets where servers are placed in, this network also need to have same routing setup between the involved subnet's. This requires a special VLAN set in the switches, that are replicated in the VMware network setup for Network 2 (Migration).
- Network 3 (Shadow), which is used to move the original MX-ONE system, as phase 1 of the migration. It is a completely isolated from the customer network. That network is used to avoid duplicated IPs when migrating the Service Nodes.

i Note:

If it is a physical server environment network, the new MX-ONE server's subnet needs to be separated/disconnected from the rest of the network. The new system needs to be kept running "offline", but isolated from the Production network. In this case, the Shadow network is not mandatory; because, the cables are moved in the switch/switches. So, if the cables are moved in three steps and they are placed in the correct ports, there is no risk for duplicate IP addresses.

The three steps cables migration process is the following:

1. Disconnect the Ethernet cables from original MX-ONE from the Production network switch.
2. Move the Ethernet cables from the new MX-ONE system to Production network switch.
3. Move the original MX-ONE system to the Migration network switch.

This chapter contains the following sections:

- [Virtualized](#)
- [Standard Infrastructure](#)
- [PC-Regen](#)
- [Migrating Provisioning Manager and Service Node Manager](#)
- [Migration Process](#)
- [Final Verification](#)

4.1 Virtualized

The VMware infrastructure should be in place. The main activities are:

- Creation of the two new networks: Migration and Shadow
- Deployment of MiVoice MX-ONE OVAs

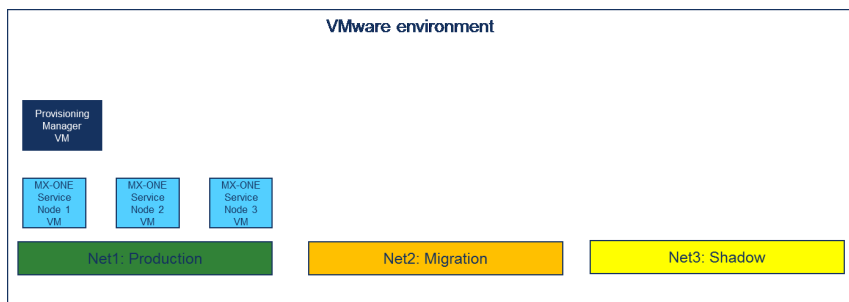
4.1.1 Setting up a Network Using VMware

This section provides network setup information related to VMware and Hyper Virtualized environments.

In the VMware® infrastructure, the Migration and Shadow networks need to be created, if you have a need for several subnets, then you might have to involve the administrator of the network.

The multi subnet is not covered, but it has the same principles to add more network elements as shown in the below figure. Contact your VMware administrator to create the networks.

Figure 1: Virtualized Environment Before Upgrade

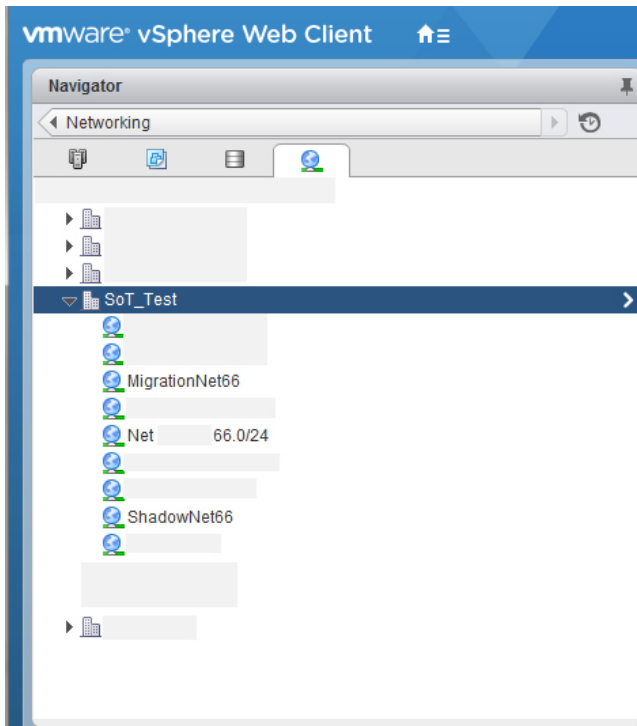


Below figure shows the VMware network setup screen for the following networks:

- NetXXXX66 is the Production network
- MigrationNet66 is the Migration network

- ShadowNet66 is the Shadow network

Figure 2: VMware Network Setup Example



Installing Microsoft Hyper-V®

To install a Hyper-V machine make sure your system meets the following requirements:

- Installed Windows Server 2008, 2012, or 2016
- Have a Windows License (no other special licenses needed)
- Runs on a Dell and HP server
- Have .vhd and .vhdx format image for installation

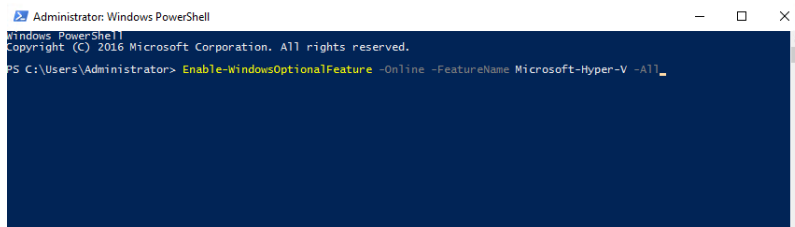
You can install Hyper-V using a PowerShell or in a GUI. To enable Hyper-V using a power shell:

1. Open a PowerShell console as Administrator.

2. You can do either of the following:

- Run the following command: `Enable-WindowsOptionalFeature -Online -FeatureName Microsoft-Hyper-V -All`

Figure 3: Windows PowerShell



- Open **Server Manager** and select **Server Roles** to add role and features and install Hyper-V.

Figure 4: Server Manager - Configure Local Server

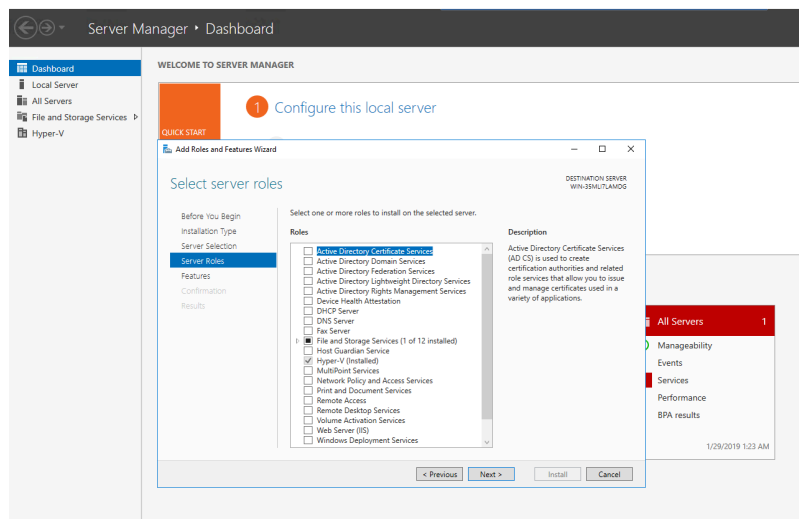


Figure 5: Adding roles to Hyper-V

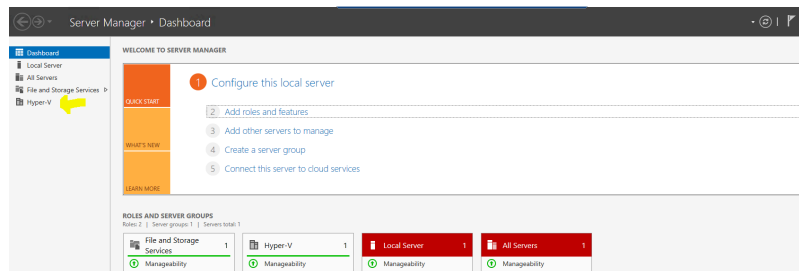
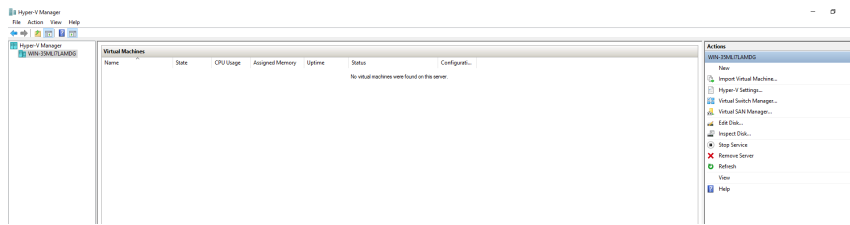


Figure 6: Microsoft Hyper-V



4.1.2 Deploy MiVoice MX-ONE OVA

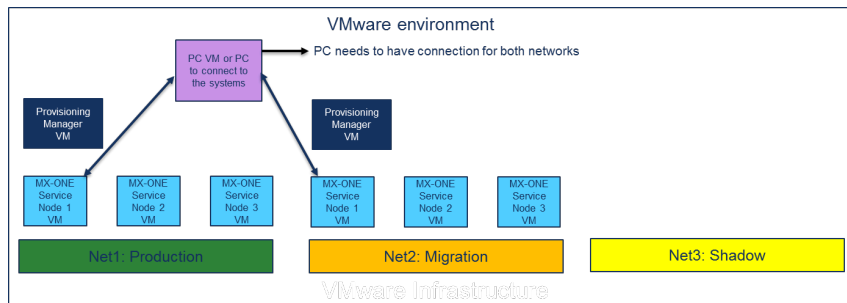
To deploy MiVoice MX-ONE OVA, do the following:

1. Create the number of Service Node / Media Server standalone Virtual Machines required based on size of the current MX-ONE system.
2. Consider consolidation of server/Media Gateways to reduce server footprint. The below figure shows the built of new system.

Note:

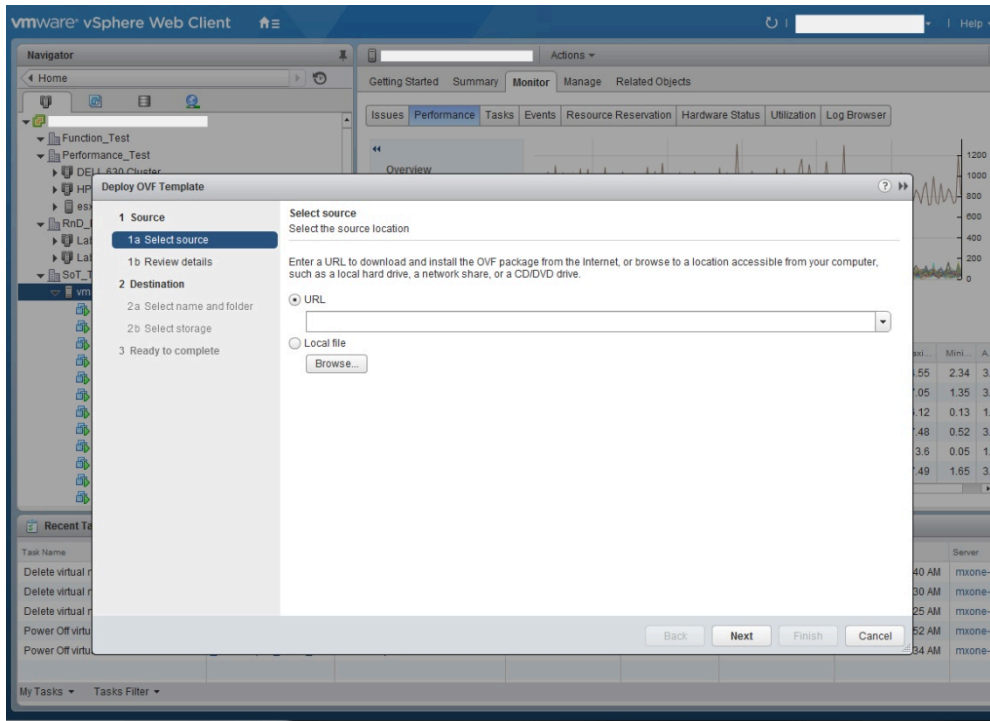
A PC is required to connect to the systems that are having access to both Production and Migration network.

Figure 7: Virtualized Environment After Deploy of New System



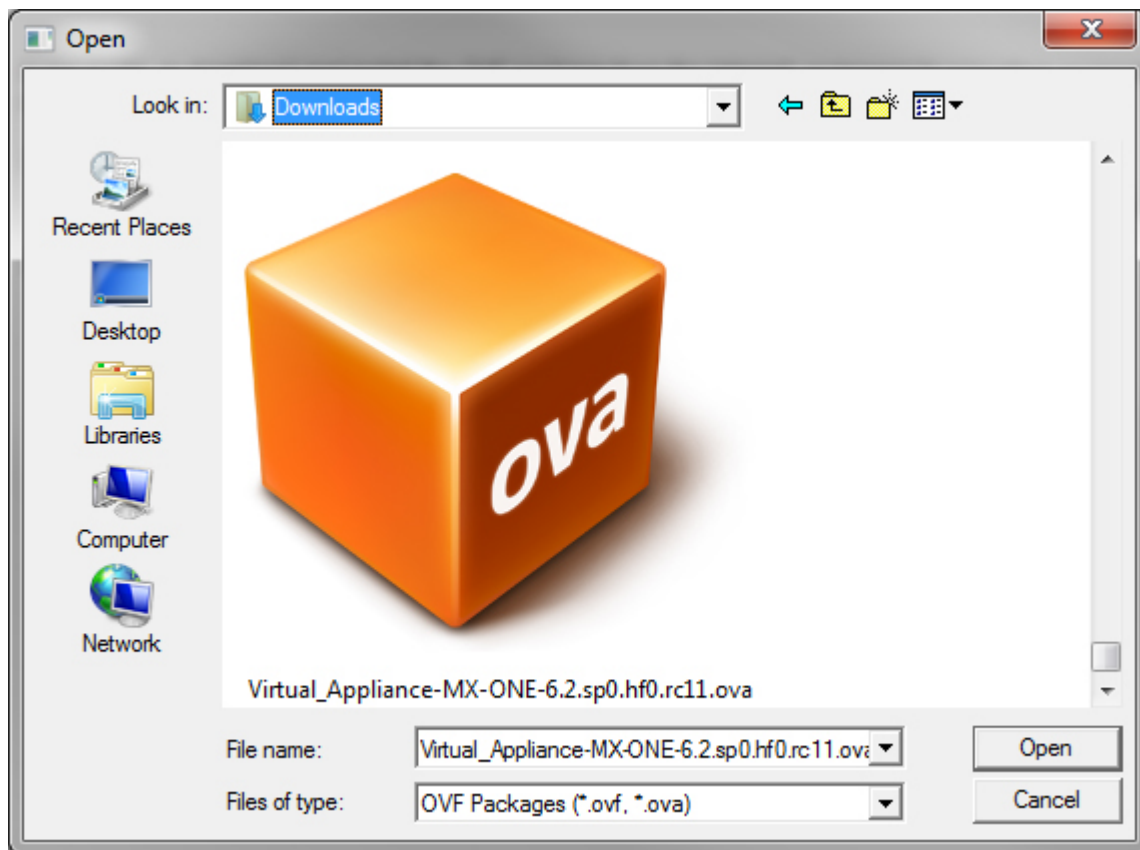
3. Install the new MX-ONE system. The Service Node is installed in the Migration network.

