MiVoice MX-ONE

Server Redundancy-Operational Directions

Release 7.3 SP2

March 16, 2021

Mitel®

Notice

Trademarks

Contents

General

This document describes server redundancy and how to configure it in MX-ONE. Server redundancy is achieved by adding one or more standby servers to the network. A standby server has the ability to take over the tasks of a faulty LIM server.

The document is intended for those who want to know more about the functionality as well as technicians that want to learn about certain procedures and specific behavior of the function.

What is Server Redundancy

Using server redundancy, a standby server can take over the tasks of a regular server suffering from, for example, hardware failure. This way, a faulty server can be replaced with a minimum of disturbance.

When using server redundancy, regular servers and an additional standby server are grouped as a cluster. The standby server is prepared with data from the regular servers in the cluster and ready to start an instance of any of these servers in case of a server fault.

To build a real fault tolerant cluster, network redundancy can be combined with server redundancy.

Figure 2.1: Server redundancy with Ethernet bonded network redundancy.

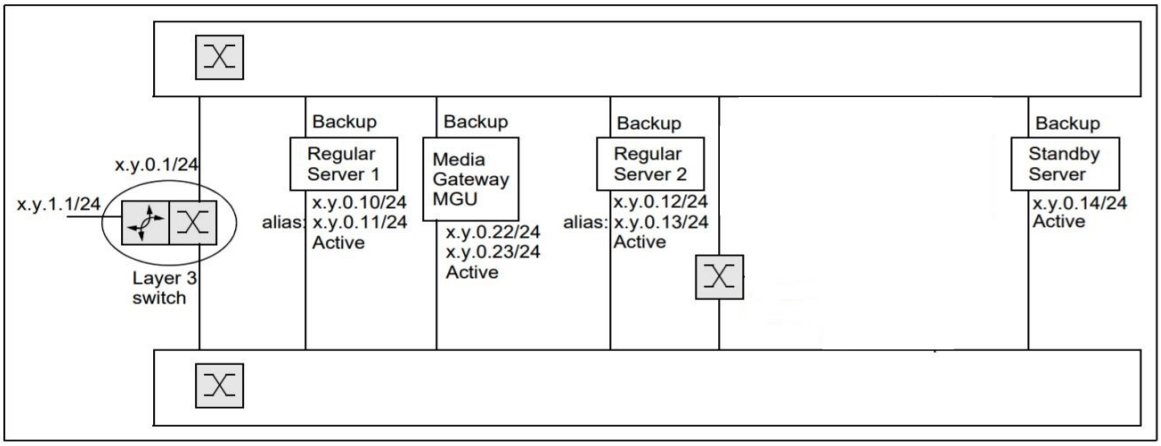
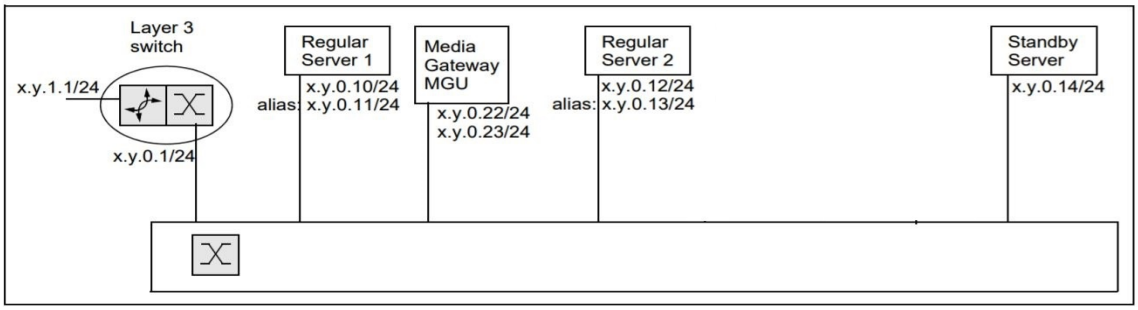


Figure 2.2: Server redundancy without network redundancy



Each server in a cluster supervises the state of the other servers. In case of a server failure or lost network connection with the regular server, the software running on the faulty regular server will be started on the standby server. The standby server will also manage the media gateways of the faulty regular server.

Particularly, when the network connection is lost, the regular as well as standby server will run the MX-ONE Service Node service. Subsequently when the network connection is restored and the regular server and the standby server detect each other running the MX-ONE Service Node service, the regular server will stop running the service. A preloaded cluster behaves as a non-preloaded cluster in this regard. Network redundancy reduce the likelihood of both servers running the service simultaneously.

If the Media Server is used, there are two different configurations, for the control the Media Gateway(s) of the failing LIM: if the MS is co-located with the (failing) Service Node, a new MS is started by the standby server. If the Media Server runs on a stand-alone server, the standby server will continue to control the separate Media Server of the failing LIM. When Media Server is co-located, both Control and

media interface must be set to the same address as the Service Node for the standby server to start the Media Server properly.

NOTE: If voice announcement functions are used, the announcement prompts must be made available (preloaded) in the standby Media Gateway.

If there are more than one faulty regular servers in a cluster, the standby server will only replace one of the faulty servers. Other faulty servers will not operate. Which of the faulty regular servers the standby server will replace depends on the regular servers priority to run on the standby server. If the priority is equal, the first regular server started on the standby server will continue running. If a server with higher priority to run on the standby server fails, while the standby server is already running a regular server, it will be replaced by the server with higher priority.

Each regular server in a cluster is configured with two addresses, a base IP address and an alias IP address. The standby server is configured with only a base IP address. In case of a faulty regular server, the standby server will take over the alias IP addresses of the faulty server.

When a regular server recovers from a failure, the MX-ONE Service Node programs running on the standby server can fallback to the regular server.

Two types of fallback exist:

- Manual fallback: A command has to be used to do the fallback to the regular server.
- Automatic fallback: The fallback will take place as soon as the regular server has recovered.

During fallback, the MX-ONE Service Node software is stopped on the regular and standby servers, and then started on the regular server.

If a cluster server finds another cluster server with the same alias address active, one of the servers will remove the alias address and stop running the telephony programs. Which server that will stop depends on configuration. Normally the regular server will be stopped and then the fallback is executed, either automatically or manually. By this measure the consequences of Split brain is avoided.

