HITACHI
Inspire the Next

USER MANUAL

FOXMAN-UN
Main/Standby Solution

Hitachi Energy

Document ID	1KHW029097	
Document edition	System Release:	R18
	Revision:	A
	Date:	2025-10-10

Copyright and confidentiality

Disclaimer

This document contains information about one or more Hitachi Energy products and may include a description of or a reference to one or more standards that may be generally relevant to the Hitachi Energy products. The presence of any such description of a standard or reference to a standard is not a representation that all the Hitachi Energy products referenced in this document support all the features of the described or referenced standard. In order to determine the specific features supported by a particular Hitachi Energy product, the reader should consult the product specifications for that Hitachi Energy product. In no event shall Hitachi Energy be liable for direct, indirect, special, incidental, or consequential damages of any nature or kind arising from the use of this document, nor shall Hitachi Energy be liable for incidental or consequential damages arising from the use of any software or hardware described in this document.
Hitachi Energy may have one or more patents or pending patent applications protecting the intellectual property in the Hitachi Energy products described in this document. The information in this document is subject to change without notice and should not be construed as a commitment by Hitachi Energy. Hitachi Energy assumes no responsibility for any errors that may appear in this document.
All people responsible for applying the equipment addressed in this manual must satisfy themselves that each intended application is suitable and acceptable, including compliance with any applicable safety or other operational requirements. Any risks in applications where a system failure and/or product failure would create a risk for harm to property or persons (including but not limited to personal injuries or death) shall be the sole responsibility of the person or entity applying the equipment, and those so responsible are hereby requested to ensure that all measures are taken to exclude or mitigate such risks.
Products described or referenced in this document are designed to be connected and to communicate information and data through network interfaces, which should be connected to a secure network. It is the sole responsibility of the system/product owner to provide and continuously ensure a secure connection between the product and the system network and/or any other networks that may be connected.
The system/product owners must establish and maintain appropriate measures, including, but not limited to, the installation of firewalls, application of authentication measures, encryption of data, installation of antivirus programs, and so on, to protect these products, the network, its system, and interfaces against security breaches, unauthorized access, interference, intrusion, leakage, and/or theft of data or information.
Hitachi Energy performs functionality testing on released products and updates. However, system/product owners are ultimately responsible for ensuring that any product updates or other major system updates (to include but not limited to code changes, configuration file changes, third-party software updates or patches, hardware change out, and so on) are compatible with the security measures implemented. The system/product owners must verify that the system and associated products function as expected in the environment in which they are deployed. Hitachi Energy and its affiliates are not liable for damages and/or losses related to security breaches, any unauthorized access, interference, intrusion, leakage, and/or theft of data or information.
This document and parts thereof must not be reproduced or copied without written permission from Hitachi Energy, and the contents thereof must not be imparted to a third party nor used for any unauthorized purpose.

Contents

1 Preface

1.1 Conventions Used

References made in the text may refer to sections in this document or to other material. The following convention is used:

- References to other sections of this manual are given by hyperlinks with chapter or section title and optional chapter and section numbers.
- References to other documents use square brackets [ ] with the referred document number.

2 Introduction

2.1 Overview

This document describes the FOXMAN-UN Main/Standby Solution. It is divided into the following chapters:

- Introduction,
- Installation,
- Mode of Operation,
- Setup and Operation,
- Configuration,
- Troubleshooting,
- Important Notes,
- Document History.

2.2 Terms and Abbreviations

- Standard Server

  A FOXMAN-UN machine that is not configured to use the Main/Standby Solution.
- Main Server

  A FOXMAN-UN machine that is configured to make use of the Main/Standby Solution and is configured to act as a Main Server (which runs under normal circumstances).
- Standby Server

  A FOXMAN-UN machine that is configured to make use of the Main/Standby Solution and is configured to act as a Standby Server (which runs under the circumstances that the Main Server is broken).
- Cold Standby Server

  A Standby Server that is ready to be activated by an operator in case of Main Server breakdown.
- Warm Standby Server

  A Standby Server that is automatically activated in case of Main Server breakdown.
- Partner Server

  Main and Standby Server always build a pair of two. Thus, a Standby Server acts as Partner Server of its assigned Main Server and vice versa. A Main Server can have more than one Standby Server as a partner, but a Standby Server can always only have one Main Server as a partner (one to many relationship).
- Local Client

  A FOXMAN-UN Client that comes installed together with a FOXMAN-UN Server. Thus, both Server and Client are running on the same physical machine.
- Remote Client

  A FOXMAN-UN Client that is installed without a FOXMAN-UN Server. Thus, the Client is running remote of the FOXMAN-UN Server.
- NEM Base Services

  A number of FOXMAN-UN services (Linux services) providing a base service infrastructure needed by superordinate FOXMAN-UN services.
- NEM Core Services

  A number of FOXMAN-UN services (Linux services) providing a higher-level application infrastructure. NEM core services can only be executed if NEM base services are already running.

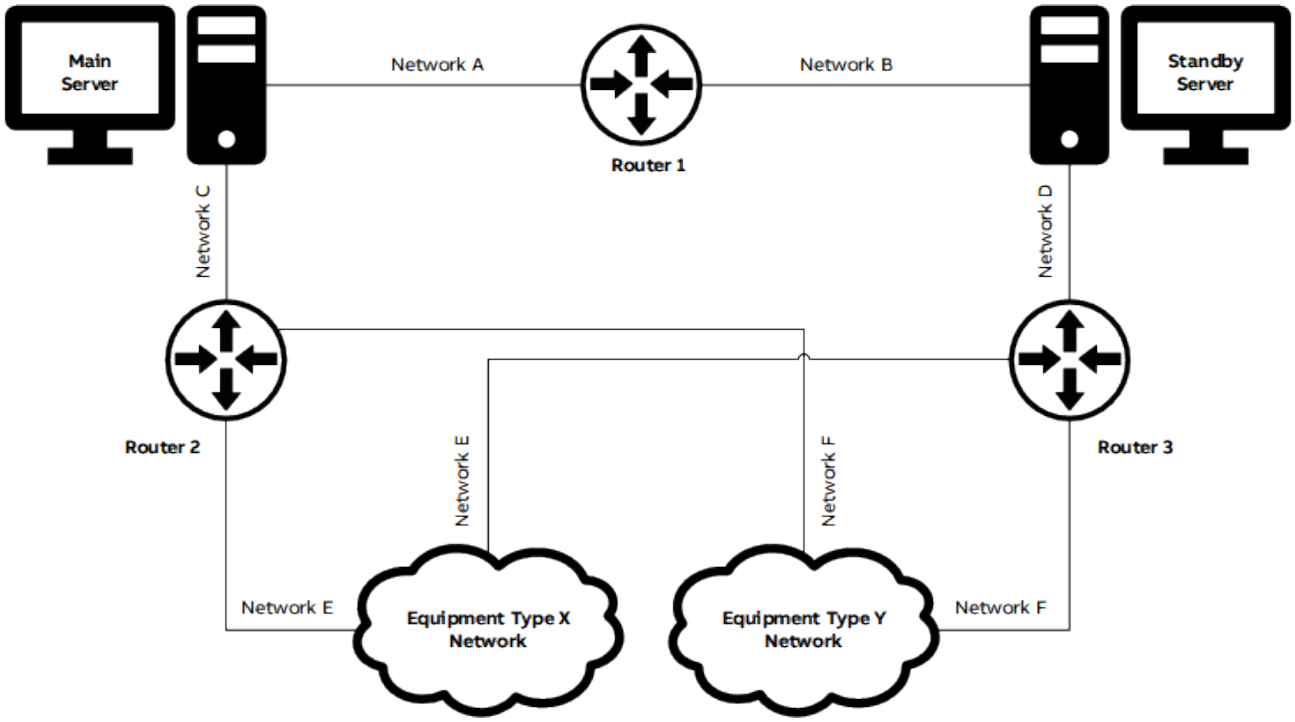
3 Installation

The Main/Standby software package is included in the FOXMAN-UN software delivery pack and works only if a license is issued and activated.