Figure 8: Deploying a New MX-ONE OVA



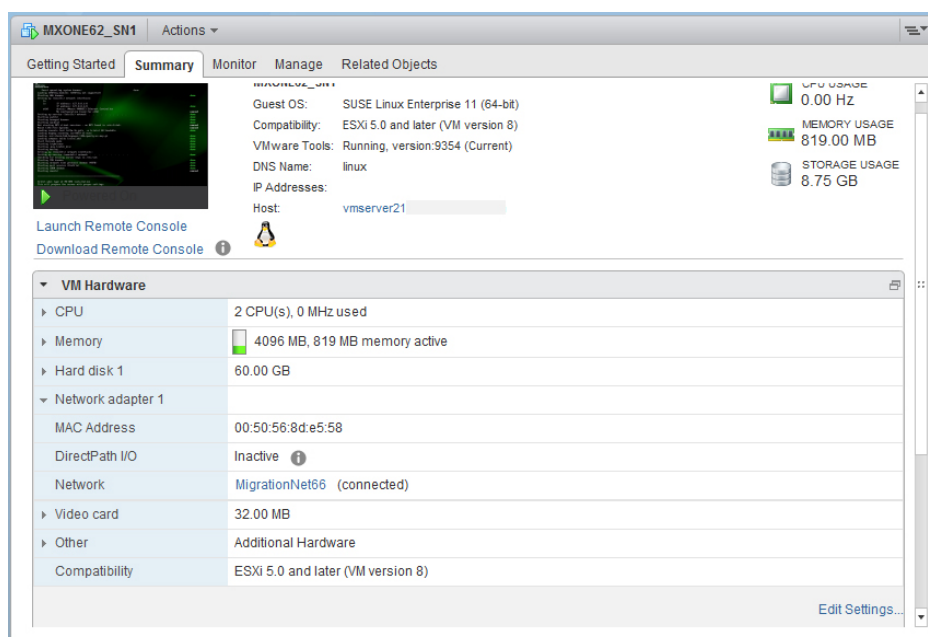
4. Select the OVA file.

Figure 9: Selecting the OVA



5. Check if the Service Node is in the Migration network as soon the deployment is done. In the example, the MigrationNet66 is used.

Figure 10: Verification of the MX-ONE VM setup



6. Deploy the OVA for the number of Service Nodes required.
7. Adjust the VMs resources (vCPU, memory, disk, and so on) according to the MX-ONE virtualization guidelines. As an example, in this document the process is done 4 times, 3 for Service Nodes and 1 for Provisioning Manager standalone.

Note:

MX-ONE requires access to Default Gateway during the installation process.

If the MX-ONE system network consists of only one subnet, a VM PC (it might be the same PC used to setup the system) can be used to simulate the Default Gateway. So, it can be placed in the Migration network with the IP address of the default gateway (DG).

Otherwise, the VMware Administrator needs to setup a valid Default Gateway in the Migration network.

Service Node setup gets fail if it cannot reach the DG by these two ways, because when setup the Service Node network, it tries to PING the default gateway. If the PC is set with the DG IP address, or the network answer, Service Node receives an answer that the operation is succeeded.

For example, default Gateway is 192.168.66.1, the VM PC is configured with this IP.

8. Access the Service Nodes and setup them according to the documentation.

Figure 11: MX-ONE Service Node Installation Screen

```

MXONE62_SN1 - VMware Remote Console
VMRC
SUSE Linux Enterprise Server
lo
lo IP address: 127.0.0.1/8
eth0 device: VMware VMXNET3 Ethernet Controller
No configuration found for eth0
Setting up service (localfs) network . . . . . done
Starting auditd done
Starting haveged daemon done
Starting rpcbind done
Not starting NFS client services - no NFS found in /etc/fstab: unused
Mount CIFS File Systems unused
Loading console font lat9u-16.psfu -m trivial G0:loadable done
Loading keymap assuming iso-8859-15 euro done
Loading /usr/share/kbd/keymaps/1586/quarter/us.map.gz done
Loading compose table latin1.add done
Start Unicode mode done
Starting irqbalance done
Starting java.binfmt_misc done
Starting mcelog... done
Setting up (remotefs) network interfaces: done
Setting up service (remotefs) network . . . . . done
Checking for missing server keys in /etc/ssh done
Starting SSH daemon done
Starting network time protocol daemon (NTPD) done
Starting mail service (Postfix) done
Starting CRON daemon done
Starting smartd unused

=====
Select what type of MX-ONE installation
This will prepare the server with proper settings

1 MiVoice MX-ONE
2 MiVoice MX-ONE Express (PM will be installed)
3 MiVoice MX-ONE SaaS (PM will be installed)

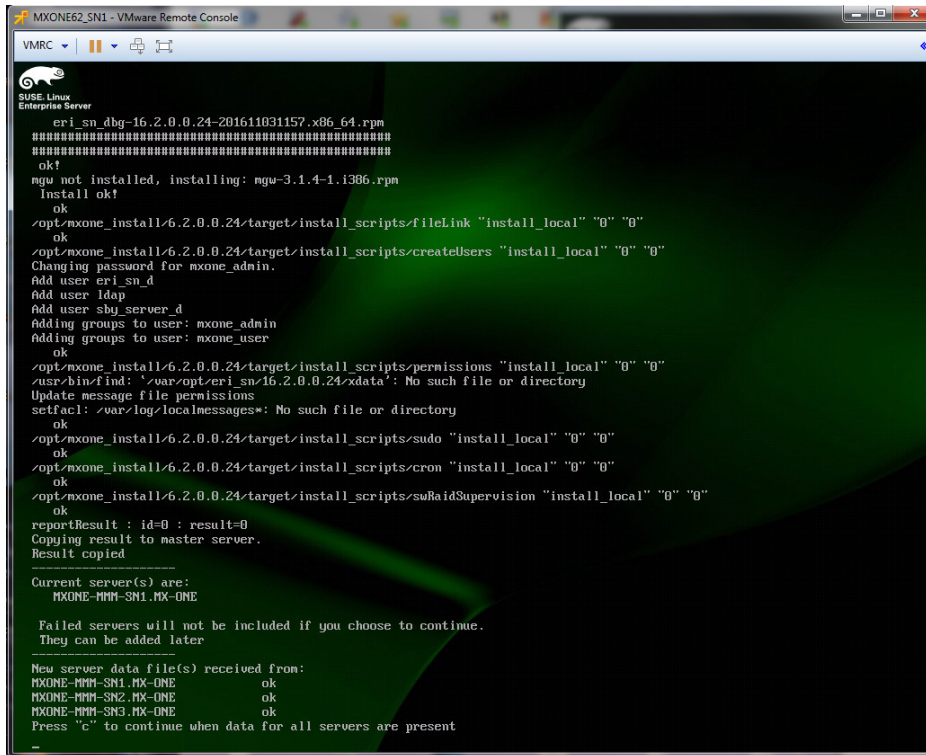
=====
Select type of install 1-3

Selection
Only digits is allowed (1-3).
Select type of install 1-3

```


9. When all the Service Nodes are setup, the following screen is displayed.

Figure 12: MX-ONE Service Node installation screen (3 Service Nodes)



```

MXONE62 SN1 - VMware Remote Console
VMRC
SUSE Linux
Enterprise Server

erl_sn_dbg-16.2.0.0-24-201611031157.x86_64.rpm
#####
ok!
mgw not installed, installing: mgw-3.1.4-1.1306.rpm
Install ok!
ok
/opt/mxone_install/6.2.0.0-24/target/install_scripts/fileLink "install_local" "0" "0"
ok
/opt/mxone_install/6.2.0.0-24/target/install_scripts/createUsers "install_local" "0" "0"
Changing password for mxone_admin.
Add user erl_sn_d
Add user ldap
Add user shy_server_d
Adding groups to user: mxone_admin
Adding groups to user: mxone_user
ok
/opt/mxone_install/6.2.0.0-24/target/install_scripts/permissions "install_local" "0" "0"
/usr/bin/find: '/var/opt/erl_sn/16.2.0.0-24/xdata': No such file or directory
Update message file permissions
setfacl: /var/log/localmessages*: No such file or directory
ok
/opt/mxone_install/6.2.0.0-24/target/install_scripts/sudo "install_local" "0" "0"
ok
/opt/mxone_install/6.2.0.0-24/target/install_scripts/cron "install_local" "0" "0"
ok
/opt/mxone_install/6.2.0.0-24/target/install_scripts/swRaidSupervision "install_local" "0" "0"
ok
reportResult : id=0 : result=0
Copying result to master server.
Result copied

Current server(s) are:
MXONE-MMM-SN1-MX-ONE

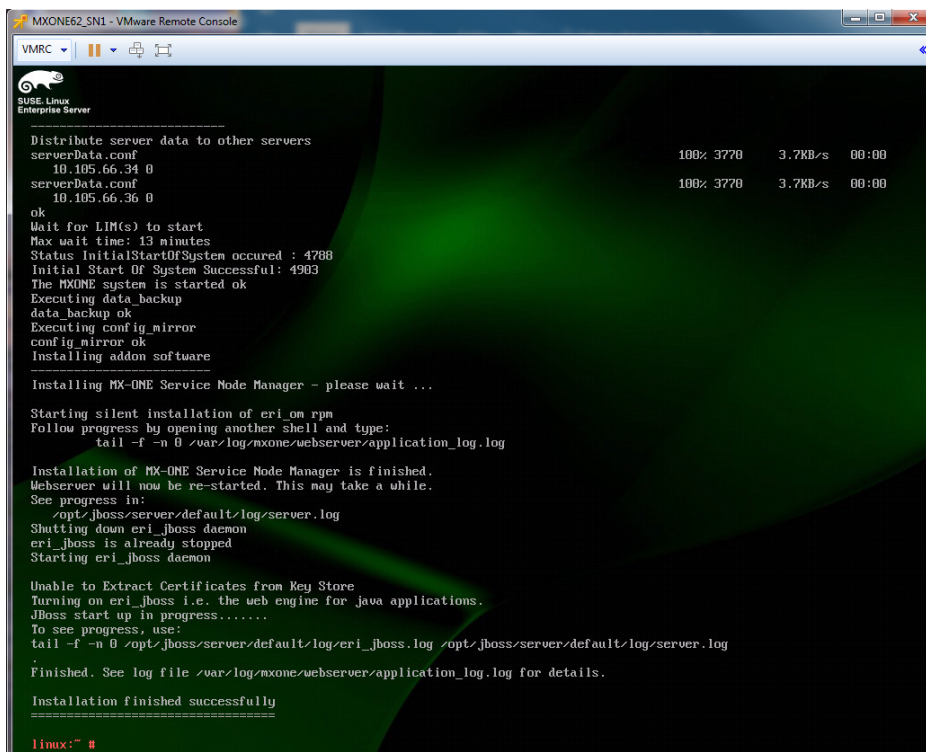
Failed servers will not be included if you choose to continue.
They can be added later

New server data file(s) received from:
MXONE-MMM-SN1-MX-ONE      ok
MXONE-MMM-SN2-MX-ONE      ok
MXONE-MMM-SN3-MX-ONE      ok
Press "c" to continue when data for all servers are present

```

10. Press **C** to continue the installation. When the installation is finished, the following screen is displayed.

Figure 13: MX-ONE Service Node Finish Setup (3 Service Nodes)



```

MXONE62 SN1 - VMware Remote Console
VMRC
SUSE Linux
Enterprise Server

Distribute server data to other servers
serverData.conf      100% 3770    3.7KB/s  00:00
10.105.66.34 0
serverData.conf      100% 3770    3.7KB/s  00:00
10.105.66.36 0
ok
Wait for LHM(s) to start
Max wait time: 13 minutes
Status InitialStartOfSystem occurred : 4788
Initial Start Of System Successful: 4903
The MXONE system is started ok
Executing data_backup
data_backup ok
Executing config_mirror
config_mirror ok
Installing addon software

Installing MX-ONE Service Mode Manager - please wait ...

Starting silent installation of erl_om rpm
Follow progress by opening another shell and type:
tail -f -n 0 /var/log/mxone/webserver/application_log.log

Installation of MX-ONE Service Mode Manager is finished.
Webserver will now be re-started. This may take a while.
See progress in:
/opt/jboss/server/default/log/server.log
Shutting down erl_jboss daemon
erl_jboss is already stopped
Starting erl_jboss daemon

Unable to Extract Certificates from Key Store
Turning on erl_jboss i.e. the web engine for java applications.
JBoss start up in progress.....
To see progress, use:
tail -f -n 0 /opt/jboss/server/default/log/erl_jboss.log /opt/jboss/server/default/log/server.log
.
Finished. See log file /var/log/mxone/webserver/application_log.log for details.

Installation finished successfully

linux:~ #

```


11. Execute basic tests in the Service Nodes without placing the configuration. You can do this during office hours without system down time.
12. Create a VMware snapshot for the new system, if desired. It might be useful in some cases.