If the alias IP address is found in use by some other network equipment (none cluster server), it can result in that the LIM is not started. This is an example of faulty network configuration.

Handling of Server Data

The standby server is prepared with data from the regular servers in the cluster and is ready to start an instance of any faulty regular server within the cluster. Reload and system database data is copied from the regular servers in the cluster to the standby server after every data backup and once every 24-hour period.

For a correct data synchronization, the server's clock have to be in sync and NTP configured properly. This is normally configured during system installation. If manual adjustments of the clocks are performed make sure servers clock are in sync. The reload data files modification times are used to select data sync direction between regular and standby servers.

Preloaded Cluster

A standby server is preloaded with program and data to make failover faster. This is only possible for a cluster consisting of one regular server and one standby server.

In a preloaded cluster the alias address is started in both servers at the same time, but it is blocked in the Linux kernel in the passive side. If the regular server fails, the blocking of the alias address is removed and the standby server is functional.

The passive side is updated with reload and system database data from the active side when the data_backup command is used on the active side. A data reload is then executed automatically in the passive side to prepare it for failover.

The time to detect a server as failed is lower in a preloaded cluster than in a regular cluster, 30 seconds.

A shorter fail detection time increases the risk for faulty detection of server failure. This puts higher requirements on the cluster servers and networks. Ensure that the cluster is configured with high performance servers. Use network and storage with enough bandwidth. Use of Network redundancy is recommended.

Failover or fallback can occur to a server (LIM) that is currently loading, but has not yet reached the preloaded state. If this happens the time to recover will be longer than with a server that has reached the preloaded state.

Using automatic fallback for instance, if the regular server is reloaded, fallback will occur as soon as the two servers have found each other. This will happen while the regular server (LIM) is still loading. The traffic disturbance at recovery using automatic fallback is in this case longer than if manual fallback is used. The manual fallback can be ordered when the reloaded server has reached the preloaded state. Manual fallback is a better alternative for preloaded clusters.

Glossary

ARP

Address Resolution Protocol. Used to find out on what hardware address (MAC) an IPv4 address is used.

Alias IP address

An alias IP address tied to a specific network interface. IP aliasing is the process of adding more than one IP address to a network interface.

Base IP address

The normal IP address for a network interface.

Cluster

A number of regular servers and a standby server are grouped together in a cluster.

CSTA

Computer Supported Telecommunication Applications.

Data backup

Exchange data are stored on disk by doing a data backup.

Gratuitous ARP

An ARP announcement of a MAC and IP address combination.

HLR redundancy

The HLR backup or redundancy feature in MX-ONE. It provides a possibility for H.323 and SIP extensions, on certain conditions, to temporarily register to a backup HLR in another server instead of to the regular HLR server.

LIM

Line Interface Module, an MX-ONE Service Node plus at least one media gateway.

MS

Media Server, a “software based” media gateway, in this context for use in the MX-ONE.

Network redundancy

The network redundancy used with MX-ONE is switched network redundancy with Ethernet bonding for the Service Nodes.

NTP

Network Time Protocol.

Regular server

A Service Node server where a LIM normally is running.

Standby server

A server that can take over for a faulty regular server.

Prerequisites

The following requirements and limitations apply for installations using server redundancy:

- A cluster can have up to ten LIMs.
- A cluster can have only one standby server.
- It is possible to have as many clusters as there are LIMs in the system (with a maximum of one standby server per LIM server).
- A standby server can belong to only one cluster.
- A LIM server can belong to only one cluster.
- All servers in a cluster must reside on the same subnet. Gratuitous ARP is used in the network to announce that a standby server has taken over the alias IP address of a faulty regular server. (ARP is a link layer protocol, operating on the local subnet.)
- The Alias IP address must be on the same subnet as the base IP address.
- A standby server must have performance enough to be able to replace any regular server in the cluster.
- A standby server must have enough free hard disk space to store two data backups (system database data included) of each regular server in the cluster.
- There must be enough bandwidth within a cluster for efficient transfer of data backups to the standby server.
- Failover behavior preloaded is used only for clusters consisting of one regular and one standby server.

Known Limitations of the Server Redundancy Functionality

Automatic Fallback

After a server failure using automatic fallback to the regular server, fallback will take place when the server is functioning again. This can create problems if the regular server starts and stops repeatedly during a short period of time

Several Regular Servers Failing at the Same Time

If there are more than one faulty regular servers in a cluster, the standby server will only replace one of the faulty servers. Other faulty servers will not operate. Which of the faulty regular servers the standby server will replace depends on the regular servers priority to run on the standby server. If they have equal priority the first started on the standby server will continue to run. Only servers with higher priority will replace an already running server

Limitations When a LIM is Running on the Standby Server

The management system, running on the primary server, is not started on the standby server.

The CSTA Phase III Web Service Application function, possibly running on the primary server, is not started on the standby server.

Other Considerations

When to use Base or Alias IP Addresses

The base IP address of a server in a cluster is used for connecting to applications on the specific server.

The alias IP address of a server in a cluster is used for applications moved between regular and standby server

For more information on when to use base and alias addresses, see the installation instructions for *INSTALLING AND CONFIGURING MIVOICE MX-ONE*.

ARP Consideration

For IPv4 Gratuitous ARP is used to update ARP caches when an alias IP address is moved between a regular server and the standby server. Routers and switches have to be configured to accept Gratuitous ARP.

If Gratuitous ARP is not accepted, the failover time will equal the ARP cache timeout time, which is normally not acceptable.

To prevent too long delay in the failover, the ARP cache timeout time should not be too long. Gratuitous ARP is sent periodically to make sure network caches are updated.

Use LIM Locking at User Controlled Server Reboot

Locking the LIM to regular server is recommended before doing user controlled server reboot, especially in clusters configured for manual fall-back. This will keep the LIM on the regular server when the reboot is completed. Do not forget to unlock the LIM when the reboot is done.

Aids

-

References

-

Procedure

Configuring and Using Server Redundancy

Cluster configuration is performed after system installation. It can be executed in a running system, preferable in low traffic time.