Please follow the FOXMAN-UN installation guide for more information on how to install and set up the FOXMAN-UN server.

3.1 Network Setup

A typical Network Setup for the Main/Standby Solution in operation looks as explained in the following diagram:



In the above network scheme, the following applies:

- Equipment Type X: SNMP managed devices
- Equipment Type Y: non SNMP managed devices; note that the FOXMAN-UN does always register in the node when the agent is started.
- The Main Server must be connected to the Standby Server through the DCN network.
- Both the Main Server and the Standby Server need network connectivity to the network elements they are monitoring.
- The Equipment Type X and Y Agents of the Main Server must be configured to use IP Addresses of Network C.
- The Equipment Type X and Y Agents of the Standby Server must be configured to use IP Addresses of Network D.
- Equipment of Type X must be configured to send notifications (e.g. SNMP traps) to both Equipment Type X Agents on the Main and the Standby Server addressing the Agent IP Address of Network C in case of the Main Server and the Agent IP Address of Network D in case of the Standby Server.
- Equipment of Type Y must be configured to send notifications (e.g. SNMP traps) to both Equipment Type Y Agents on the Main and the Standby Server addressing the Agent IP Address of Network C in case of the Main Server and the Agent IP Address of Network D in case of the Standby Server.

3.2 Components

The Main/Standby Solution consists of the following basic components:

- Main/Standby Services

  A number of Linux Services which keep Main and Standby Server data synchronized.

- NEM Remote Admin Tool (RAT)

  A Graphical User Interface which servesconfiguration, supervision and control of the Main/Standby Solution.

Moreover, it also affects the following established FOXMAN-UN components:

- NEM Login Window

  Displaying additional information whether a Server is a Standard, Main or a Standby Server and whether this Server is in “Not running”, “Standby” or “Running” state.

- NEM Host Manager

  Displaying additional information whether a Server is a Standard, Main or a Standby Server and whether this Server is in “Not running”, “Standby” or “Running” state. It also shows the corresponding Partner Server of a Main or a Standby Sever.

- NEM Desktop

  Displaying additional information in the “connected to field” whether the client is currently connected to a Standard, Main or a Standby Server.

- FOXMAN-UN Alarm and Event List

  Displaying alarms and events which are related to theoperation of the Main/Standby Solution.

4 Mode of Operation

4.1 Server States

The operating system and the services of a FOXMAN-UN server can be in different states. In the FOXMAN-UN context these states will be mapped to so called Server States depending on whether a FOXMAN-UN server is of type Standard, Main or Standby. The possible Server States are listed in the following table:

FOXMAN-UN Services State	State of Standard Server	State of Main Server	State of Standby Server	Remark
Operating System (Linux) not running	No Connection	No Connection	No Connection	
Operating System (Linux) restarting	No Connection	No Connection	No Connection	In case of a Main or a Standby Server, restarting the OS will result in started up Base Services and not started up Cores Services. In case of a Standard Server, restarting the OS will result in started up Base and Core Services.
Base Services not running	No Connection	No Connection	No Connection	
Base Services restarting	No Connection	No Connection	No Connection	Restarting the base services will also restart the core services (if they are running).
Base Services running and Core Services not running	Not Running	Not Running	Standby	
Core Services stopping	Stopping	Stopping	Stopping	
Core Services starting	Starting	Starting	Starting	
Core Services restarting	Restarting	Restarting	Restarting	
Base and Core Services running	Running	Running	Running	Core Services can only be running if also base services are running.

4.2 Normal operation (Main Server running / Standby Server standby)

The basic concept of the Main/Standby Solution is that the Standby Server takes the role of the running server in case the Main Server breaks down. In normal operation mode the Main Server is in “Running” state and manages a network of equipment. “Running” state signifies that all FOXMAN-UN base services and all FOXMAN-UN core services are running. In normal operation mode the Standby Server is in “Standby” state. “Standby” state signifies that all FOXMAN-UN base services are running but no FOXMAN-UN core services are running. Both Servers periodically do a backup of the following information:

- FOXMAN-UN Database,
- DIRAC database (if DIRAC server is installed),
- ALS Database (if ALS is installed).

The Standby Server is waiting to take over network management in case of a Main Server breakdown. Thereto it periodically polls the Main Server for new database backups and, if available, transfers them to itself. Immediately after the transfer has occurred the backups will be imported to the corresponding databases on the Standby Server. Server-specific information such as e.g. equipment agent IP addresses will be exchanged during import. Now the Standby Server is ready to take over network management in case of a Main Server breakdown.

4.3 Main Server breakdown

The Standby Server deems the Main Server to be broken down in the following cases:

- Main Server core services not running (state: “Not running”);
- Main Server base services not running (state: “No connection”);
- No IP connectivity to the Main Server (state: “No connection”).

To detect those breakdown conditions the Standby Server periodically pings the Main Server. If the ping-reply either equals to state “Not running” or state “No connection” the Standby Server will do the following depending on its type:

- nothing in case it is configured as Cold Standby Server;
- start up its core services in case it is configured as Warm Standby Server.

If the Main Server breaks down, any FOXMAN-UN client (local or remote client) connected to it will lose its connection. Thus, the operator becomes aware that there is a problem with the Main Server. Now they can connect to the Standby Server to continue managing the network. In case the Standby Server is of type “Cold Standby Server” they afore need to start up the core services on the latter manually.

4.4 Connection loss of Main to Standby Server

A special situation occurs when the Main Server in normal operation (base and core services running) loses connection to the Standby Server for the reason of a broken network cable or a broken network interface card as an example. Then the Main Server will raise a “Standby Server is not reachable” alarm and event (if configured). If the Standby Server is of type “Warm Standby Server” it will automatically start up its core services and raise a “Main Server is not reachable” alarm and event (if configured). Once the connection problem is fixed and core services on both servers are still running, each server will raise a “Main Server and Standby Server running both at the same time” alarm and event (if configured).

4.5 Exceptional operation (Main Server not running / Standby Server running)

During exceptional operation the Standby Server is in “Running” state (base and core services running) and an arbitrary number of FOXMAN-UN clients might be connected to the server. The Main Server on the other hand is in another state than “Running” state. During this phase typically, the problem on the Main Server can be located and fixed.

4.6 Back to normal operation

Once the problem on the Main Server is fixed it is ready to be brought back into operation again. Before doing so, it is good practice to first bring the Standby Server back to “Standby” state. This can be achieved by means of stopping its core services. Once back in “Standby” state, again all clients connected to the Standby Server will lose connection. Now, on the Main Server, the operator must import the latest database backups from the Standby Server. Server-specific information such as e.g. equipment agent IP addresses will be exchanged during import. Then

they will start the base and core services so that Main Server becomes running again and clients can connect back to the Main Server.

Of course, one can also bring back the Main Server to “Running” state without before bringing the Standby Server back to “Standby” state (leaving it in “Running” state). In this case all FOXMAN-UN clients connected to the Main or the Standby Server will observe a “Main Server and Standby Server running both at the same time” alarm in the FOXMAN-UN alarm list.