4.1.3 Setting up Microsoft Hyper-V® for MiVoice MX-ONE

To install a Hyper-V machine instance make sure your system meets the following requirements:

- Installed Windows Server 2008, 2012, or 2016
- Have a Windows License (no other special licenses needed)
- Runs on a Dell and HP server
- Have .vhd and .vhdx format image for installation

Enabling Hyper-V

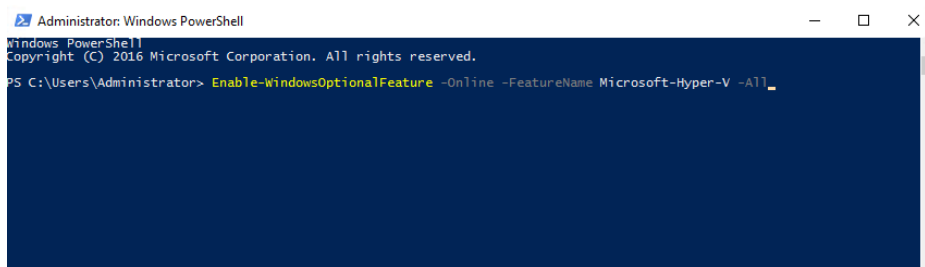
To enable Hyper-V using a power shell:

1. Open a PowerShell console as Administrator.

2. You can do either of the following:

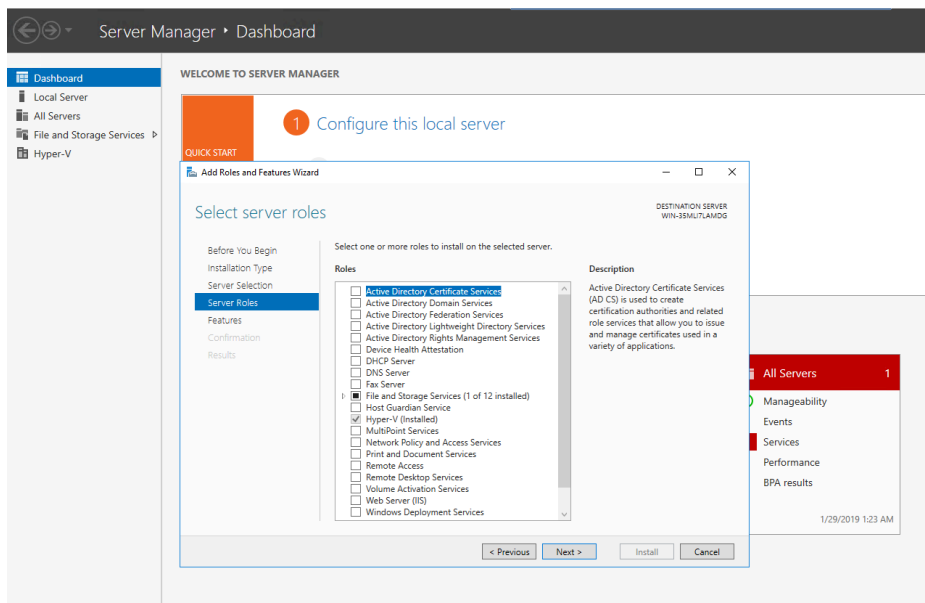
- Run the following command: `Enable-WindowsOptionalFeature -Online -FeatureName Microsoft-Hyper-V -All`

Figure 14: Windows PowerShell



- Open **Server Manager** and select Server Roles to add role and features and Install Hyper-V

Figure 15: Server Manager - Configure Local Server

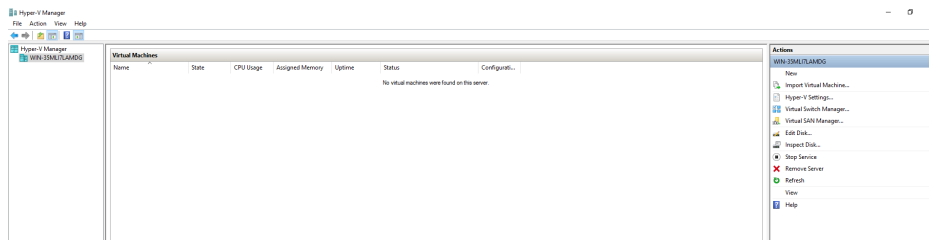


Installing Hyper-V

- Before you install Hyper-V, create a Virtual Switch Manager for Hyper-V to give network access to the virtual machines.

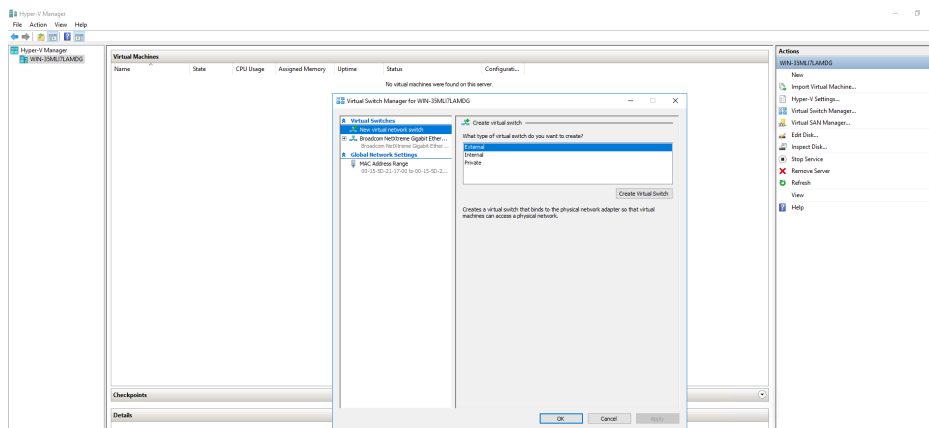
- Select **Virtual Switch Manager**.

Figure 16: Virtual Switch Select



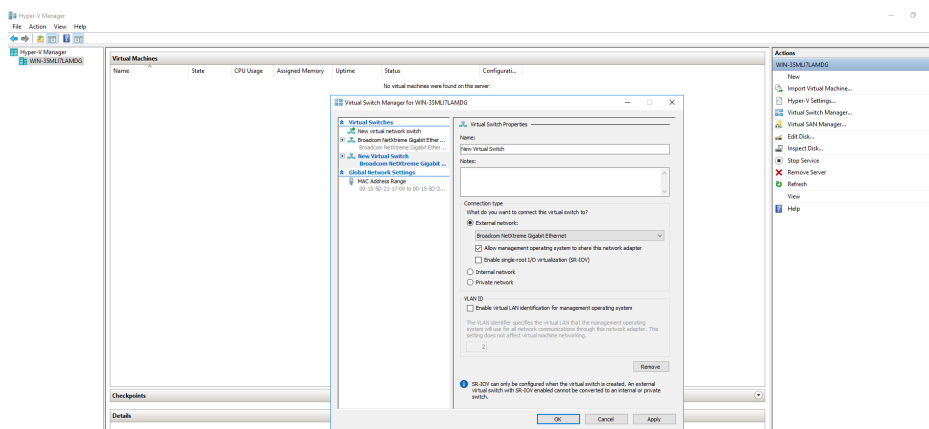
- Select type of switch, **External Switch**.

Figure 17: Switch Type



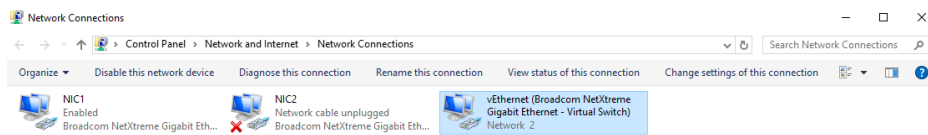
- Enter the name to the switch and click **Apply**.

Figure 18: Switch Name



- d. Go to Control Panel > Network Internet > Network Connections to view the new virtual manager that you created in the above step.

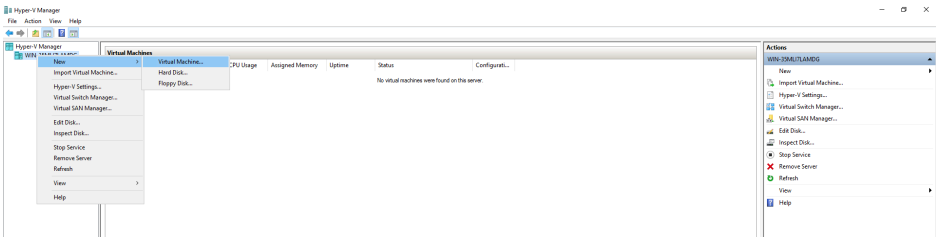
Figure 19: Network Connections



2. Create a Virtual instance:

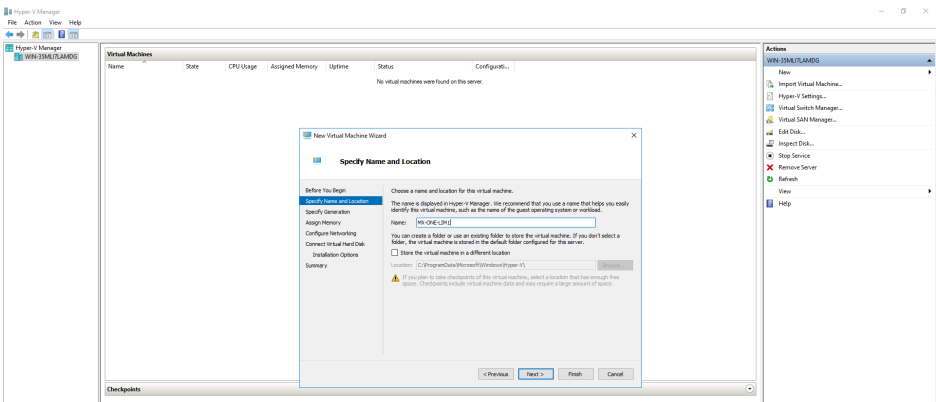
a. Select **New > Virtual Machine**.

Figure 20: Virtual Machine - New



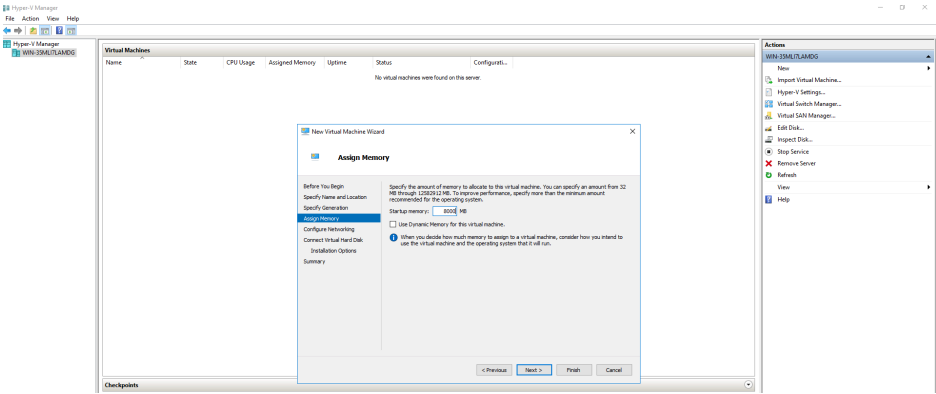
b. Enter the name of the virtual instance.

Figure 21: Specify VM Name and Location



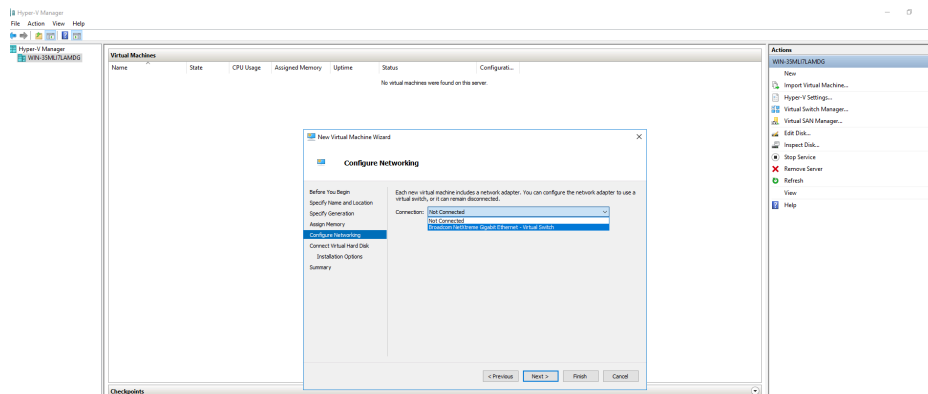
c. Assign the memory required for the virtual instance.

Figure 22: Assign Memory



d. Select the network switch that you configured initially.

Figure 23: Network Selection



- e. Select the image (VHD). Use an existing virtual Hard disk and select the location where your VHD image is stored. For MX-ONE, unzip the Hyper-V image and select the Virtual Hard Disk.

Figure 24: Image Selection_1

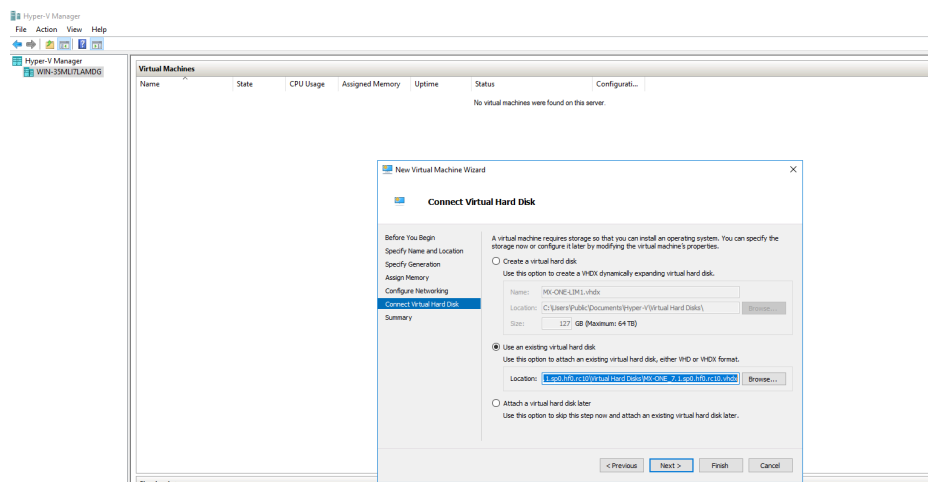
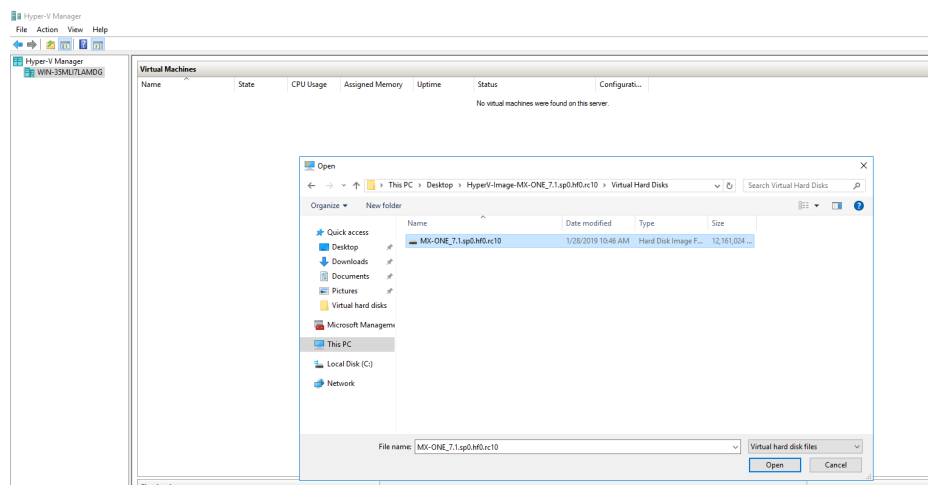
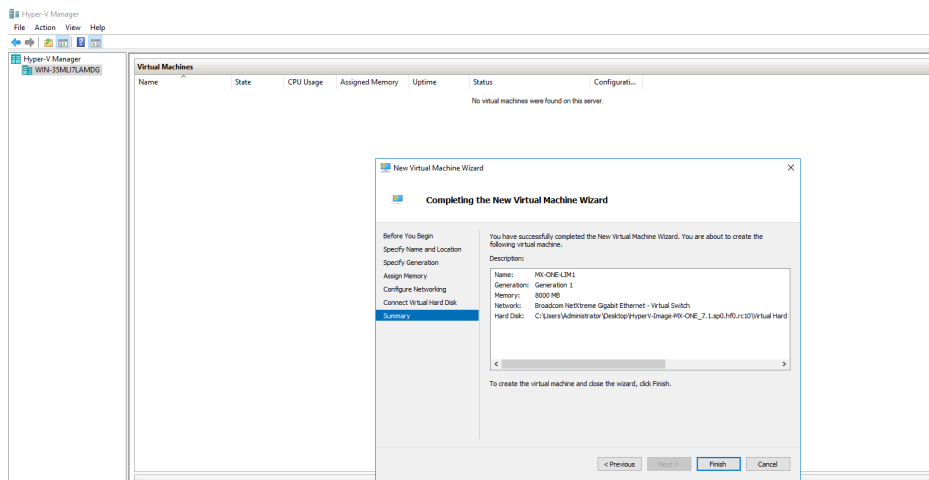