Every regular LIM server needs an extra IP address in the cluster. This address, which is entered during cluster configuration, will become the new base address. The old base address will be used as alias address. This trick will remove the need for restarts during configuration.

The cluster configuration are performed using the MX-ONE Maintenance Utility.Log-in as user **mxone_admin**, and run the `sudo -H /opt/mxone_install/bin/mxone_maintenance` command and select **Cluster handling**.

The following actions are possible:

- List all clusters
- Show status
- Create new cluster in system
- Change fallback type or priority
- Change failover behavior to preloaded
- Add a LIM to existing cluster
- Remove a LIM from existing cluster
- Delete cluster in system
- Move LIM from standby to regular server
- Lock LIM to server
- Unlock LIM from server
- Sync exchange data within cluster

Some of the actions listed above will remove old xdata-versions (reload and system database data) that are incompatible with current configuration.

After these actions only one xdata-version exist:

- Create new cluster in system
- Change fallback type or priority
- Change failover behavior to preloaded
- Add a LIM to existing cluster
- Remove a LIM from existing cluster
- Delete cluster in system

Installing PM/SNM Redundancy

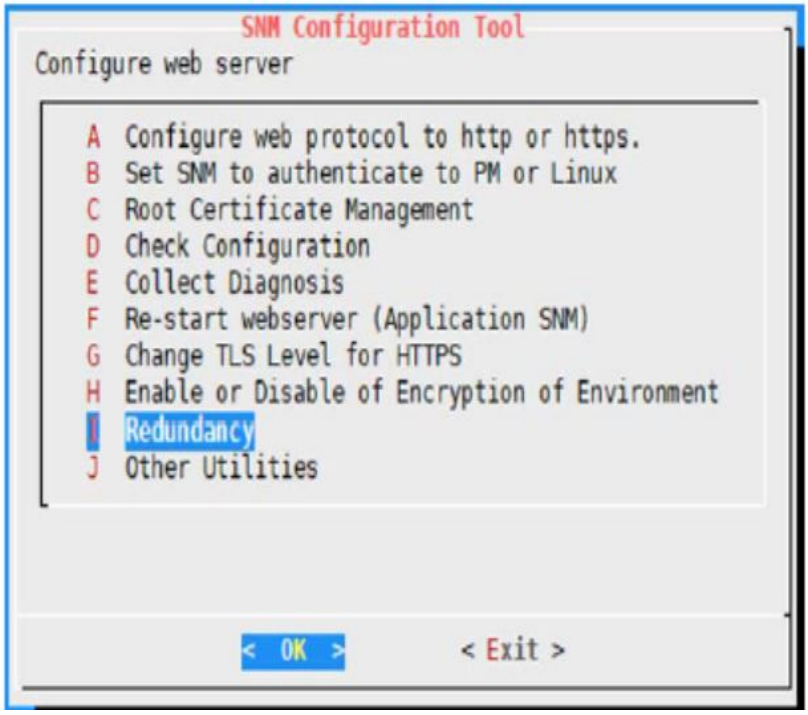
Master Configuration

1. Ensure SN redundancy is set, before PM/SNM redundancy set up is started.
2. Login into the Master server and execute the `webserver_config` command.
3. Select **Redundancy** from the **Configure web server** list

   NOTE: This option is available only if Lim1 is in cluster) shown in the following screen.

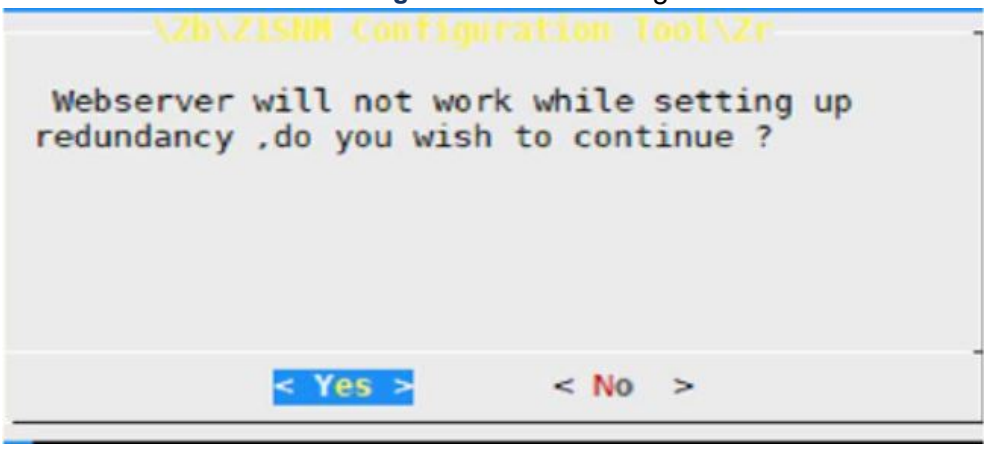
   Follow the below steps to set up Redundancy in Master Server for PM/SNM after execution of the `webserver_config` command.

Figure 9.1: Redundancy



4. Select **Yes** to continue. After you select **Yes**, the system itself finds Master Standby and Cluster IPs.

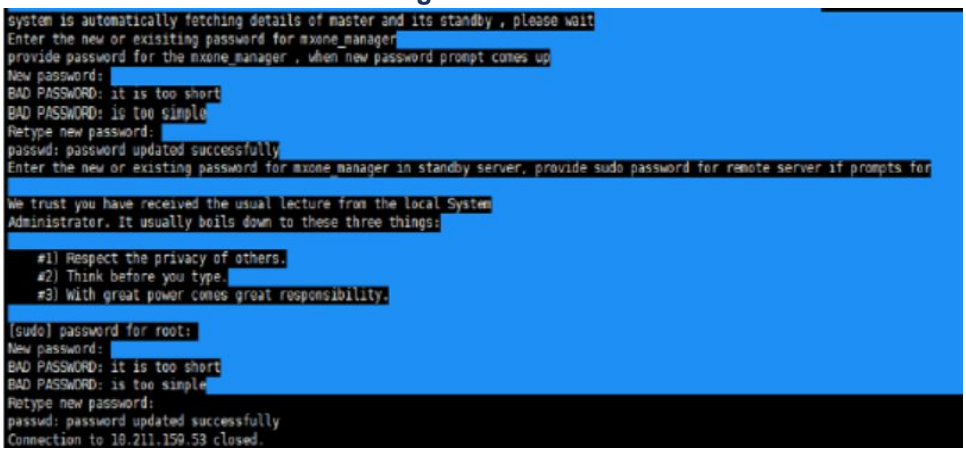
Figure 9.2: SNM Configuration



5. Select **Yes** to continue after the **Redundancy** option is selected
6. Set password for mxone_manager user both in Master and Standby server.
7. Confirm the password that is set for mxone_manager that allows you to login to Standby server.
8. Enter the **sudo** password of Standby server.