However, having both servers in “Running” state shall be handled with care. This might increase the network load and the CPU load on the individual network elements (processing requests from two FOXMAN-UN at the same time). Far worse, some services created on one FOXMAN-UN will not be reflected to the other one (because its configuration data is only stored in the local FOXMAN-UN database).

4.7 Alarms and Events

4.7.1 Alarm and Event Types

The Main/Standby Solution generates alarms and events under certain conditions that are visible in the alarm and event list of any FOXMAN-UN client connected to the Main or the Standby Server. The following table lists all possible alarms and events, their raise conditions and on which server the corresponding alarm or event is visible:

Use Case	Alarm/Event Condition	Alarm/Event	Text	Visible on Server	Remark
Standby Server periodically pings the Main Server.	Main Server not pingable.	Alarm: yes Event: yes	Switchover from Main Server (hostname) to Standby Server (hostname) due to a connectivity loss. Standby Server is now active.	Standby	Will only be created on a Standby Server of type “Warm Standby” after its core services have automatically started up.
Main Server periodically pings the Standby Server.	Standby Server not pingable.	Alarm: yes Event: yes	Standby Server (hostname) is not reachable.	Main	Will only be created in case the core services of the Main Server are running.
Both servers are running at the same time.	Core Services on Main and Standby Server are running.	Alarm: yes Event: yes	Main Server (hostname) and Standby Server (hostname) running both at the same time.	Main and Standby	Will only be created on the Main Server in case the core services of the Main Server are running. Will only be created on the Standby Server in case the core services of the Standby Server are running.
Scheduled Database Backup on Main Server.	Scheduled Database Backup failed.	Alarm: yes Event: yes	Periodic backup to /$/periodicbackup-x.bck on Main Server has failed.	Main	Will only be created in case the core services of the Main Server are running.
Scheduled Database Backup on Standby Server.	Scheduled Database Backup failed.	Alarm: yes Event: yes	Periodic backup to /$/periodicbackup-x.bck on Standby Server has failed.	Standby	Will only be created in case the core services of the Standby Server are running.
Standby Server copies latest scheduled Database Backup from Main Server.	Copy operation fails.	Alarm: yes Event: no	Transfer of Database Backup from Main Server (hostname) to Standby Server (hostname) has failed.	Main	Will only be created in case the core services of the Main Server are running.

Use Case	Alarm/Event Condition	Alarm/Event	Text	Visible on Server	Remark
Standby Server imports latest copied Database Backup from Main Server.	Database import fails.	Alarm: yes Event: no	Import of Database Backup from Main Server (hostname) on Standby Server (hostname) has failed.	Main	Will only be created in case the core services of the Main Server are running and the core services on the Standby system are not running.
Standby Server imports latest copied Database Backup from Main Server.	Database import fails.	Alarm: yes Event: no	Import of Database Backup from Main Server (hostname) on Standby Server (hostname) is not possible due to a running Standby system.	Main	Will only be created in case both the core services of the Main Server are running and the core services on the Standby system are running.
Compatibility check between Main and Standby Server.	Server versions of Main and Standby Server do not match.	Alarm: yes Event: no	Server version on Main Server (hostname) and Standby Server (hostname) are incompatible.	Main	Will only be created in case the core services of the Main Server are running.

4.7.2 Clearance of Alarms

The alarms which are generated by the Main/Standby Solution have been designed in such a way that raised alarms will be cleared under the following circumstances:

- Raised alarms will be cleared automatically by the system upon the point where the raise condition is no longer fulfilled. Exception: the “Switchover from Main Server (hostname) to Standby Server (hostname) due to a connectivity loss. Standby Server is now active” alarm will never be cleared by the system.
- All alarms can explicitly be cleared by the user.

5 Setup and Operation

This chapter describes how to setup a Main/Standby Server pair and how to bring it into operation.

5.1 Preconditions

The following preconditions need to be fulfilled to continue with the configuration:

- Two FOXMAN-UN servers available;
- The FOXMAN-UN system on both servers must be of the same version;
- Both FOXMAN-UN systems are equally configured w.r.t. the managed network;
- Base services running on both servers;
- The host file on both server machines and any remote client machine contains the IP address and the host name of both servers.
- Also read and apply the contents of section IP Address Translation for FOXMAN-UN Element Agents when using Element Agents or nodes in different subnets for Main and Standby servers.

For this setup example will use the following two servers:

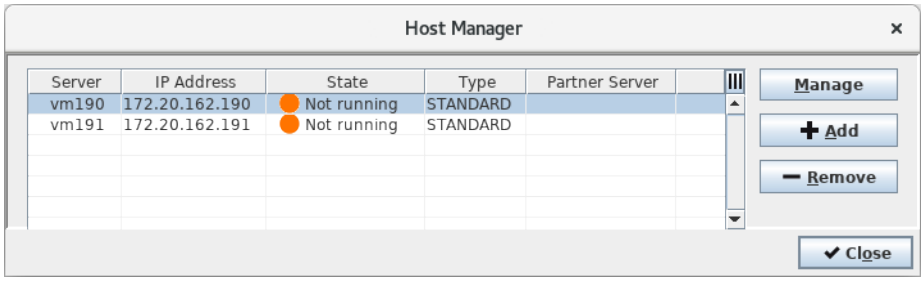
- Main Server:
  - hostname: vm190,
  - IP: 172.20.162.190,
- Standby Server:
  - hostname: vm191,
  - IP: 172.20.162.191,
  - type: Warm Standby Server.

5.2 Pairing the Servers

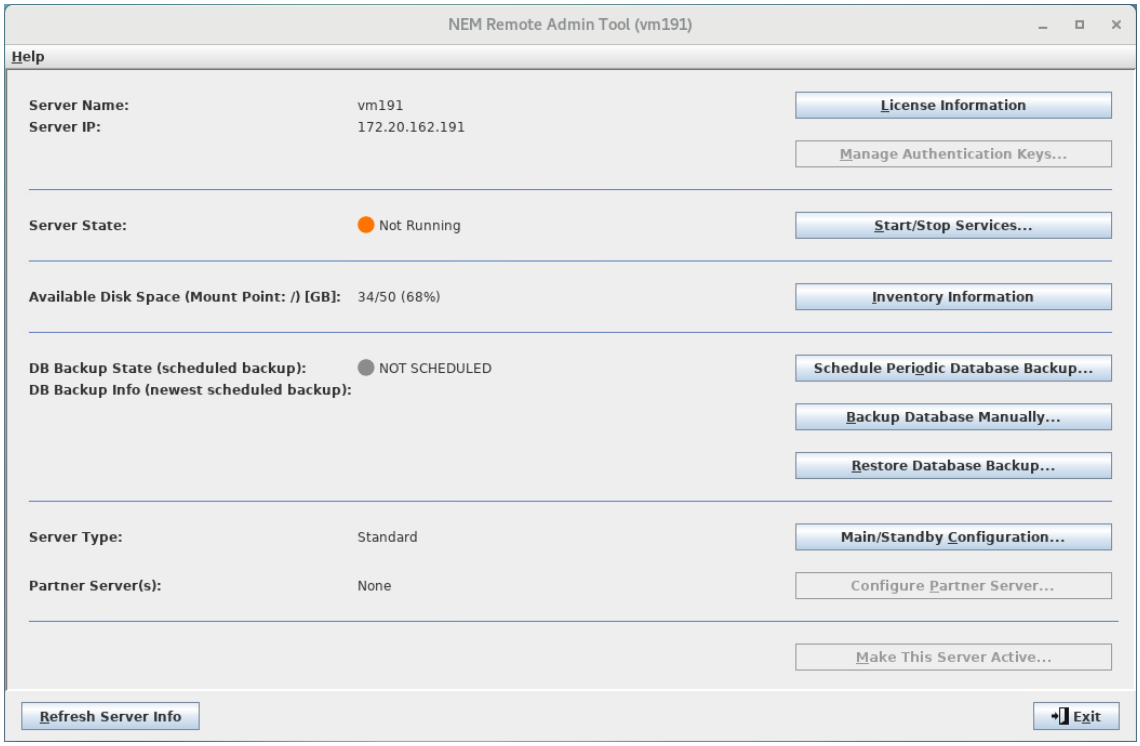
As a first step the servers need to be paired. Thereto open a NEM Login window (local or remote client). In the Login Window click on the gearwheel icon ⚙. The Host Manager will open. Next, click on the <+Add> button to display the <Edit Connection> dialog. Add “vm190” to the <Host Name> field. Click into the <IP Address> field. The IP belonging to the host name will automatically be added. Confirm with the <OK> button. Repeat the same steps for “vm191”.