Figure 25: Image Selection_2



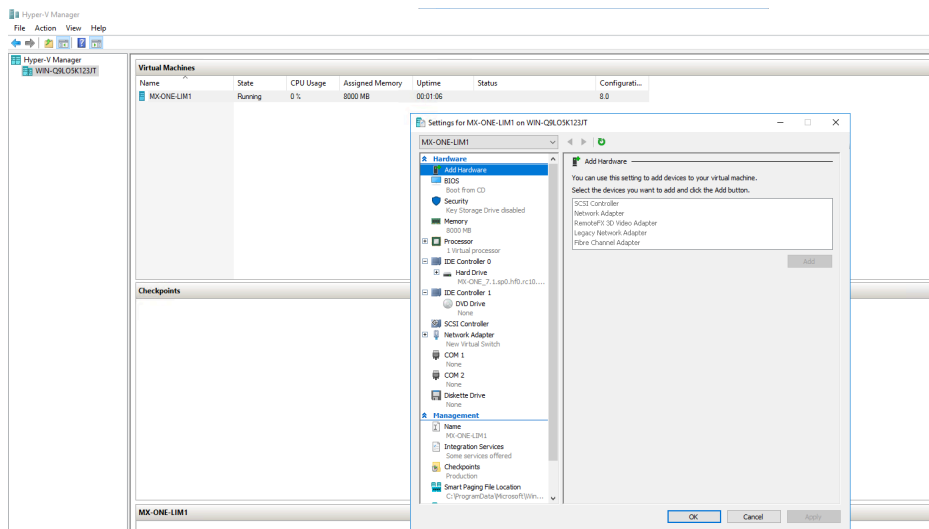
- f. Review the summary of the configuration details and click **Finish**.

Figure 26: Review Summary



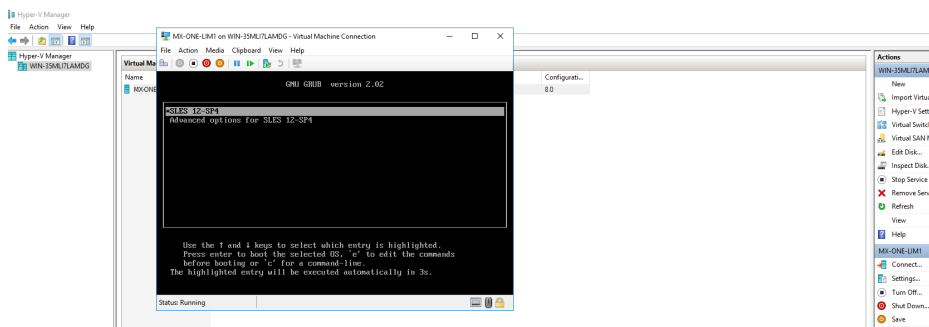
3. Change virtual machine settings as per the requirement.

Figure 27: Change VM Settings



4. Start the virtual machine.

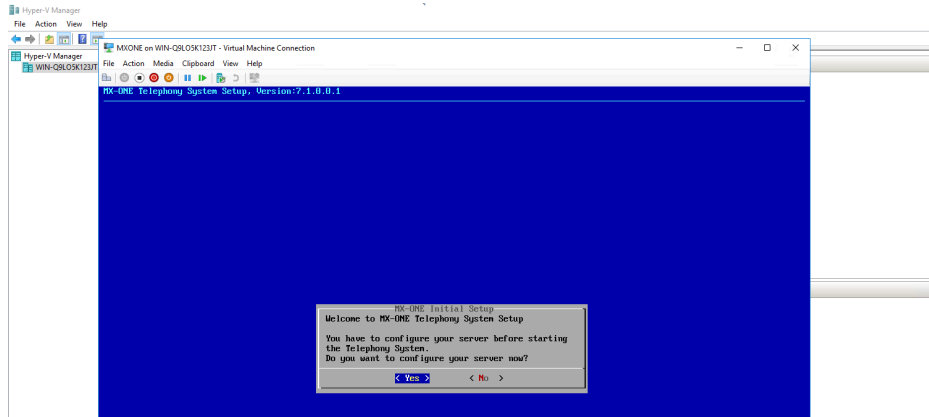
Figure 28: Select VM



5. Install MX-ONE on the virtual machine instance:

- a. Click **Yes** to configure the MX-ONE server.

Figure 29: MX-ONE Initial Setup



- b. The network service restarts:

Figure 30: Network service restart

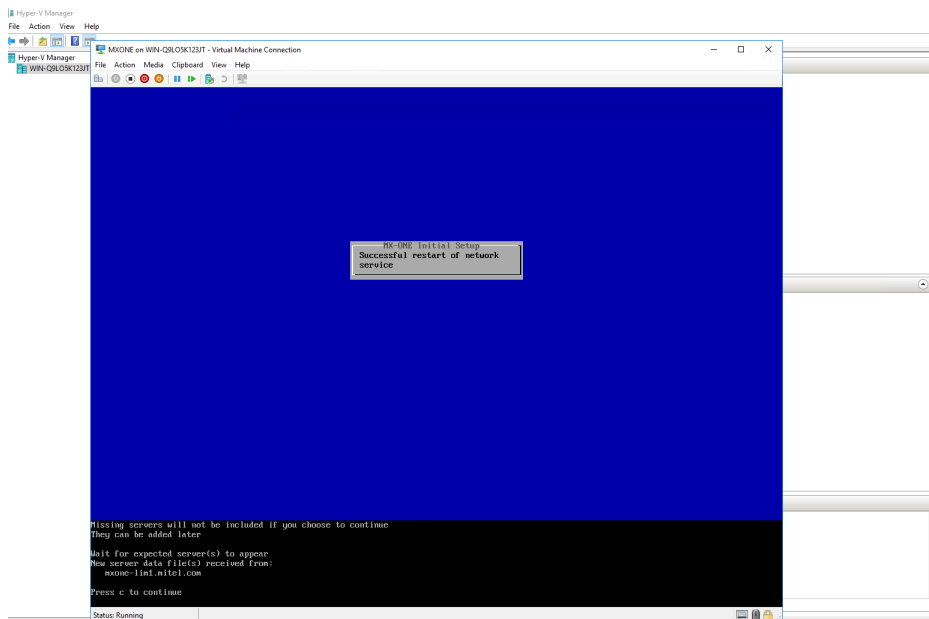
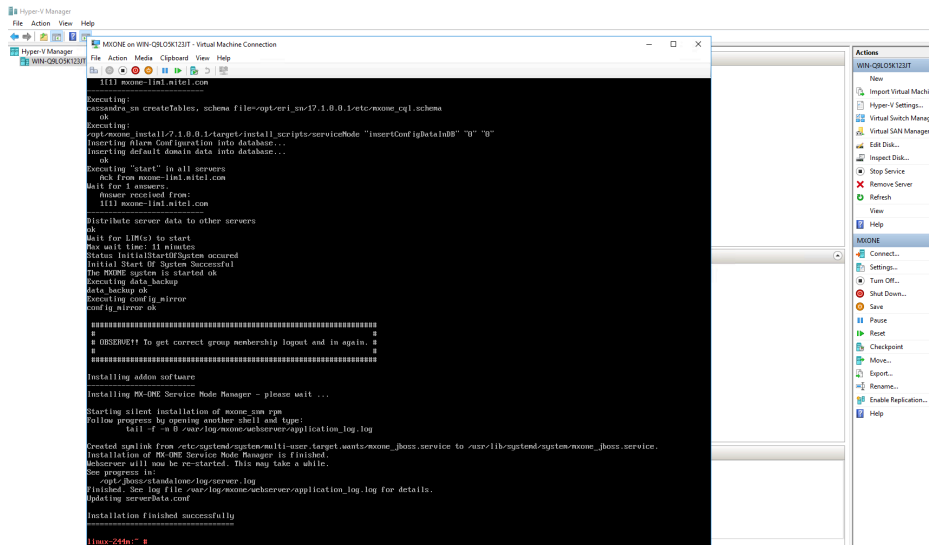


Figure 31: MX-ONE Setup Complete



4.2 Standard Infrastructure

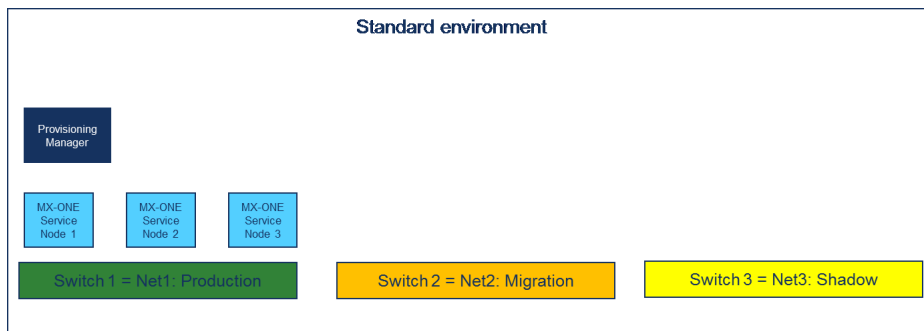
The standard infrastructure needs to be in place. The main activities are:

- Creation of the two new networks, Migration and Shadow (it is not mandatory in this case).
- Deploy MiVoice MX-ONE.

4.2.1 Network Setup

In the standard infrastructure, the Migration and Shadow networks are created in an isolated switch in the customer or partner network.

Figure 32: Standard Environment Upgrade (before)



4.2.2 Deploy MiVoice MX-ONE

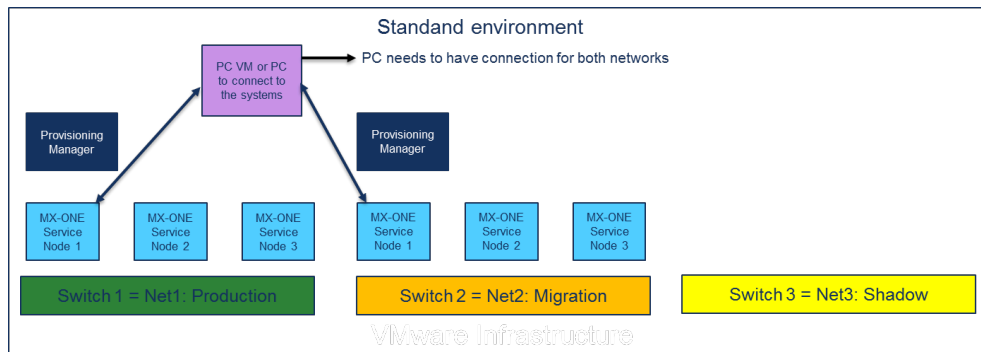
To deploy MiVoice MX-ONE, do the following:

1. Create the number of Service Nodes required based on size of the current MX-ONE system.
2. Consider consolidation of server/Media Gateways to reduce footprint.
3. Install the new MX-ONE following standard MX-ONE installation documentation.
4. Configure required functionalities for the specific customer. For example, synchronization between the Service Nodes.
5. Execute basic tests in the Service Nodes without placing the configuration. You can do this during office hours without system down time.

Note:

When a PC is connected to the systems, it access both Production and Migration network.

Figure 33: Standard Environment New System Deployed (after)



4.3 PC-Regen

PC-Regen is a MX-ONE tool used to collect the current customer data. A PC-Regen from the system that is going to be upgraded needs to be done.

Consult your PC-Regen in MX-ONE CPI documentation in order to execute the steps below.

4.3.1 Collecting the Current Data

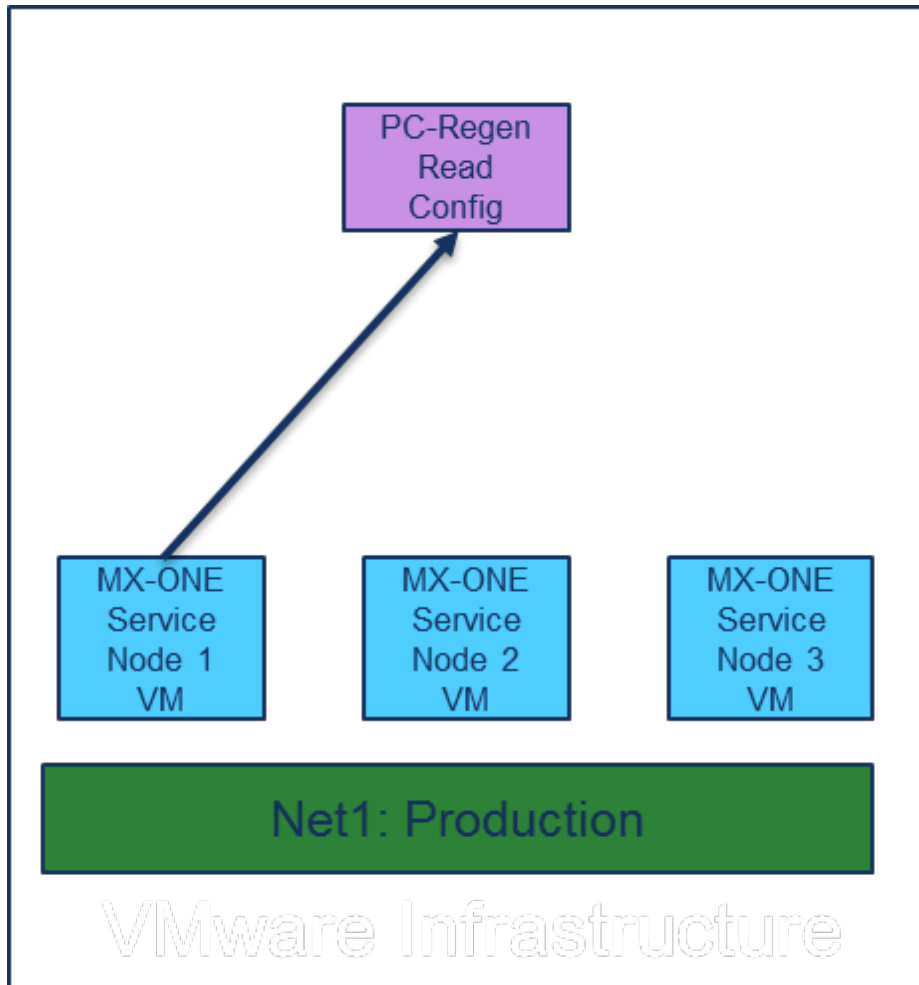
PC-REGEN must be available at the customer site or must be connected remotely (if that is allowed by the customer) to read/fetch the current customer data.