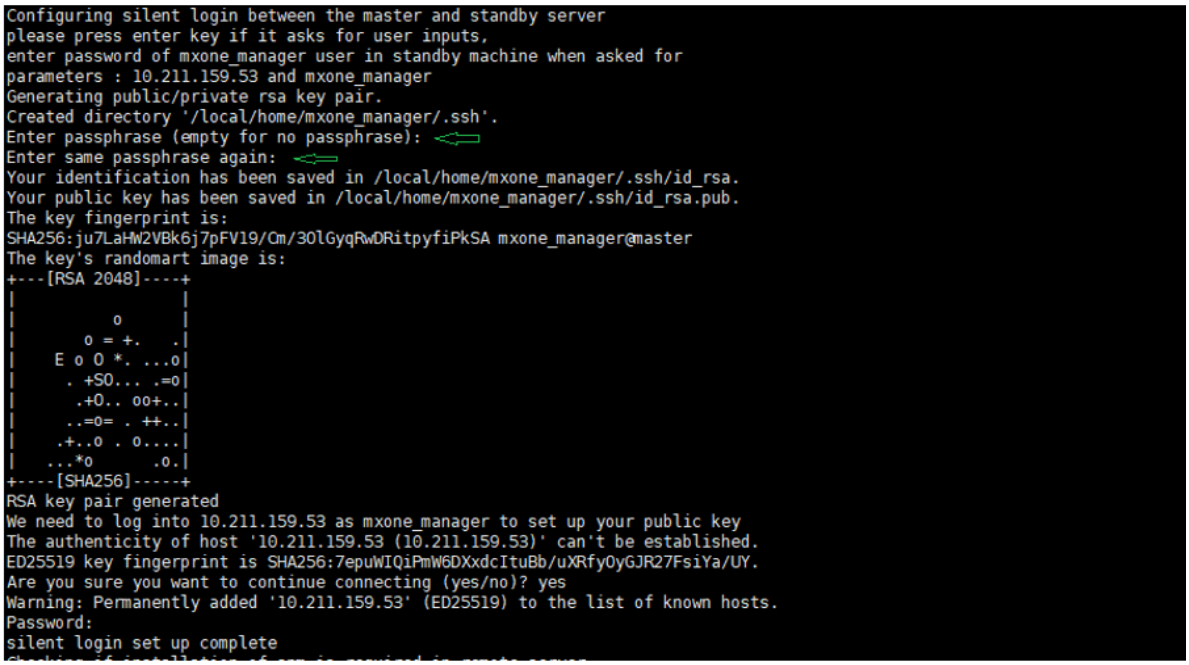
   The following screenshot describes about the above mentioned steps (6,7,8) and note that 10.211.159.53 is IP of the standby server.

Figure 9.3: Password Set



9. Once password for mxone_manager is set in both Master and Standby server, silent login between master and standby servers is set.
10. Press **Enter** key when it asks for passphrase (shown as green arrow in the following screenshot)