Please note:
In case the NEM Login Window is opened on a local client, the Host Manager will already contain the local server (host) in its host list. In case the NEM Login Window is opened on a remote client, the Host Manager will not contain any servers (hosts) in its host list.

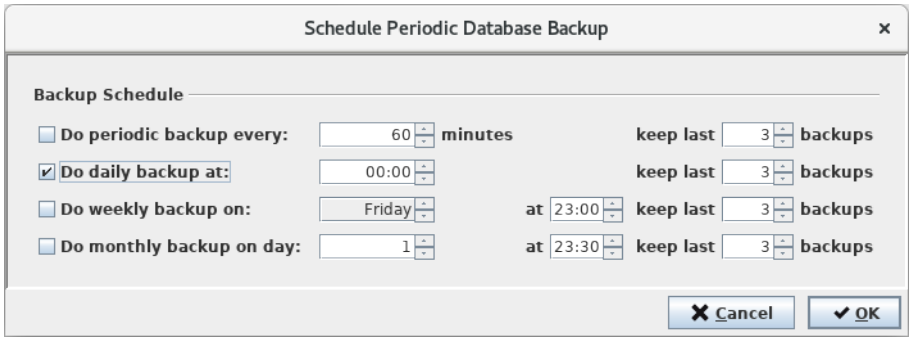
After these steps have been carried out the Host Manager will look as follows:



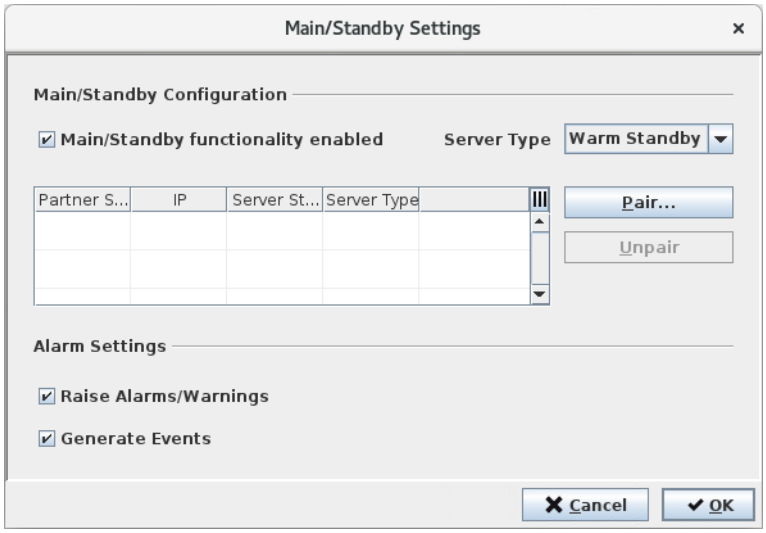
Now select the “vm191” row in the Host Manager. Click on the <Manage> button. The <Login> dialog of the Remote Admin Tool will show up. Log in to the server as an administrator user. Now the Remote Admin Tool will start up.



As a next step a periodic database backup must be scheduled. Open the <Schedule Periodic Database Backup> dialog by clicking on the <Schedule Periodic Database Backup…> button. Schedule a periodic backup, e.g. once a day at midnight and confirm by clicking on the <OK> button.



Now open the <Main/Standby Settings> dialog by clicking on the <Main/Standby Configuration…> dialog. Enable the Main/Standby functionality and select Server Type “Warm Standby”. Confirm by clicking on the <OK> button.

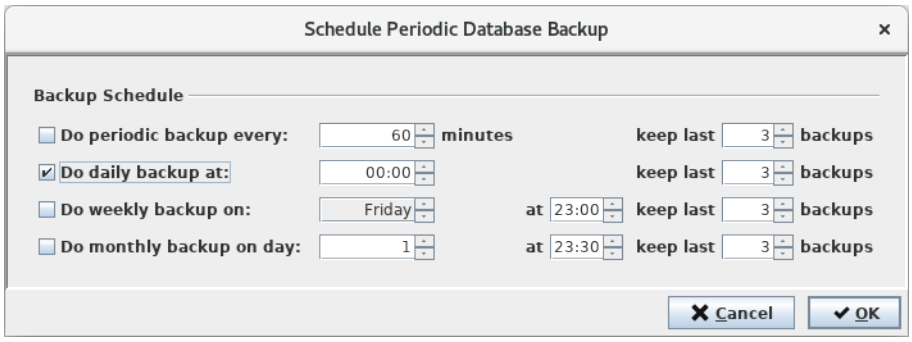


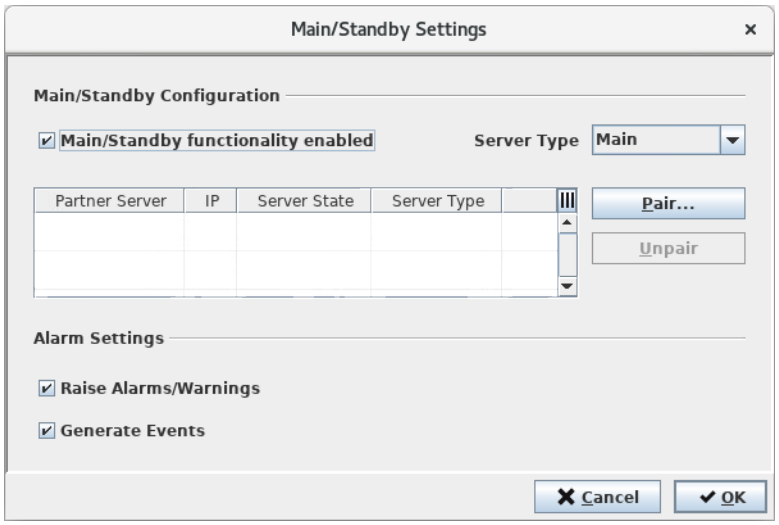
Close the Remote Admin Tool by clicking on the <Exit> button on the tool's main window.

Switch back to the Host Manager and select the "vm190" row. Click on the <Manage> button (alternatively you can also double-click on the selected row). The <Login> dialog of the Remote Admin Tool will show up. Log in to the server as an administrator user. Now the Remote Admin Tool will startup.