This is done during office hours without no system down time.

Note:

When the PC-Regen is collected and the customer constantly does MAC (Move, Add and Change) in the system, it is recommended that the changes stored in a file must be sent to the system afterwards.

Figure 34: PC-Regen Setup



4.3.2 Send the Data to the New System

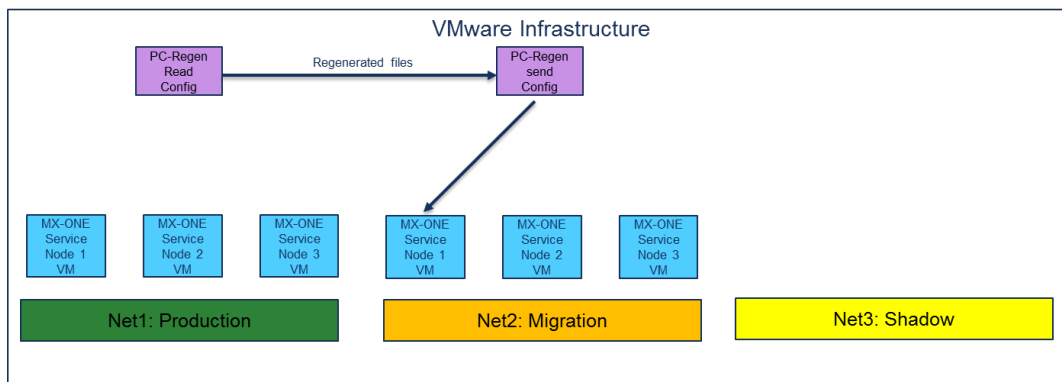
The collected data is regenerated via PC-Regen. Send the configuration files to MX-ONE as per the MX-ONE CPI documentation.

Note:

Disable the security check if a considerable amount of data is sent to the system. Depending of the system size this activity can take hours or days. Sometimes, the PC-Regen of a system with 12000 users are sent over the weekend. See the *MiVoice MX-ONE Administration Guide, Chapter 13, Server Hardening*.

When the system setup is completed, execute MX-ONE backup and a VMware snapshot, if desired. This is done during office hours without no system down time.

Figure 35: PC-Regen File Send Process (to the new system)



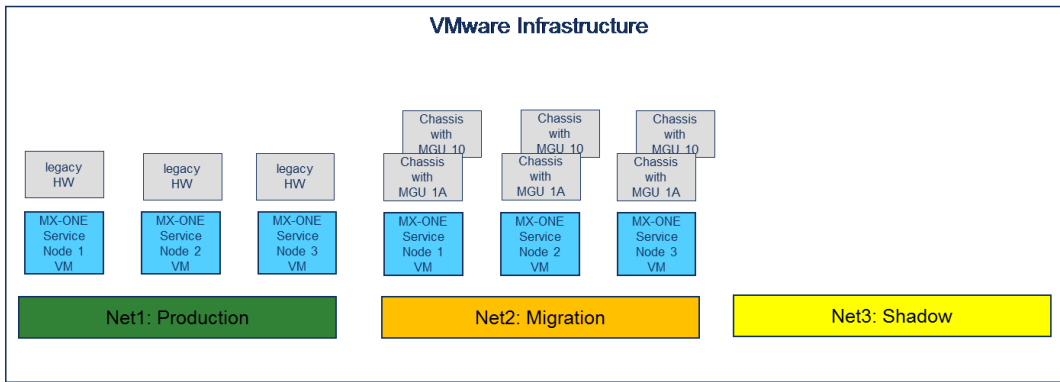
4.3.3 Media Gateway and Media Server Setup

If old hardware is replaced by new chassis with MGU (recommended scenario), update the MGUs if they are not with the latest software. This procedure is not described in this document, refer the *MX-ONE CPI* documentation.

If the customer is using Media Server, then install and configure it. And to follow the procedure, refer the *MX-ONE CPI* documentation.

Execute all tests required in the new system. This work is done during office hours – no down time.

Figure 36: Environment with Media Gateways



4.4 Migrating Provisioning Manager and Service Node Manager

To migrate Provisioning Manager and Service Node Manager, the database backups are required.

For more information, see *Chapter 5, UPGRADING OR UPDATING TO MIVOICE MX-ONE 7.X, Installation Instruction document*.

4.4.1 Backup Service Node Manager (Manager Telephony Server in MX-one 5.0)

To backup Service Node Manager database in the MX-ONE 5.0 SP7, execute the following:

1. Make sure that you are logged in as root.
2. Create a folder. For example, `/home/eri_sn_admin/TSBackup/`
3. Change the permission to allow postgres to write in the folder, such as `chmod 757 /home/eri_sn_admin/TSBackup`.
4. Save all data of WBM database.
 - Run the following command: `su postgres -c "pg_dump -a -D -d WBM -f /home/eri_sn_admin/TSBackup/wbm_data_only.sql"`
 - It may be necessary to enter the password for the database, which by default is default in MX-ONE 5.0.
5. Save all data of QoS Database and run the following command: `su postgres -c "pg_dump -U postgres QoS -f /home/eri_sn_admin/TSBackup/QoS_entire_data.sql -C --inserts"`
6. Enter the password for the database, which is default in MX-ONE 5.0.
7. Copy the created files to an external media, for example a USB memory, or another safe location.

Template Data Backup

1. Ensure that you are logged in as root on the Manager Telephony System Server.

2. Run the following command to archive the templates: `"tar -cf customer.tar --directory=/opt/jboss/server/default/conf/templates"`
3. Copy the customer.tar file to an external media. For example, to a USB memory.

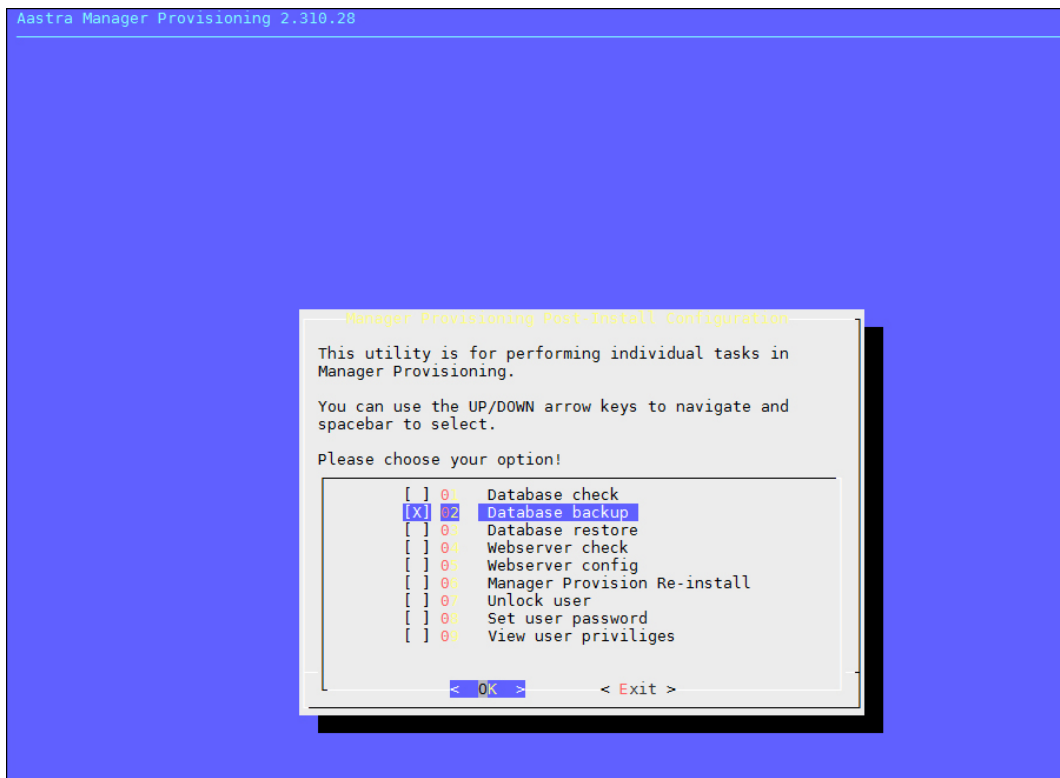
4.4.2 Backup Provisioning Manager (Manager Provisioning in MX-ONE 5.0)

If Provisioning Manager and Service Node Manager are installed on the same server or on different servers, the data for Provisioning Manager must be saved. Because, upgrading Service Node Manager clears the database that is used by Provisioning Manager.

To backup Provisioning Manager database in the MX-ONE 5.0 SP7, execute the following:

1. Logon on Manager Provisioning server as root.
2. Create a Folder `/home/eri_sn_admin/TSBackup/` if it does not exist. Such as, `mkdir -p /home/eri_sn_admin/TSBackup/`
3. Enter the command `mp_config` and select **Database backup**.

Figure 37: Manager Provisioning mp_config Utility



4. Backup MP database is stored in directory `/var/opt/mxone_pm_config/` with a file name starting with “mpManagerPostgresDump” followed by date, rpm version and release details.

Figure 38: Manager Provisioning Backup Result

```
MXONE50SN1:/var/opt/eri_mp_config # ls -la
total 56724
drwxr-xr-x 3 root root 4096 Nov 22 12:18 .
drwxr-xr-x 7 root root 4096 Nov 3 16:12 ..
-rw-r----- 1 jboss jboss 29002706 Nov 21 10:21 mpManagerPostgresDump.20161121102113-2.310.28_201512230909
-rw-r----- 1 jboss jboss 29002706 Nov 22 12:19 mpManagerPostgresDump.20161122121857-2.310.28_201512230909
```

5. Save all data of Quartz Database using the following command: `su postgres -c "pg_dump -a -D -d Quartz -f /home/eri_sn_admin/TSBackup/Quartz_data_only.sql"`
6. Enter the password for the database, which is default in MX-ONE 5.0.
7. Copy the created files (or the entire directory) to an external media, for example a USB memory, or another safe location.

Manager Provisioning Template Data Backup

1. Ensure that you are logged in as root on the Manager Provisioning Server. This is useful when the Manager Provisioning is in different server (standalone).
2. Run the following command to backup the templates: `tar -cf customer_mp.tar --directory=/opt/jboss/server/default/conf/templates.`
3. Copy the customer_mp.tar file to an external media, for example an USB memory.

4.4.3 Restore Service Node Manager

Note:

Before executing this step, first restore MX-ONE data by using PC-Regen. Ensure that the required resources to the Service Node Manager are in place. Adjust the Jboss heap memory of the server according to the Service Node Manager. To do this, refer the Service Node Manager Installation document in MX-ONE CPI.

To restore Service Node Manager, do the following:

1. Go to the new Service Node Manager installed in the Service Node 1.
2. Copy the Manager Telephony System's data files (wbm_data_only.sql, QoS_entire_data.sql, customer.tar) to `/home/eri_sn_admin/TSBackup` Directory.
3. Provide the 755 permissions to these files.
4. Execute the snm_upgrade script then follows the instructions. This script restores WBM, QoS and customer.tar (customer templates) to the system.

4.4.4 Restore Provisioning Manager

Note:

Restore Service Node Manager before restoring Provisioning Manager in case of Co-existence system. The Provisioning Manager in this example has 23 K users that were synchronized via Active Directory with the MX-ONE 5.0. The system has 15 K SIP extensions. So, this requires a Provisioning Manager standalone.