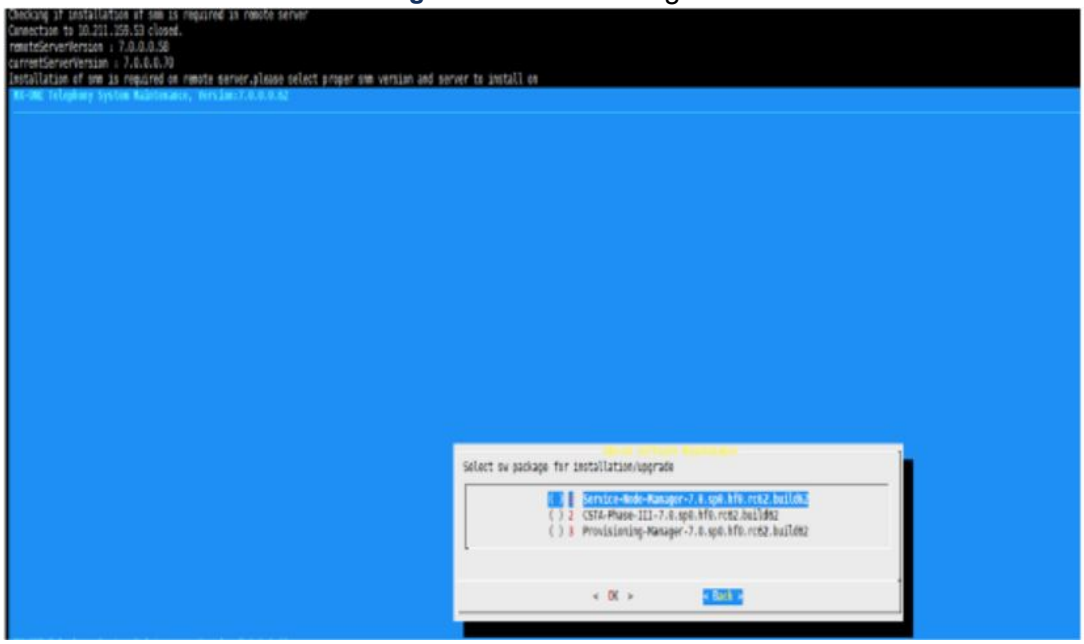
Figure 9.4: Silent Login Setup



11. Enter password for mxone_manager user in Standby server, which completes silent login to Standby from Master server.

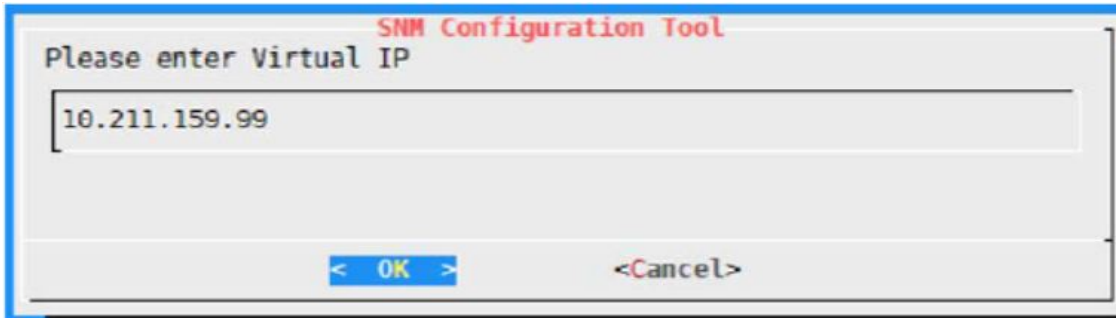
12. System checks if SNM is installed in standby server; if not installed, it shows a pop-up to select and install the same (SNM).
13. In case of co-existing system, ensure that PM is installed both in Master and Standby server in this step. The following screenshot describes about the step 12 and 13.

Figure 9.5: SW Package Installation



14. Enter **Virtual IP** (common IP, which re-routes itself to corresponding active server at any point of time).

Figure 9.6: Virtual IP



NOTE: You can enter the Alias IP address, however make sure you **DO NOT** use the Alias IP address that is currently in use by the redundancy server. Doing so will result in re-installation of the entire system.

15. Enter username and password for creating a replication role for postgres as shown below. Ensure that the same username and password for the replication role is provided when setting UP Standby server.

Figure 9.7: User Name for Replication Role

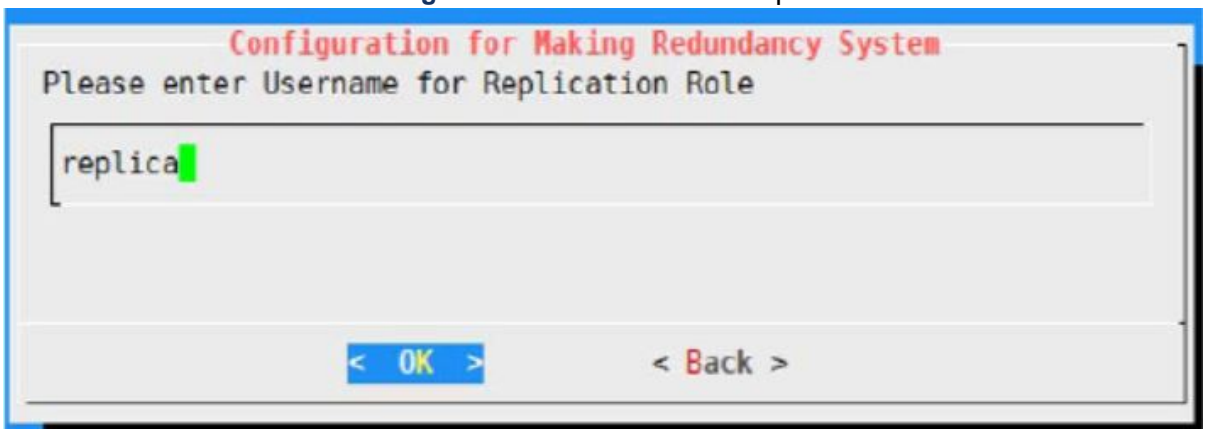
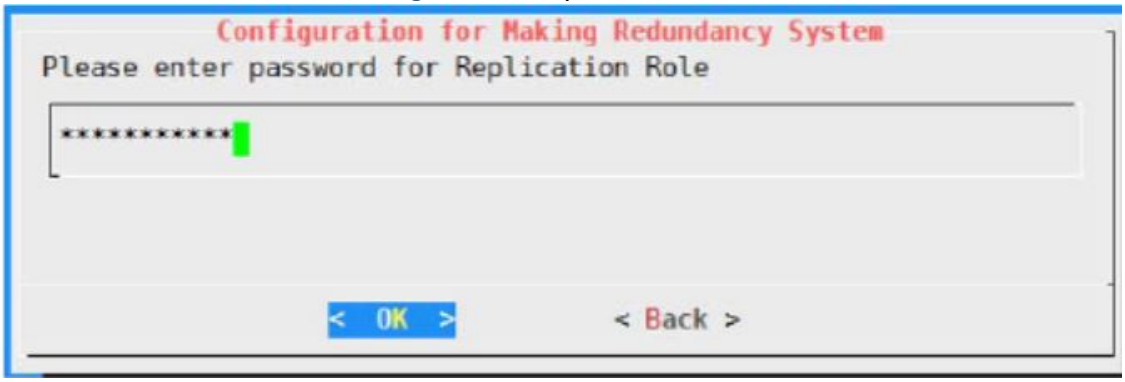