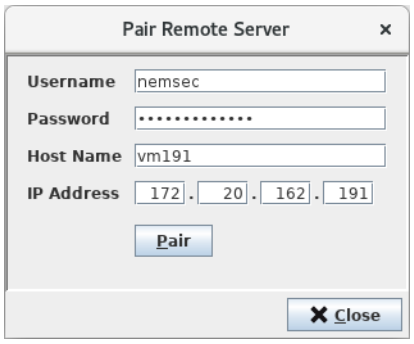
Again, schedule a periodic database backup, enable the Main/Standby functionality and this time select Server Type "Main".

Please note:
It is recommended to define the same periodical backup schedule for both servers.



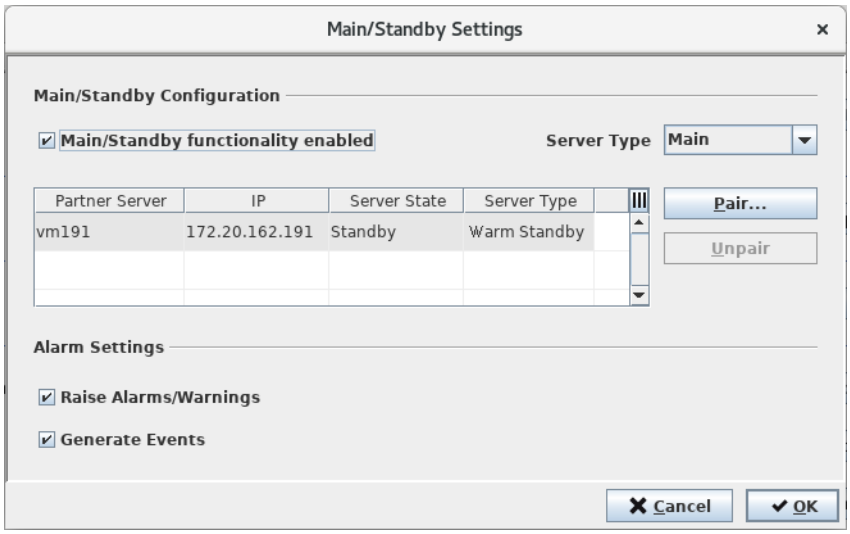


Now everything is prepared for the actual pairing operation. Select the <Pair…> button and on the displayed <Pair Remote Server> dialog enter the NEM security administrator username and password, the hostname, and the IP address of the Standby Server. Then click on the <Pair> button to complete the pairing.



Successful pairing will be confirmed.

Acknowledge the message by clicking on the <OK> button. On the <Main/Standby Settings> dialog the Standby Server now is visible as an entry in the partner server list.



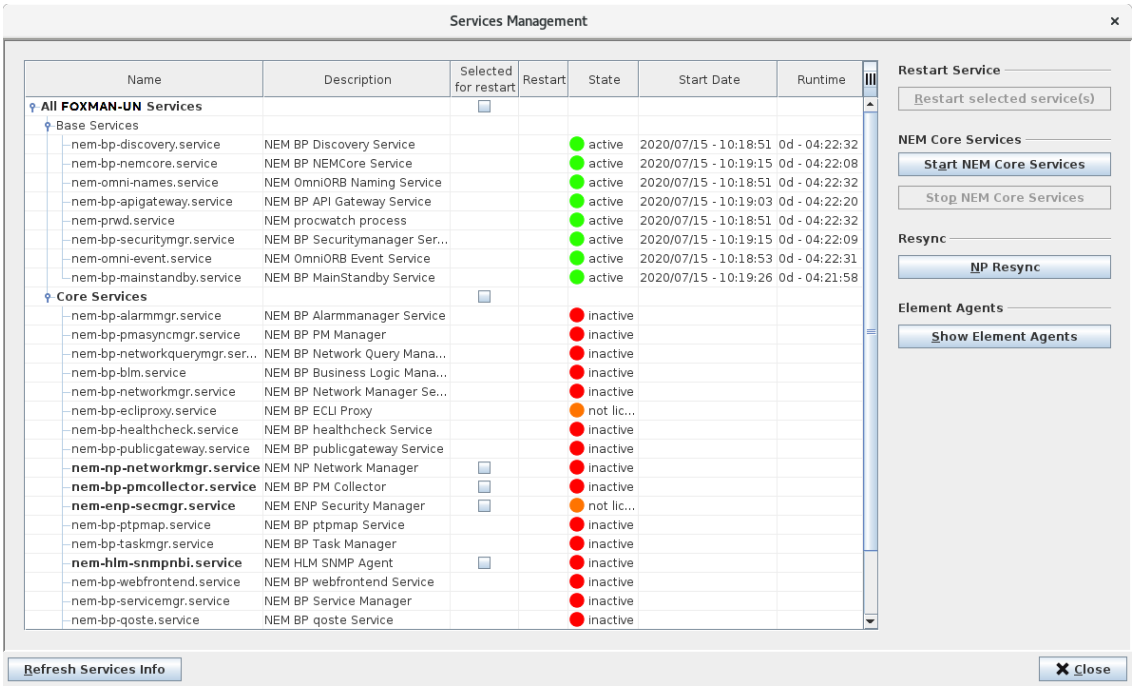
Please note:
Unchecking the <Main/Standby functionality enabled> checkbox for already paired servers on any server will disable (uncheck) the Main/Standby functionality on all paired servers.

Checking the <Main/Standby functionality enabled> checkbox for already paired servers on any server will enable (check) the Main/Standby functionality on all paired servers.

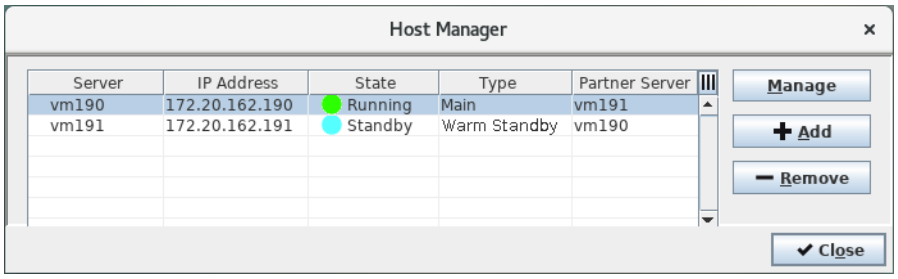
5.3 Bring up Main Server in operational state

Main and Standby Server are paired now. On both servers, only the base services are running. In this state one speaks of state “Standby” for the Standby Server and state “Not running” for the Main Server. Whereas for the Standby Server this is the desired state, the Main Server must be brought up to state “Running”. This can be achieved by starting the core services on the Main Server, either directly on the Main Server via console command “nemstart” or again by

means of the Remote Admin Tool. Thereto, on the Remote Admin Tool" which is connected to the Main Server, click on the <Start/Stop Services…> button. The <Services Management> dialog will show up. Then click on the <Start NEM Core Services> button and wait until the core services have started up. Close the dialog.

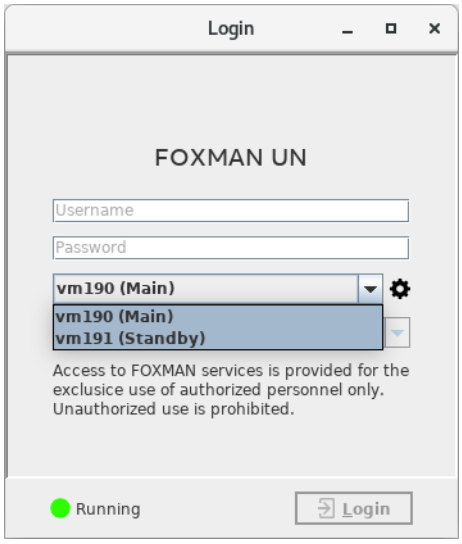


Now both the Main and the Standby Server are in operational state. The Main Server is in state "Running" and the Standby Server is in state "Standby". This can also be verified in the Main Server's <Host Manager> dialog.