Figure 39: Restore Service Node Manager

```

MXONE-MMM-SN1:/local/home/mxone_admin/TSBackup # snm_upgrade
The 5.x to 6.x data restore Process Needs Restart of PostgreSQL Database and PM/SNM/CSTAPhaseIII applications.
Do you still want to Continue to Restore the Data [YES/NO]
yes

Restoring previous data to Service Node Manager...

Current RPM Version 6.2.0.0.9.479
Current RPM Release 201611031016
customer/
customer/AccountCode/
customer/AnalogueExtension/
customer/AuthorizationCode_AUCOP/
customer/AuthorizationCode_IndAUCOP/
customer/CommonAbNum/
customer/Csp/
customer/Fax/
customer/HuntGroup/
customer/HuntGroupMember/
customer/IPEExtension/
customer/IPFunctionKey/
customer/IPPhoneConfigFile/
customer/MobileExtension/
customer/PersonalNumber/
customer/PickupGroup/
customer/Route/
customer/VirtualExtension/
customer/TelephonyServer/
customer/TelephonyServer/IP-template_4_IPEExtension/
customer/TelephonyServer/IP-template_4_IPEExtension/TemplateInfo.xml
customer/TelephonyServer/IP-template_4_IPEExtension/PELCP.xml
customer/TelephonyServer/IP-template_4_IPEExtension/GEDIP.xml
customer/TelephonyServer/IP-template_4_IPEExtension/GEADP.xml
customer/TelephonyServer/IP-template_4_IPEExtension/IPEXP.xml
customer/TelephonyServer/IP-template_4_IPEExtension/NIINP.xml
customer/TelephonyServer/IP-template_4_IPEExtension/PELPP.xml
customer/TelephonyServer/IP-template_4_IPEExtension/PNNames.xml
customer/TelephonyServer/IP-template_4_IPEExtension/SUSIP.xml
customer/TelephonyServer/IP-template_4_IPEExtension/GEFKP.xml
...Restore of data completed.
See /var/log/mxone/eri_om/eri_om_rpm_6.2.0.0.9.479_201611031016_5_0_to_6_0.log
Starting the Application...
Starting eri_jboss daemon

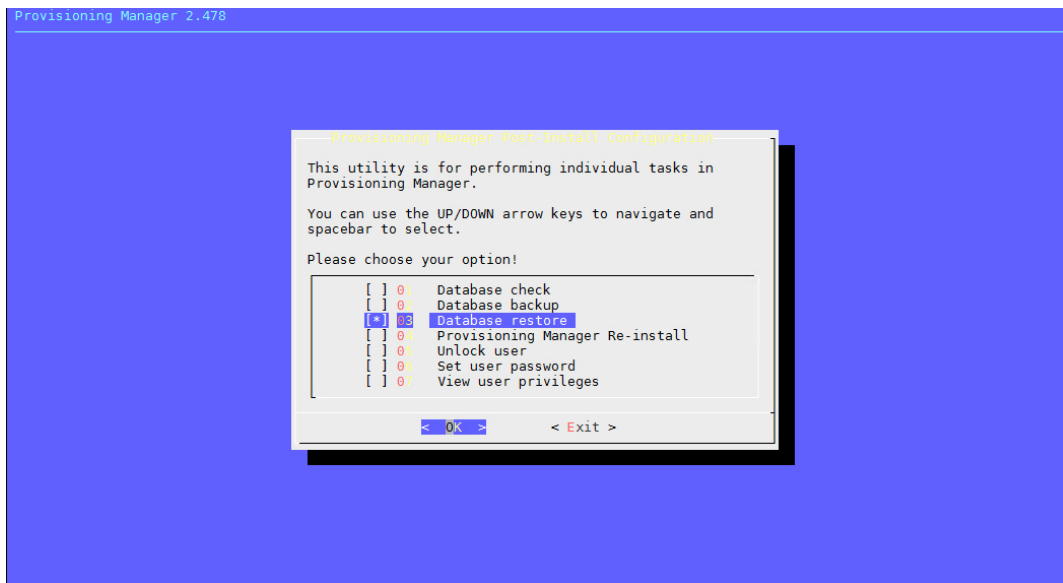
Unable to Extract Certificates from Key Store
Turning on eri_jboss i.e. the web engine for java applications.
JBoss start up in progress.....
To see progress, use:
tail -f -n 0 /opt/jboss/server/default/log/eri_jboss.log /opt/jboss/server/default/log/server.log
MXONE-MMM-SN1:/local/home/mxone_admin/TSBackup #

```

To restore the backup in Provisioning Manager, execute the following:

1. Copy the Manager Provisioning data files (mpManagerPostgresDumpxxxxxx, Quartz_data_only.sql, customer_mp.ear) files to /var/opt/mxone_pm_config/ Directory.
2. Make sure that the files are owned by "root" user.

3. Execute `mp_config` and select **Database restore**. The script takes care of restoring PM, Quartz databases and `Customer_mp.tar` (Customer template) data.

Figure 40: Provisioning Manager `mp_config` Utility

4. Remove the `Quartz_data_only.sql` and `customer_mp.tar` from `/var/opt/mxone_pm_config` directory after data restore.
5. Execute the following command: `cd /var/opt/ mxone_pm_config rm -f Quartz_data_only.sql customer_mp.tar.`

4.4.5 Verify Provisioning Manager and Service Node Manager setup

After restoring the database, both software needs get verified to execute the sanity check.

Provisioning Manager Details

To view Provision Manager:

1. Login in to the Provisioning Manager and change the administrator password if it is not in compliance with MX-ONE 6.X requirements.

Figure 41: Provisioning Manager Page (after restore)

Mitel | Provisioning Manager Logged in as: administrator About User Guide Site Map Logout

Own Settings

General

General [Help](#)

[Apply](#)

The current password is not compliance with MX-ONE 6.x and above security standards. Please change it to strong password

First Name: pm_administrator Last Name: pm

User Id: administrator

Current Password:

New Password:

Confirm New Password:

Security Profile: System Setup Admin

Email Address:

Alternate First Names:

Keywords:

Department(s): ABS_packets; Denver

Preferences

Use Last Selection: ☒

Provisioning Manager Language: English

[Apply](#)

2. Go to user task and check if users are present in the Manager Provisioning 5.0 in the new system. In the Provisioning Manager User task, the first page is presented below showing the first 200 users.

Figure 42: User Task (all users page 1)

Mitel | Provisioning Manager Logged in as: administrator About User Guide Site Map Logout

Users Services Administrators System Logs Own Settings

User Departments UDF Mapping Unlock

User [Help](#)

[Add](#)

Enter User Name(s), Extension Number, Department: *

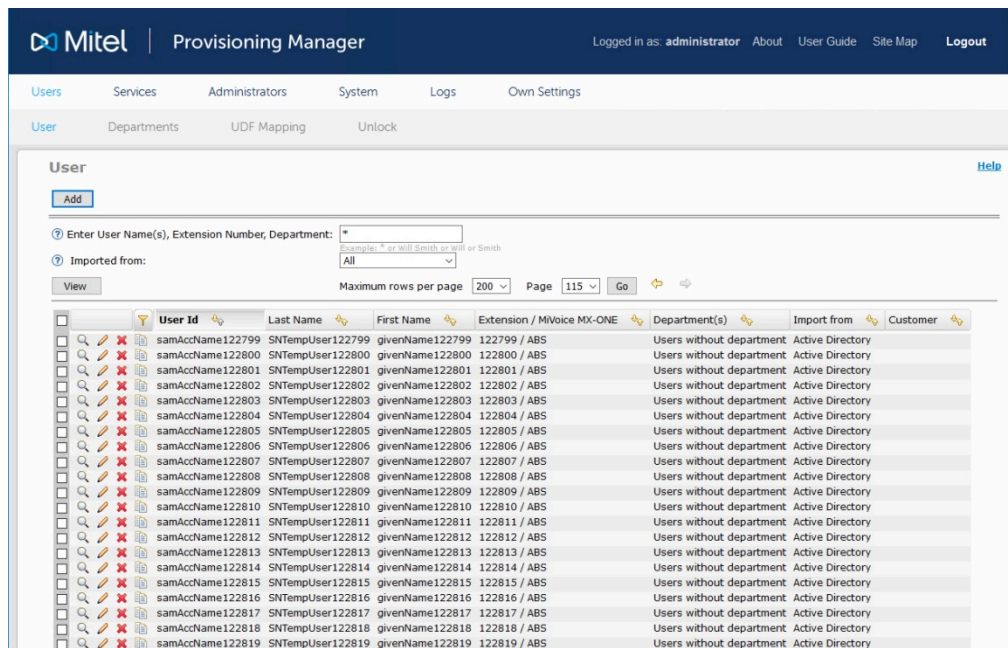
Imported from: All

Maximum rows per page: 200 Page: 1 Go

	User Id	Last Name	First Name	Extension / MiVoice MX-ONE	Department(s)	Import from	Customer
<input checked="" type="checkbox"/>	pm_administrator	pm	pm_administrator		ABS_packets		
<input checked="" type="checkbox"/>	samAccName100000	SNTempUser100000	givenName100000	100000 / ABS	Users without department	Active Directory	
<input checked="" type="checkbox"/>	samAccName100001	SNTempUser100001	givenName100001	100001 / ABS	Users without department	Active Directory	
<input checked="" type="checkbox"/>	samAccName100002	SNTempUser100002	givenName100002	100002 / ABS	Users without department	Active Directory	
<input checked="" type="checkbox"/>	samAccName100003	SNTempUser100003	givenName100003	100003 / ABS	Users without department	Active Directory	
<input checked="" type="checkbox"/>	samAccName100004	SNTempUser100004	givenName100004	100004 / ABS	Users without department	Active Directory	
<input checked="" type="checkbox"/>	samAccName100005	SNTempUser100005	givenName100005	100005 / ABS	Users without department	Active Directory	
<input checked="" type="checkbox"/>	samAccName100006	SNTempUser100006	givenName100006	100006 / ABS	Users without department	Active Directory	
<input checked="" type="checkbox"/>	samAccName100007	SNTempUser100007	givenName100007	100007 / ABS	Users without department	Active Directory	
<input checked="" type="checkbox"/>	samAccName100008	SNTempUser100008	givenName100008	100008 / ABS	Users without department	Active Directory	
<input checked="" type="checkbox"/>	samAccName100009	SNTempUser100009	givenName100009	100009 / ABS	Users without department	Active Directory	
<input checked="" type="checkbox"/>	samAccName100010	SNTempUser100010	givenName100010	100010 / ABS	Users without department	Active Directory	
<input checked="" type="checkbox"/>	samAccName100011	SNTempUser100011	givenName100011	100011 / ABS	Users without department	Active Directory	
<input checked="" type="checkbox"/>	samAccName100012	SNTempUser100012	givenName100012	100012 / ABS	Users without department	Active Directory	
<input checked="" type="checkbox"/>	samAccName100013	SNTempUser100013	givenName100013	100013 / ABS	Users without department	Active Directory	
<input checked="" type="checkbox"/>	samAccName100014	SNTempUser100014	givenName100014	100014 / ABS	Users without department	Active Directory	
<input checked="" type="checkbox"/>	samAccName100015	SNTempUser100015	givenName100015	100015 / ABS	Users without department	Active Directory	
<input checked="" type="checkbox"/>	samAccName100016	SNTempUser100016	givenName100016	100016 / ABS	Users without department	Active Directory	
<input checked="" type="checkbox"/>	samAccName100017	SNTempUser100017	givenName100017	100017 / ABS	Users without department	Active Directory	
<input checked="" type="checkbox"/>	samAccName100018	SNTempUser100018	givenName100018	100018 / ABS	Users without department	Active Directory	
<input checked="" type="checkbox"/>	samAccName100019	SNTempUser100019	givenName100019	100019 / ABS	Users without department	Active Directory	

3. In the Provisioning Manager User task, below is the last page is presented showing the remaining 200 users. In this system 200 users per page, 115 pages, resulting in 23000 users.

Figure 43: User Task (all users page 1)



4. Go to user task and add a new administrator user to manager the system (AlaCarte Service Provider).

Figure 44: User Task All Users (Page 115)

The screenshot shows the 'User - Add - Step 1 / 2' form. The form has a 'User' section with fields for 'First Name', 'User Id', 'Password', 'Email Address', 'Alternate First Names', and 'Keywords'. The 'First Name' field is 'admin', 'User Id' is 'admin_rd', 'Password' is '*****', 'Email Address' is empty, 'Alternate First Names' is empty, and 'Keywords' is empty. There are also fields for 'Last Name' (rd), 'Confirm Password' (*****), 'SMS', and 'Alternate Last Names'. Below the 'User' section is the 'User Defined Fields' section with fields for 'Business', 'Mobile Phone', 'Department(s)', 'Business 2', and 'Mobile Phone 2'. The 'Department(s)' field is selected, showing a list of departments: 'ABS_packets\12kusers_system\Users without de', 'ABS_packets\12kusers_system; Denver', and 'ABS_packets; Denver'. The 'Business' field is empty, 'Mobile Phone' is empty, 'Business 2' is empty, and 'Mobile Phone 2' is empty. At the bottom, there is a 'Preferences' section with a checkbox for 'Use Last Selection' (checked) and a dropdown for 'Provisioning Manager Language' (English). The form has 'Back', 'Next', 'Apply', and 'Cancel' buttons.

5. Go to Administrator task and select Administrator and click **Add**.

6. Select the new administrator user and the Security Profile AlaCarte Service Provider, make the other setup and click **Apply**.

Figure 45: Add Administrator Page

UsersServicesAdministratorsSystemLogsOwn Settings

AdministratorSecurity Profiles

Administrator - Add

ApplyCancel

User Name(s),
Extension Number,
Department:

adSearch

☒ admin_rd , admin rd , Users without department

AlaCarte Service ProviderView...Edit...

Security Profile:

AlaCarte Service ProviderView...Edit...

Access to
Department(s):

Existing Department(s),
Location(s):

ABS_packets; Denver
ABS_packets\12Kusers_system; Denver
ABS_packets\12Kusers_system\Users without department; Denver

Selected
Department(s),
Location(s):

All

--><--Move UpMove Down

Access to Subsystems
in Location(s):

All
Denver

ApplyCancel

7. If the new administrator user is successfully created, the following screen is presented.

Figure 46: Add New User Result

User - Add - Result

Done

Add operation successful for:

User Id: admin_rd

User

Property	Value
User Id	admin_rd
First Name	admin
Last Name	rd
Department(s)	ABS_packets\12Kusers_system\Users without department; Denver ABS_packets\12Kusers_system; Denver ABS_packets; Denver
Preferences	
Use Last Selection	Yes
Provisioning Manager Language	English

Add New...Change This...Remove ThisAdd From This...Done

8. If the security profile for new administrator user is successfully assigned, the following screen is presented.

Figure 47: Add Administrator Result

Administrator - Add - Result

Done

Add operation successful for:

- User Id: admin_rd

Property	Value
User Id	admin_rd
Security Profile	AlaCarte Service Provider
Access to Department(s)	ABS_packets; Denver ABS_packets\12Kusers_system; Denver ABS_packets\12Kusers_system\Users without department; Denver
Access to Subsystems in Location(s)	Denver

Add New... Change This... Remove This Add From This... Done

9. Login with the new administrator user, in the example admin_rd.
10. Go to **System menu> Subsystem**, change the **Subsystem** information, **Version** and User ID in **Subsystem**.

Figure 48: Subsystem View Page

Subsystem - Change - ABS

Apply Cancel

? Subsystem Type: MiVoice MX-ONE

? Use HTTPS: ☐

? Subsystem Name: * ABS

? Version: 5.0 SP7

? IP Address: * 10.105.66.30

? Port: 80

? User ID in Subsystem: administrator

? Password in Subsystem:

? Confirm Password in Subsystem:

? Terminal Password:

? Confirm Terminal Password:

? IP Phone Server: Enter Manual URL

? Domain Folder:

? Location: Denver Edit...

Apply Cancel

11. Subsystem change result is presented below.

Figure 49: Subsystem Change Result

Subsystem - Change - ABS - Result

Done

Change operation successful for:

- **Subsystem Name:** ABS

Property	Value
Subsystem Type	MiVoice MX-ONE
Use HTTPS	No
Subsystem Name	ABS
Version	6.2
IP Address	10.105.66.30
Port	80
User ID in Subsystem	admin_rd
IP Phone Server	
Location	Denver

Change This...