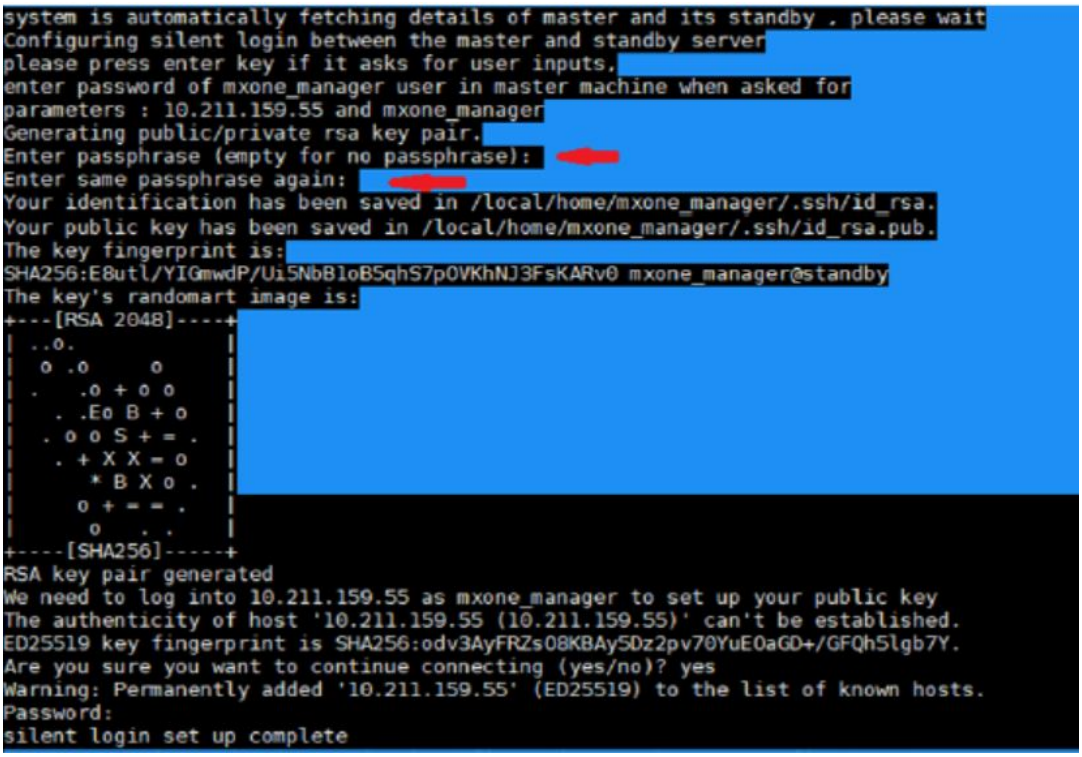
Figure 9.8: Replication Role Password



Standby Configuration

1. Ensure that SN redundancy is set, before PM/SNM redundancy set up is started. Follow the below steps for setting up Standby server.
2. Execute `webserver_config` and select **Redundancy** as is done in master server. System automatically fetches master and standby details.
3. To setup silent login of Standby to Master server, press **Enter** wherever red arrow is highlighted as shown in the following screenshot:

Figure 9.9: Silent Login of Standby Configuration



4. Enter the **Virtual IP** and **Replication role** details that were given while configuring the Master server.

Figure 9.10: Standby Virtual IP Configuration

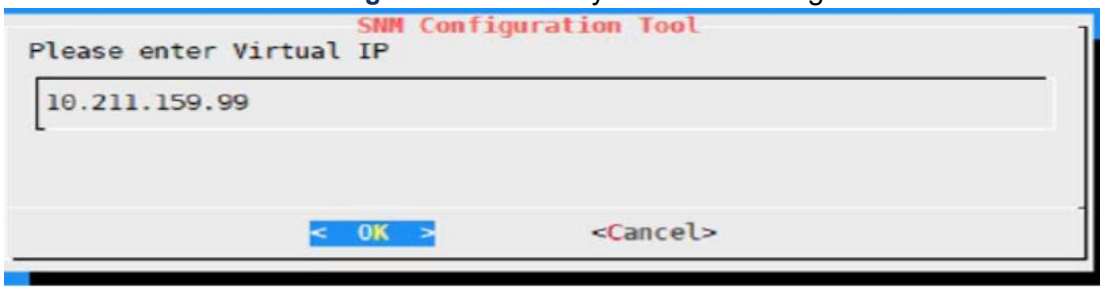


Figure 9.11: Standby Replication Role User Name

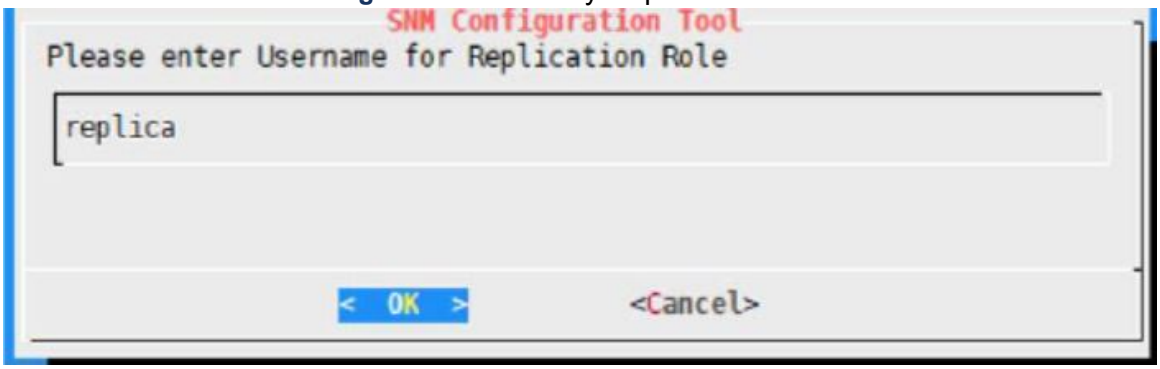
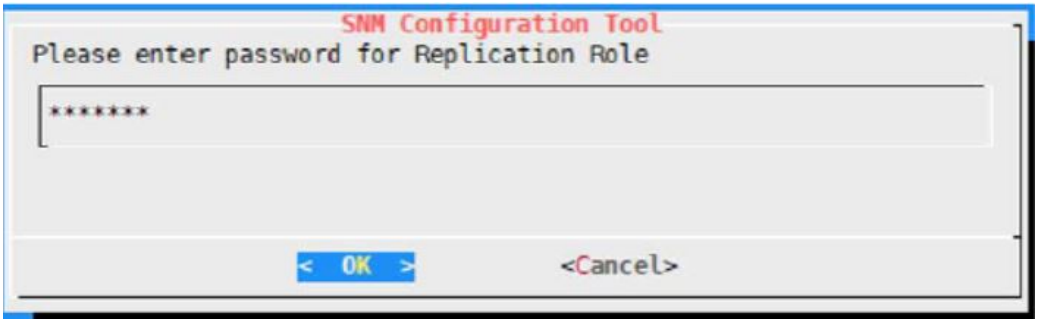
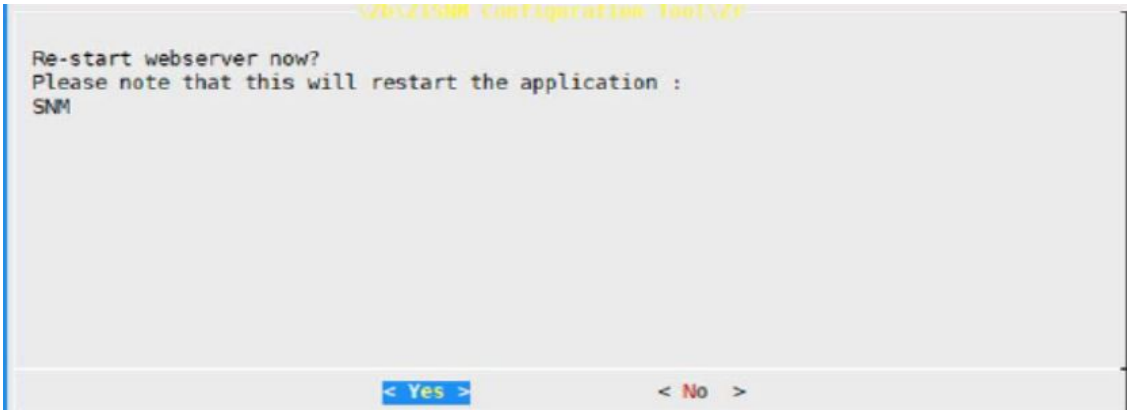