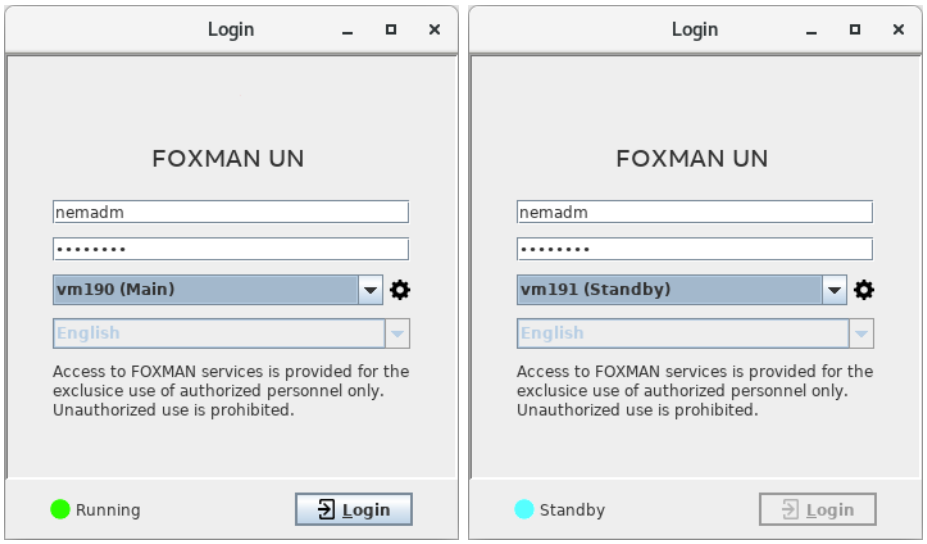


5.4 NEM Login Window

The NEM Login Window of any FOXMAN-UN client offers login to all hosts as added in the NEM Host Manager of the respective client. Servers available in the hosts combo box are amended by the term "(Main)" if the corresponding server is of type "Main" or by the term "(Standby)" if the corresponding server is of type "Cold Standby" or "Warm Standby". Servers of type "Standard" will not be labeled specially.



The server state with a corresponding color icon is shown in the lower left corner of the Login Window. Log in to a selected server is only possible if its state equals to “Running”.



A click on the gearwheel icon will open the Host Manager.

5.5 NEM Host Manager

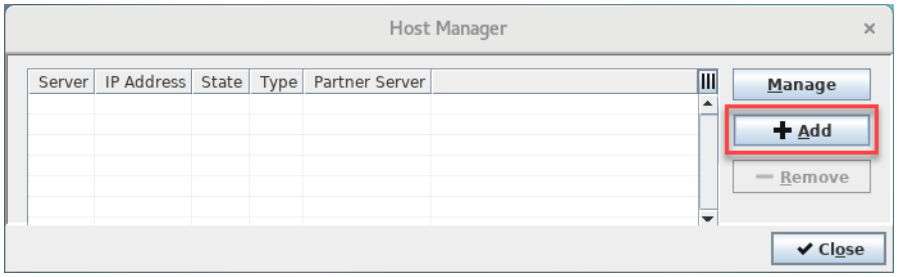
The NEM Host Manager serves definition of hosts to which the user can connect from the NEM Login Window. It can be launched by clicking on the gearwheel icon on the Login Window. Every FOXMAN-UN client needs to define its own list of hosts. Prior to being able to add hosts in the Host Manager, all desired hosts must be added to the hosts file of the corresponding client machine. On Linux systems the host file named “hosts” resides under /etc and on Windows systems under C:\Windows\System32\drivers\etc\

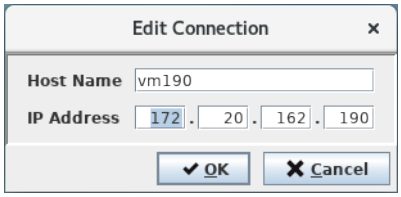
```
[nemadmin@vm190 ~]$ cat /etc/hosts
127.0.0.1         localhost localhost.localdomain
172.20.162.190    vm190 vm190.localdomain
172.20.162.191    vm191 vm191.localdomain
```

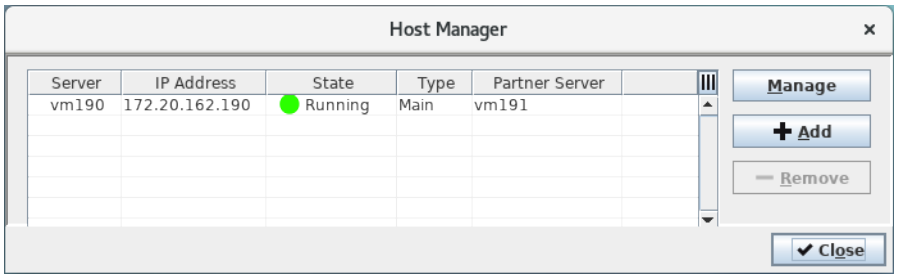
Please note:
If a DNS Server is configured for the respective system, the hosts file must not be adapted.

Once done host can be added in the Host Manager by means of the <+Add> button. Clicking on the button will open an <Edit Connection> dialog. Therein a desired hostname and correspond-

ing IP address can be specified. Confirmed by the <OK> button the host will be added to the hosts list of the Host Manager.



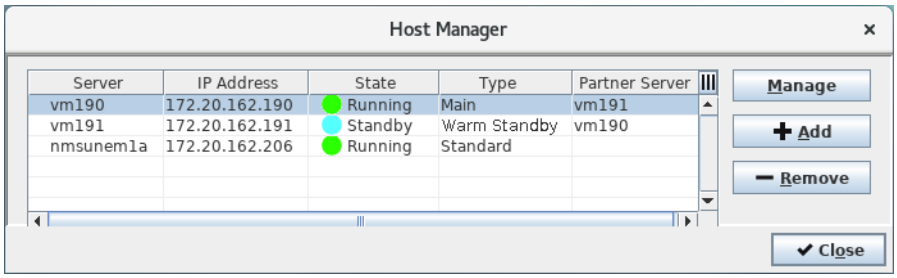




All added hosts will be visible in the hosts list of the Host Manager with the following attributes:

- Server (hostname)
- IP Address
- State
- Type
- Partner Server

Partner servers will only be visible if they have been paired properly. Following an example of a Host Manager showing three servers of different type:

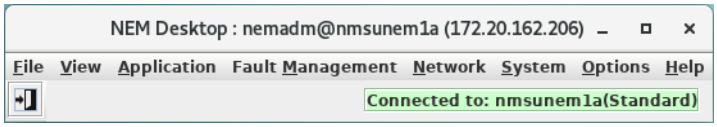


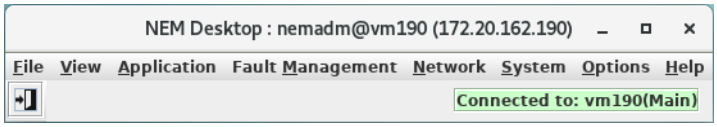
Selection of a server in the hosts list and clicking on the <Manage> button will start the Remote Admin Tool for the selected server (refer to chapter 6.1 "Remote Admin Tool"). Double-clicking on a row in the hosts list will close the Host Manager and enter the respective host in the “host field” of the NEM Login Window.