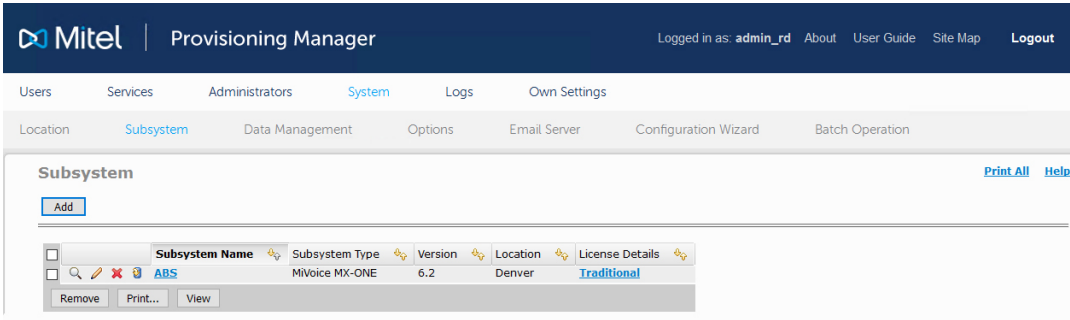
Done

Note:

In this example Provisioning Manager is used for the Service Node Manager authentication

12. If the setup is correct, the license information is shown as below.

Figure 50: Subsystem Page



13. Go to User task and select for example first and the last user and check if the extension information is correct.

- Click in the pencil icon to change or magnifier to view the extension configuration.

Figure 51: User Change Service Summary

User - Change - samAccName100000

User **Service Summary** **Scheduling**

Extension

?

 Assigned Extensions:

Extension Number

100000

MiVoice MX-ONE
ABS

?

 Assign Existing Extension:

Extension Number

MiVoice MX-ONE

ABS

?

 Template For New Extension:

<Select template>

?

 Add New Extension:

Add...

Advanced...

Below the change page is shown for the extension 100000.



Figure 52: User change extension page

Extension - Change - 100000-MultiTerminal-ABS

Continue

Cancel

General

② MiVoice MX-ONE:	ABS
② Extension Number:	100000
② Description:	<div></div>
② Server Number:	1
② Extension Type:	Multi-Terminal
② Customer:	None
② Common Service Profile:	2 - (None) ▾
② Phone Language:	Default ▾
② Backup Answering Position Number:	<div></div>
② Allow Security Exception:	<input checked="" type="checkbox"/>
② Boss/Secretary:	None ▾
② Home Area Code:	<div></div>
② DECT Extension:	<div>Add...</div>
② Mobile Extension:	<div>Add...</div>
② IP Extension:	<div>  100000</div>
② SIP Remote Terminal:	<div>Add...</div>
② SIP Auto-registered Terminal:	<div>Add...</div>
② SIP DECT Terminal:	<div>Add...</div>

Name Identity

② First Name:	<div>n100000</div>
② Last Name:	<div>100000</div>

Authorization Code

② Authorization Codes:	<div>Edit...</div>
------------------------	--------------------



Ring Signal

② Ring Signals:	<div>Edit...</div>
-----------------	--------------------

Personal Number

② Personal Number List:	<div>Edit...</div>
-------------------------	--------------------

1: Profile1:Active
5: Profile5:Set

15. Click in the pencil to change or magnifier to view the extension configuration.

Figure 53: User Change Service Summary

User - Change - samAccName122998




ApplyCancel

UserService SummaryScheduling

Extension

Assigned Extensions:

Extension Number

 122998

MiVoice MX-ONE
ABS

Assign Existing Extension:

Extension Number

MiVoice MX-ONE
ABS ▾

Template For New Extension:

<Select template> ▾

Add New Extension:

Add...

Advanced...

ApplyCancel

16. Below the change page is shown for the extension 122998.

Figure 54: User Change Extension Page

Extension - Change - 122998-IP-ABS

Continue
Cancel

General

MiVoice MX-ONE:
ABS

Extension Number:
122998

Description:

Server Number:
2

Extension Type:
IP

Customer:
None

Common Service Profile:
2 - (None)

Phone Language:
Default

Backup Answering Position Number:

Allow Security Exception:
☒

Allow EDN:
NO

Boss/Secretary:
None

Home Area Code:

Protocol:

☐ SIP
☒ IP

Free on Second Line:
Yes, but can be changed via terminal menu

Name Identity

First Name:

Last Name:

Authorization Code

Authorization Codes:
Edit...

Ring Signal

Ring Signals:
Edit...

Personal Number

Personal Number List:
Edit...

Logged On Status

Registered Phone Type:
NOT REGISTERED

Function Keys

Phone Type:
Other type

Panel Type:
No panel

Function Keys:
Change...

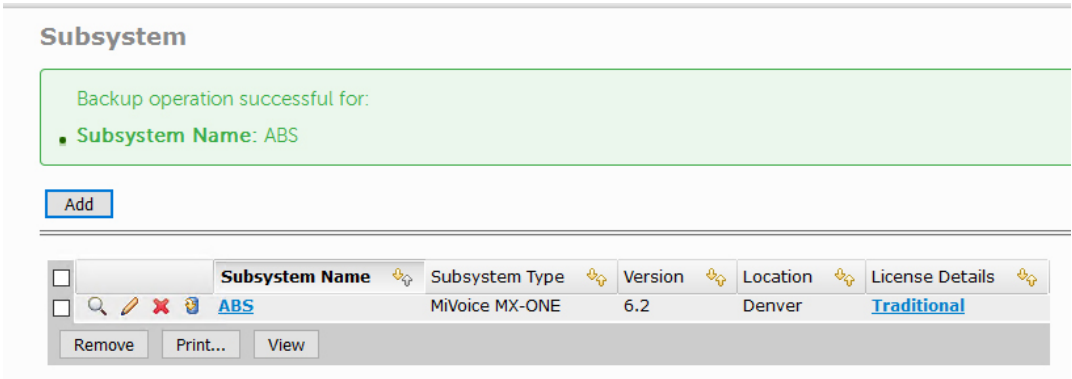
165/1531-ANF 901 14 Uen F 2023-12-21

Upgrade Process Minimizing System Downtime

40

17. Go to Subsystem and perform a Service Node backup if it is required.

Figure 55: Service Node Backup Result

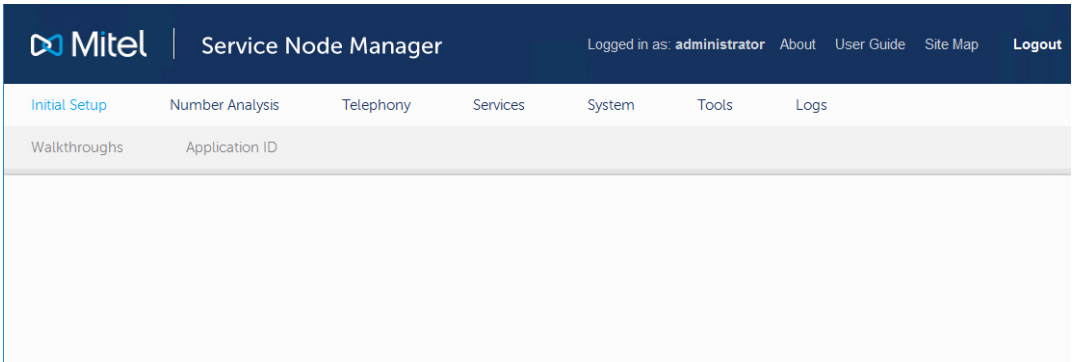


18. Click in the Subsystem Name link to open Service Node Manager.

Service Node Manager

1. Verify the Service Node Manager functionality.

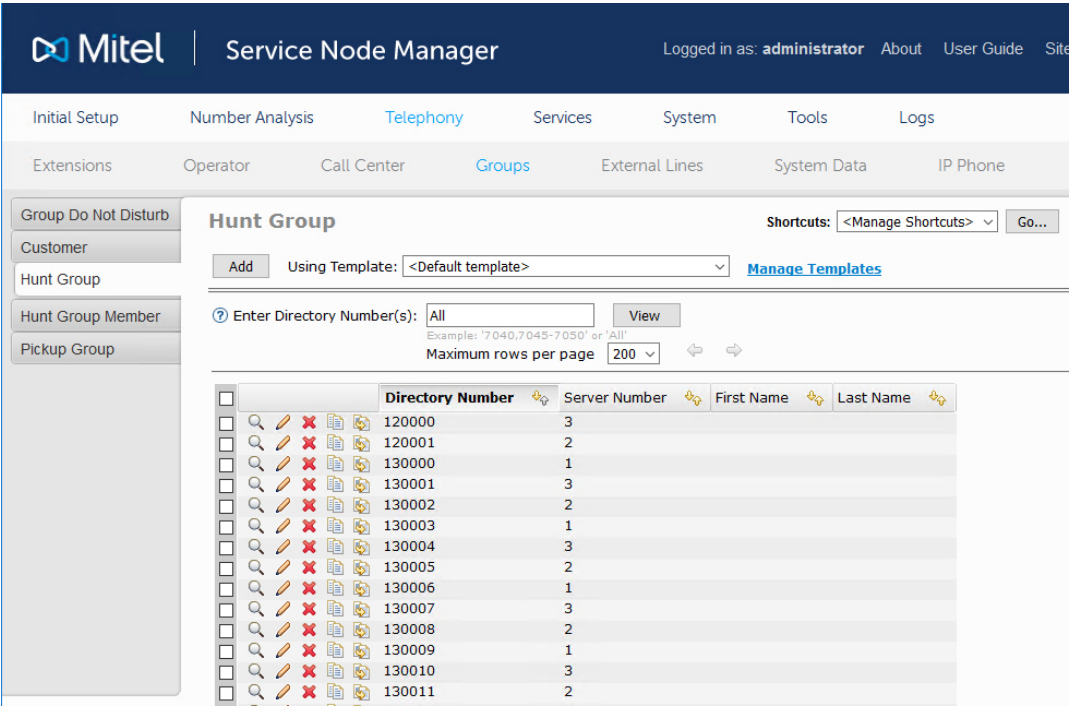
Figure 56: Service Node Manager Main Page



2. Navigate in the tool and check if the configuration is correct.

3. In Telephony menu, click **Groups** and then **Hunt Group**

Figure 57: Service Node Manager Hunt Group Page



If everything is correct, then start the migration.

4.5 Migration Process

If all the setup is working as desired, it is time to execute the migration. The procedure below just shows the Virtualized system; however, the bare metal is quite similar. Instead of moving the server between networks, the Ethernet cables must be changed between the switches ports (VLANs).

i Note:

If the old system is equipped with MGU boards and those need to be updated, load the new FW on the MGU while the old system is in place and then activate the new FW from the old MX-ONE 5.0/6.x system (board_sw command), when the activate command is sent and completed, wait for 30 seconds and proceed with the Migration part 1.

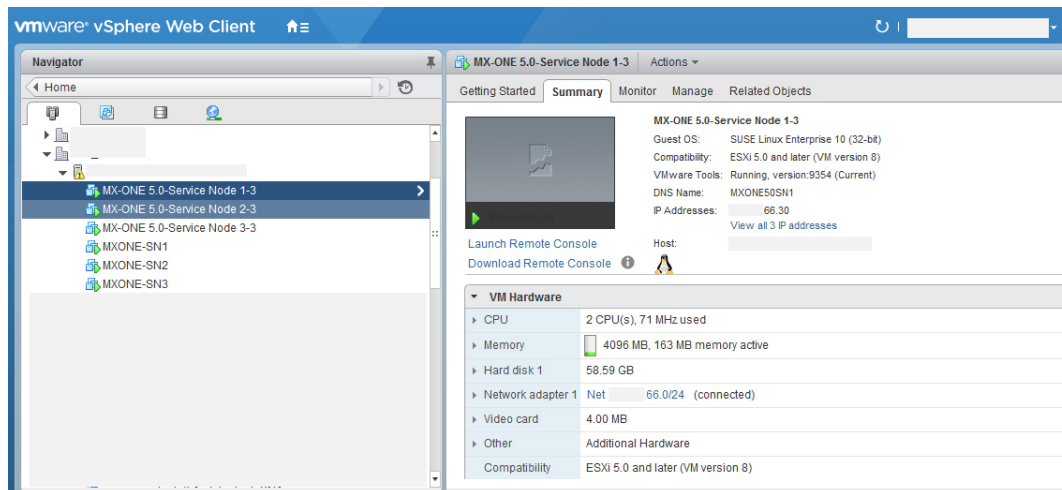
Though it is not a mandatory step, but it saves time in the overall upgrade process. Because, while the MGUs are installing the new software and rebooting, the MX-ONE migration can happen.

4.5.1 Migration Part 1

This phase starts the downtime period. Before starting the migration, the MX-ONEs have the following settings:

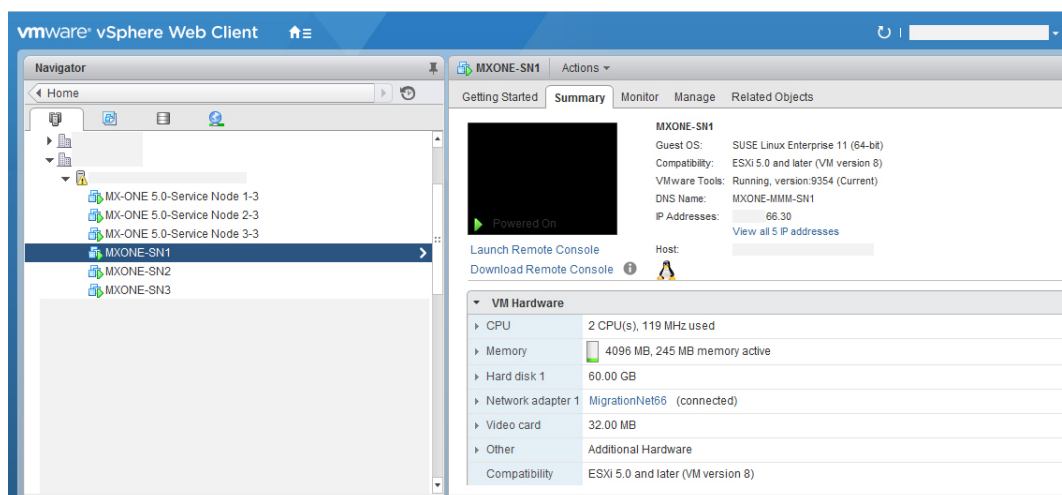
- Current system
- Production network
- IP address X.Y.66.30

Figure 58: MX-ONE 5.0 Production Network



- New System
- Migration Network
- IP address X.Y.66.30.