Figure 9.12: Standby Replication Role Password



5. Press **Yes** to restart the webserver.

Figure 9.13: Webserver Restart

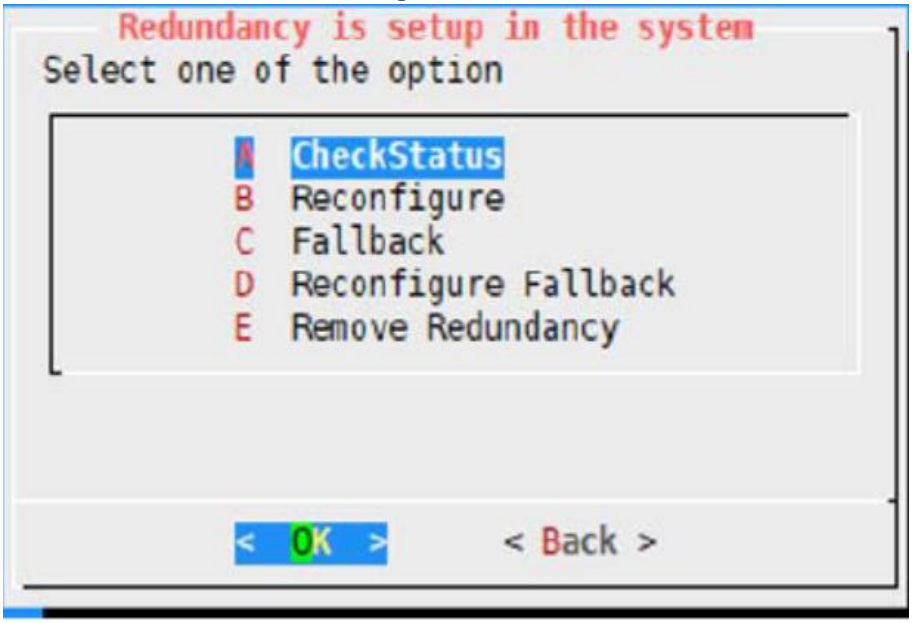


6. Enter the following URL to access the current active server type: **http:Virtual_IP>/mp or http:Virtual_IP>/wbm**.

Utilities While Redundancy is Set

1. To access other utilities related to redundancy after redundancy is set, execute `webserver_config` and then select Redundancy, the following screen is displayed:

Figure 9.14: CheckStatus

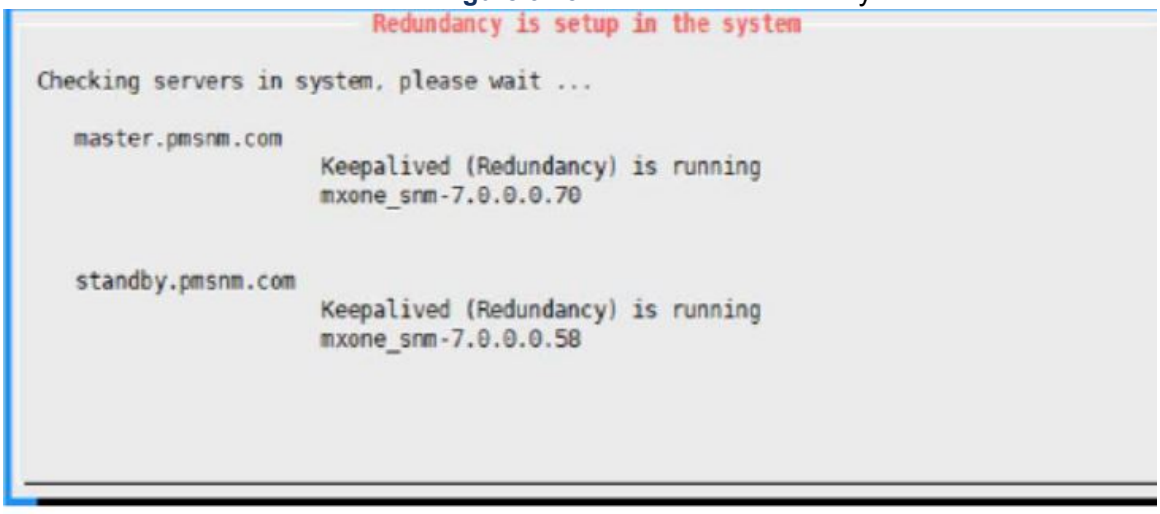


The following options describe about the Redundancy Setup process:

a. CheckStatus

Shows the status of redundancy as shown below.

Figure 9.15: Status of redundancy



b. Reconfigure

Reconfiguring of redundancy can be used if it is required to re-configure the set-up. Ensure that it is executed in Master first, and then followed by Standby.

c. Fallback

If fallback type is Manual, once Master server comes up/ready, SN falls back to Master, and then we need to login to master server and then you select this option; so that, PM/SNM redundancy is also fall back to Master.

d. Reconfigure Fallback

If fallback type of cluster is changed, the same must be done in PM/SNM side to login to Master server. Select this option to set the fallback that is same as the cluster fallback type.

e. Remove Redundancy

To remove the PM/SNM redundancy, select this option to ensure that it is removed in Master first and then followed by Standby.