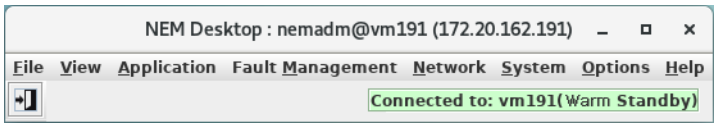
5.6 NEM Desktop

Successful login to a Server from the NEM Login Window of a FOXMAN-UN client will start the NEM Desktop. In the lower right corner of the NEM Desktop Window a status field is shown,

indicating to which server (host) and server type the client is currently connected. The green color of the field indicates a successful connection to the server.

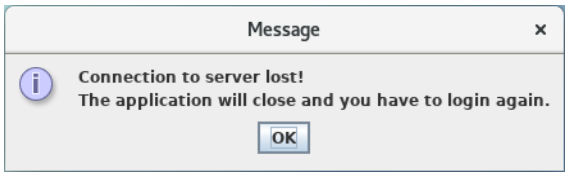


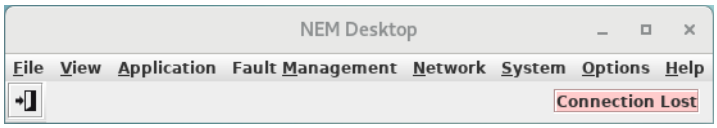




If both the Main Server and the Standby Server are running at the same time, the Server status field is colored orange.

If the connection to a server is lost, a message box will be shown informing the user correspondingly. The status field of the NEM Desktop Window will display the text “Connection Lost” and its color changes from green to red.

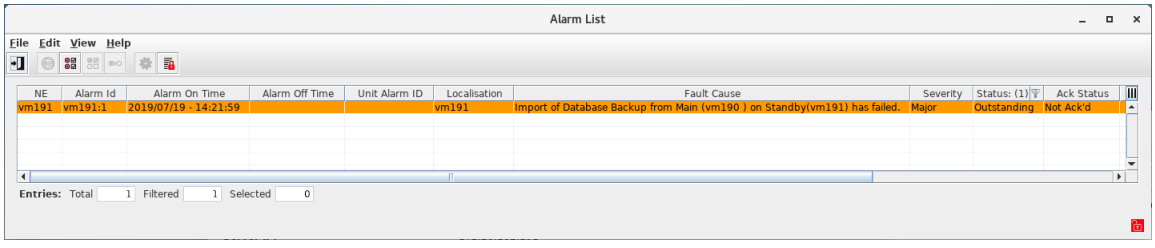


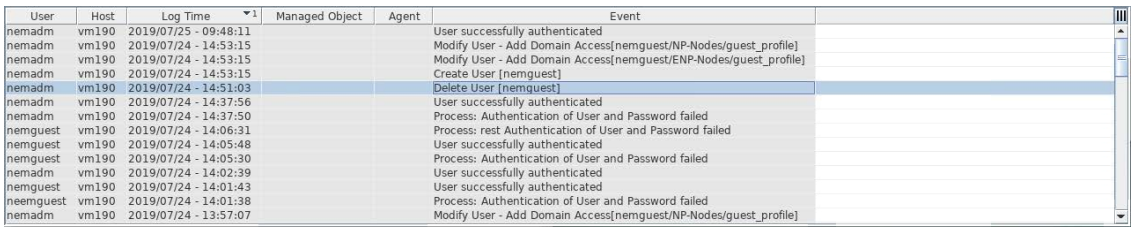


Clicking on the <OK> button of the message box will close the NEM Desktop Window and show the NEM Login Window.

5.7 NEM Alarm and Event List

The Main/Standby Solution generates alarms and events under certain conditions (refer to chapter 4.7 "Alarms and Events") that are visible in the alarm and event list of any FOXMAN-UN client connected to the Main or the Standby Server. These alarms and events inform the user about incidents on the system that are related to the solution and thus help them to react in an appropriate manner.





6 Configuration

6.1 Remote Admin Tool

6.1.1 Overview

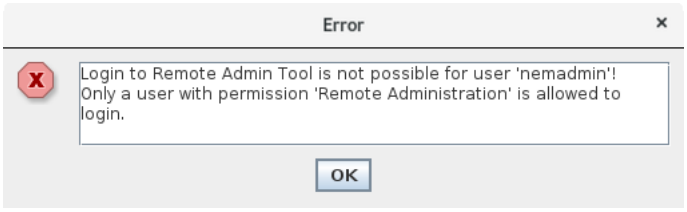
The Remote Admin Tool (RAT) is a Graphical User Interface that serves administration of a FOXMAN-UN server.

It is essential for setup and configuration of the Main/Standby Solution.

Startup of the RAT is only possible for FOXMAN-UN admin users. Users with less privileges than admin users on the respective FOXMAN-UN server will not be able to select the Remote Admin Tool menu entry in the GUI. When executing the client script

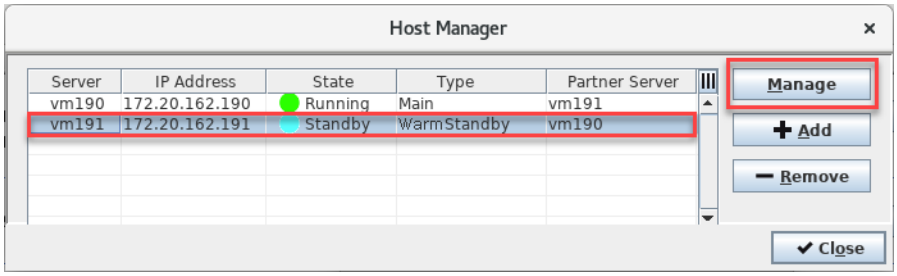
```
/opt/nem/client/bin/remoteadmintool -i <ServerIPAddress> -s <ServerName>
```

and logging in to the server with insufficient permissions, they will be prompted with a corresponding error message after login:

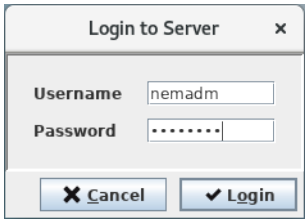


6.1.2 Startup

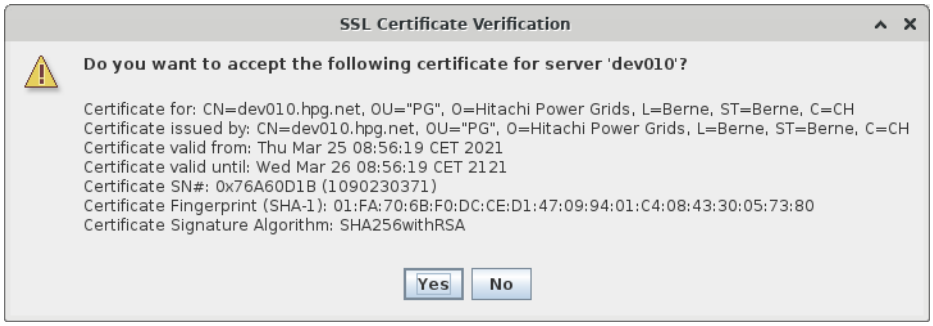
The RAT can be started either from the NEM Host Manager or the NEM Desktop. In the NEM Host Manager select the table row containing the server for which the RAT shall be started, and click on the <Manage> button.



Then the login screen will be shown and login to the Server as a FOXMAN-UN admin user must be performed.