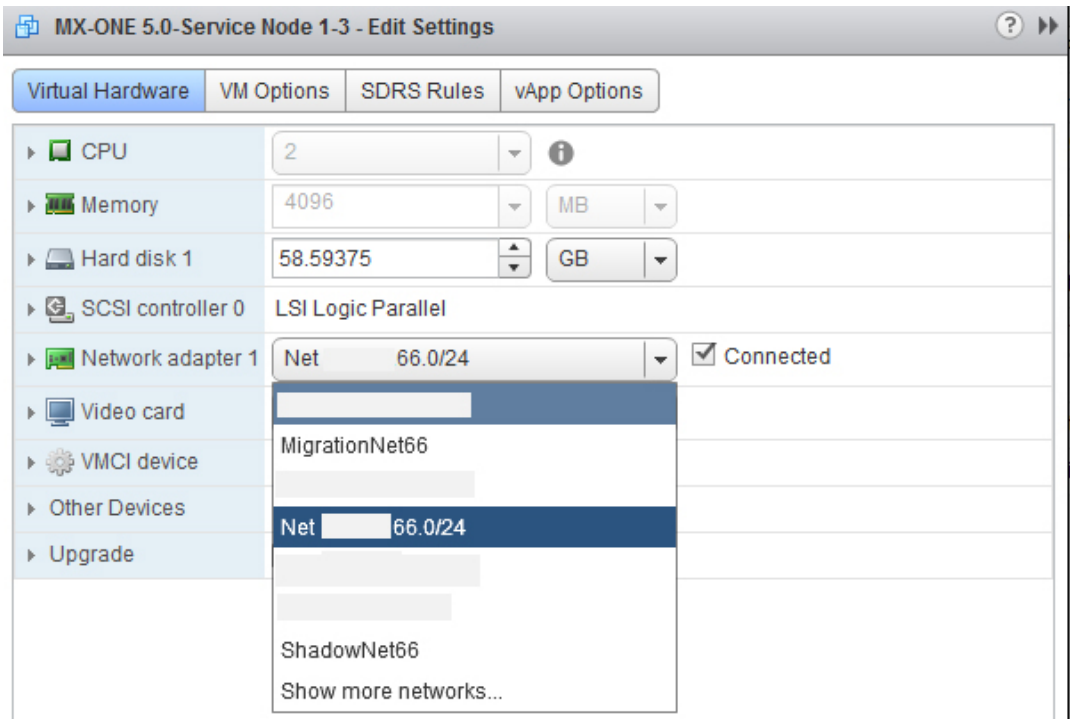
Figure 59: MX-ONE 6.X Migration Network



Move the current system from Production network to the Shadow network.

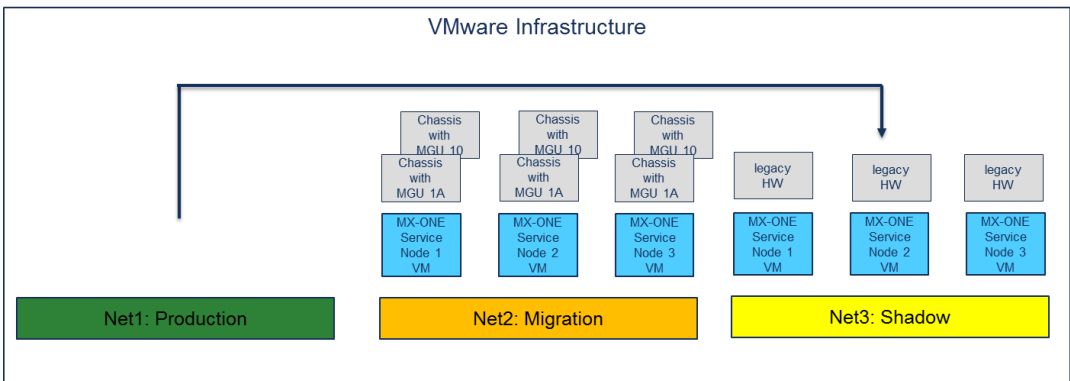
1. Go to the Virtual Machines for all Service Nodes server that compose the existing MX-ONE system and assign them to the Shadow network. During this process, there is no telephony service.

Figure 60: Migrating MX-ONE 5.0 Networks



2. MX-ONE executes a data reload after the migration to the Shadow network is completed.

Figure 61: Environment After Migrating MX-ONE 5.0 Networks



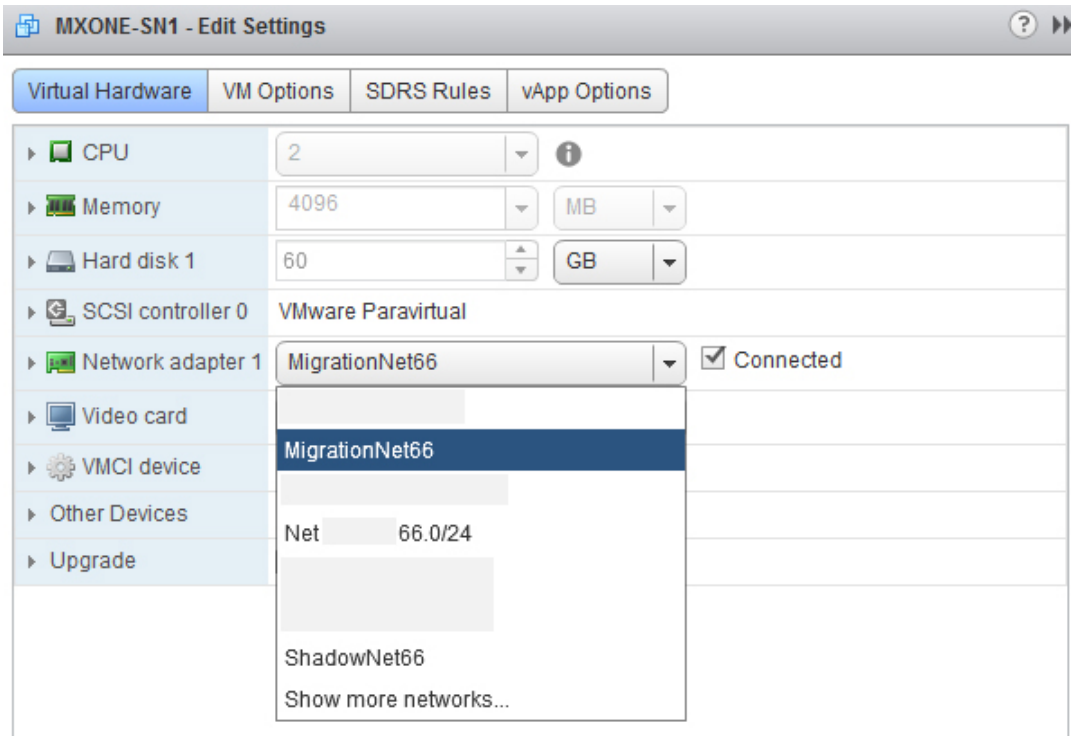
4.5.2 Migration Part 2

In this Migration Part 2 phase, do the following:

1. Move the new system from Migration network to Production network.

- 2. Go to the Virtual Machines that compose the MX-ONE system and move them across.

Figure 62: Migrating MX-ONE 6.2 to Production Network



In the Virtualized system, this operation (migration part 1 and part 2) does not take more than two minutes, but that depends of the number of servers that are part of the solution. Practically, this took 1 minute and 10 seconds to migrate all 6 servers and the PC in the solution presented in this document.

Figure 63: MX-ONE 5.0 in the Shadow Network

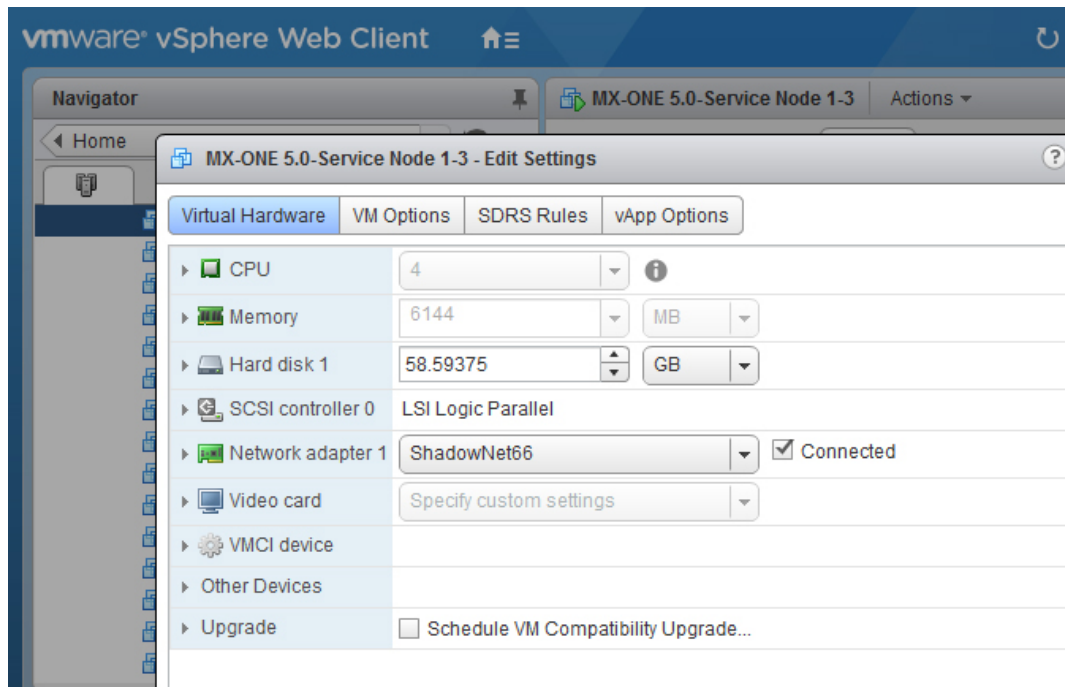
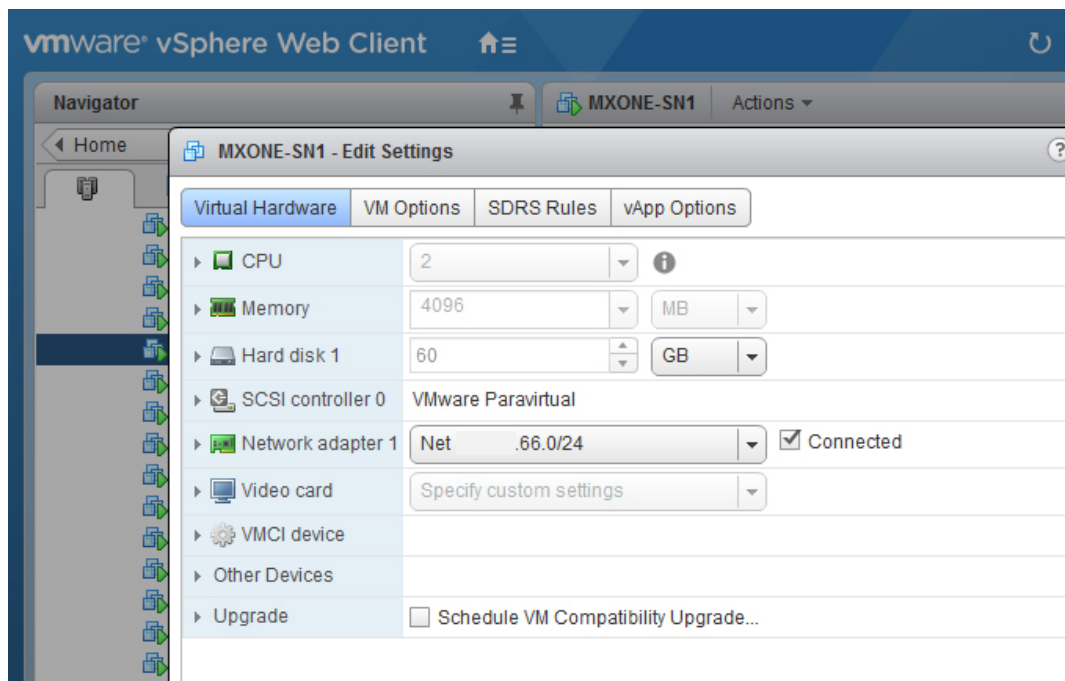
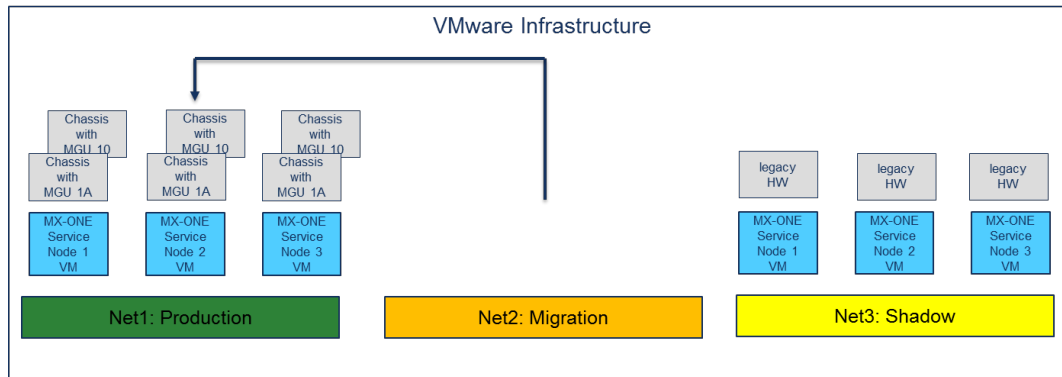


Figure 64: MX-ONE 6.2 in the Production Network



3. MX-ONE executes a data reload after the migration to the Production network is completed.

Figure 65: Environment After Migrating MX-ONE 6.X Networks



Down Time Phase

During the migration period down time occurs. The combined phase 1 and phase 2 duration is total time that MX-ONE system is out of service (no telephony service).

The total upgrade time in a customer when all the preparation was done in advanced can vary from a matter of 10 minutes to an hour for a centralized system with 1-10 servers on VMware, depending on size of MX-ONE system, number of MGUs involved and the number of SIP extensions.

Note:

It depends of the customer infrastructure and the numbers above are average.

4.6 Final Verification

The following process narrates about the final verification steps:

1. Execute all tests required in the new system.

- Verify that the MGUs (and associated end-points) are up and running and if all the SIP/IP extensions are moved to the new system.
- Verify that all application interfaces are reconnected to the new system and working as per normal - MiCollab AM (formerly One Box), MiContactCenter Enterprise, InAttend, MiCollab, and so on.

2. Maintain the old system in standby on the Shadow network until final acceptance date of the new system.
 - Keep the old system in the Shadow network for a particular time frame as customer wants.
 - In case of a serious cutover/failure or serious problems found with the new system, the Standby network brings back online with minimal downtime.
 - Once the acceptance phase is completed, this network is shut down and dismantled.
3. Perform backups in Service Node, Provisioning Manager, and Service Node Manager and transfer them to a safe place.
4. Keep all backup up to date.
5. Delete the old VMware snapshots, if they were created.