Considerations and Limitations

The following are the considerations and limitations in PM/SNM redundancy:

1. `webserver_config` functionalities like protocol changes, authentication changes, certificate changes must be done separately in active and Standby server.
2. Few of the UI functionalities, which store files in server are not replicated to Standby and vice-versa, like database backup from GUI, and so on.

Execution

Add a Cluster

1. Install new server.
   For detailed information, see *INSTALLING AND CONFIGURING MIVOICE MX-ONE*.
2. On LIM 1 log in as user **mxone_admin**.
3. Run the `sudo -H /opt/mxone_install/bin/mxone_maintenance` command to start MX-ONE Maintenance Utility.
4. Select **Server in system** to add a new server to system.

   Follow the procedure as instructed on screen.
5. Select **Standby server in system** to convert free server to standby server.

   Follow the procedure as instructed on screen.
6. Select **Cluster handling** to create a new cluster in system.

Follow the procedure as instructed on screen.

Remove a Cluster

1. On LIM 1 log in as user **mxone_admin**.
2. Run the `sudo -H /opt/mxone_install/bin/mxone_maintenance` command to start MX-ONE Mainte-nance Utility.
3. Select **Cluster handling** to delete cluster in system.

   Follow the procedure as instructed on screen.
4. Select **Standby server in system** to convert standby server to free server.

   Follow the procedure as instructed on screen.
5. Select **Server in system** to remove server to system.

Follow the procedure as instructed on screen.

Add a LIM to a Cluster

A LIM can be added to a cluster. An additional IP address has to be entered. This IP address will be the new base address for the interface. Use utility: **/opt/mxone_in-stall/bin/mxone_maintenance** > **cluster** > **add**.

1. On LIM 1 log in as user **mxone_admin**.
2. Run the `sudo -H /opt/mxone_install/bin/mxone_maintenance` command to start MX-ONE Mainte-nance Utility.
3. Select **Cluster handling** to add lim to existing cluster.

Follow the procedure as instructed on screen.

Remove a LIM from a Cluster

A LIM can be removed from a cluster. If the last LIM in the cluster is removed, the complete cluster will be removed.

1. On LIM 1 log in as user **mxone_admin**.
2. Run the `sudo -H /opt/mxone_install/bin/mxone_maintenance` command to start MX-ONE Maintenance Utility.
3. Select **Cluster handling** to remove lim to existing cluster.

Follow the procedure as instructed on screen.

Print Cluster Status

1. On LIM 1 log in as user **mxone_admin**.
2. Run the `sudo -H /opt/mxone_install/bin/mxone_maintenance` command to start MX-ONE Maintenance Utility.
3. Select **Cluster handling** to show status of all clusters.

Print Cluster Configuration

1. On LIM 1 log in as user **mxone_admin**.
2. Run the `sudo -H /opt/mxone_install/bin/mxone_maintenance` command to start MX-ONE Mainte-nance Utility.
3. Select **Cluster handling** to list all clusters .

Change Fallback Type and LIM

The fallback type and the LIM priority to run on the standby server can be changed.

Fallback type can be automatic or manual

A lower priority value, gives higher priority to run on the standby server.

1. On LIM 1 log in as user **mxone_admin**.
2. Run the `sudo -H /opt/mxone_install/bin/mxone_maintenance` command to start MX-ONE Mainte-nance Utility.
3. Select **Cluster handling** to change fallback type or priority.

Change Failover Behaviour to Preloaded

A cluster consisting of one regular and one standby server is configured and preloaded.

To remove preloading, cluster must be removed.

1. On LIM 1 log in as user **mxone_admin**.
2. Run the `sudo -H /opt/mxone_install/bin/mxone_maintenance` command to start MX-ONE Mainte-nance Utility.
3. Select **Cluster handling** to change failover behavior to preloaded.

Execute Manual Fallback to Regular Server

1. On LIM 1 log in as user **mxone_admin**.
2. Execute the `sudo -H /opt/mxone_install/bin/mxone_maintenance` command to start MX-ONE Maintenance Utility.
3. Select **Cluster handling** to change failover behavior to get preloaded.

Execute a Manual Ordered Synch of Data

1. On LIM 1 log in as user **mxone_admin**.
2. Execute the `sudo -H /opt/mxone_install/bin/mxone_maintenance` command to start MX-ONE Maintenance Utility.
3. Select **Cluster handling** to synch exchange data within clust

Lock or Unlock a LIM to a Specific Server

A LIM can be locked to a regular server or a standby server to prevent failover.

When a LIM is unlocked from a server, failover actions can occur again.

If a LIM locked to the standby is unlocked, the clusters configured fallback type deter-mines what will happen. With automatic fallback, the LIM will fallback to regular server (if it is functional). With manual fallback the user has to manually order the fallback.

1. On LIM 1 log in as user **mxone_admin**.
2. Execute the `sudo -H /opt/mxone_install/bin/mxone_maintenance` command to start MX-ONE Maintenance Utility.
3. Select **Cluster handling** either to lock lim to the server or to unlock lim from server.

Alarms

This chapter describes MX-ONE alarms related to server redundancy.

LIM is Running on Standby Server

This alarm is received when a LIM is running on the standby server.

The alarm indicates that a regular server has a network problem, faulty hardware, or is rebooting. If the fault is of a more serious character, manual measures might be needed.

If the alarms are seen on the standby server, then it is a normal behavior for pre-loaded standby. In such server the Service Node is running, but the services are blocked in the firewall from accessing the network.

As this is the standby server, then it generates the alarm that the LIM runs on standby. The same alarm will remain once the regular is off and the standby becomes real active. Also, the alarms for no contact with media gateway, no contacts with other LIMs, common functions out of order are *normal* for pre-loaded, because this LIM can be seen as isolated from the rest of the infrastructure.

Standby Server is Out of Order

This alarm is received when contact with a standby server is lost.

The alarm indicates that the standby server has a network problem, faulty hardware, or is rebooting. If the fault is of a more serious character, manual measures might be needed.

Standby Cluster has Failed to Synchronize Data

This alarm is received when a standby server has failed to synchronize exchange data with the regular servers in a cluster.

Termination

-