If a user logs in to the specified host for the first time, they will be prompted an “SSL Certificate Verification” dialog upon pressing the <Login> button which looks as the following sample dialog:



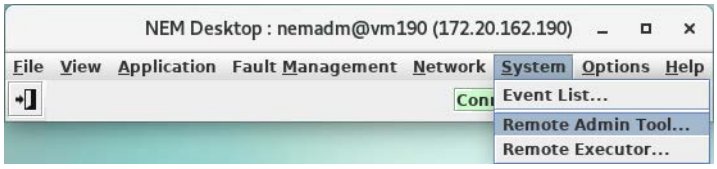
If the user presses the <No> button, they will not be able to connect to the FOXMAN-UN server. The next time they try to login to the same host from the same client, they will be prompted again the “SSL Certificate Verification” dialog.

If the user presses the <Yes> button, they will be connected to the FOXMAN-UN server. The next time they try to login to the same host from the same client, they will directly be connected to the server (they will no longer be prompted the “SSL Certificate Verification” dialog).

Please note:
Make sure that you are connecting to the correct server especially from a remote client. This is particularly important when you are working in a non-safe network environment like for instance accessing a FOXMAN-UN server over the public Internet.

Validation can be done by the user by contacting the server administrator and comparing the fingerprint of the FOXMAN-UN server certificate stored on the server to the one presented in the “SSL Certificate Verification” dialog on the FOXMAN-UN client.

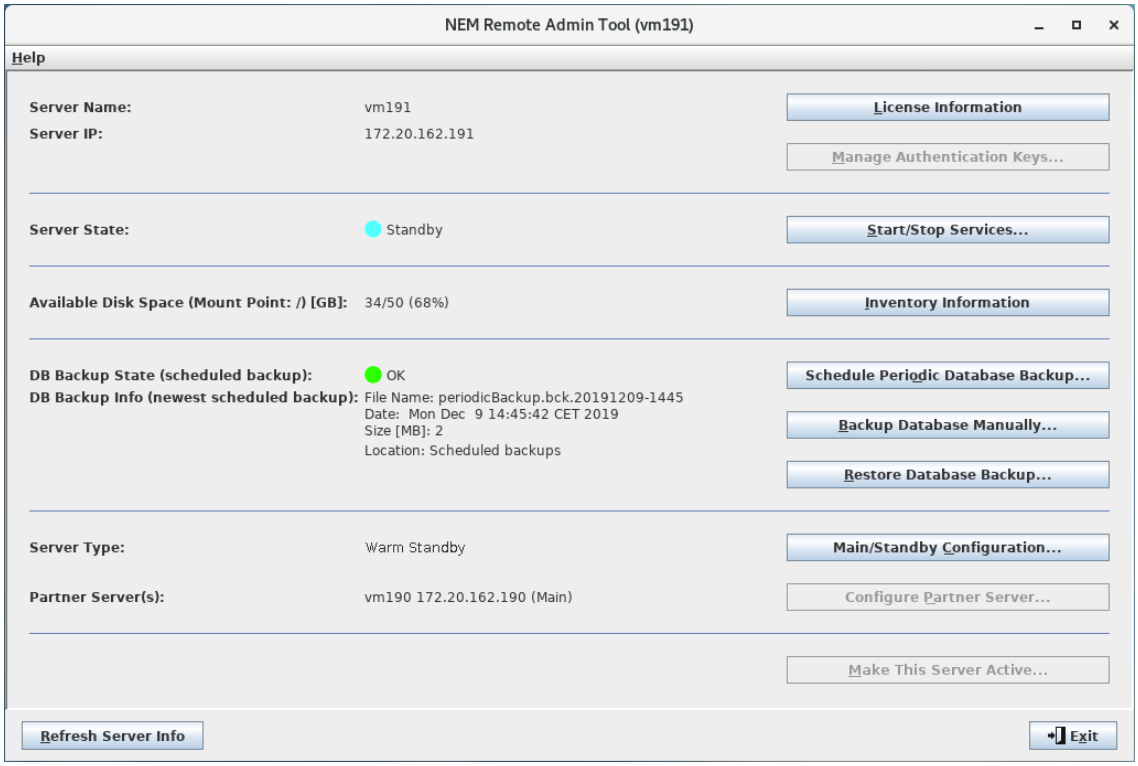
To start up the Remote Admin Tool from the NEM Desktop open the menu <System> <Remote Admin Tool…>. The RAT will directly start up without the need to log in to the server.



6.1.3 Main Window

The RAT’s main window displays the following basic information:

- Server Name
- Server IP
- Server State
- Available Disk Space
- Database Backup State (scheduled backup)
- Database Backup Info (newest scheduled backup)
- Server Type
- Partner Server(s)



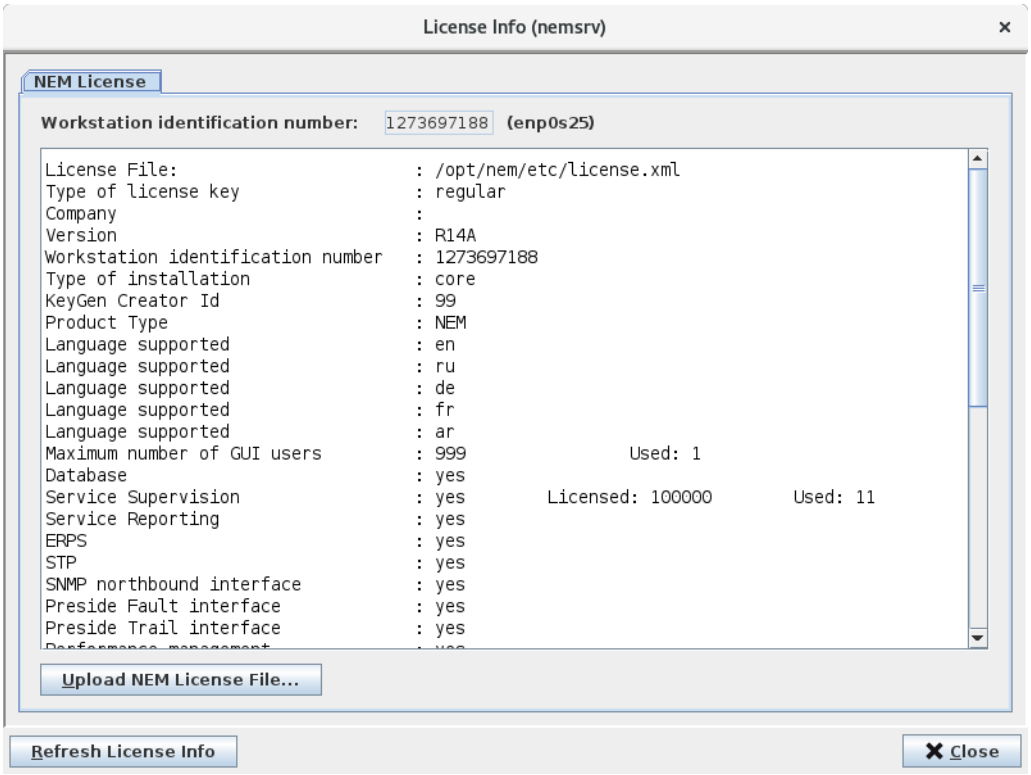
The Remote Admin Tool periodically polls the server to which it is connected for its most recent data. Retrieved information then is automatically updated on the Main Window. However, the <Refresh Server Info> button allows the user to update the information displayed on the window on request. Clicking on the button will immediately retrieve the most recent data from the server and update the Main Window correspondingly.

6.1.4 License Info Dialog

Clicking on the <License Information> button on the Main Window of the RAT will open its <License Info> dialog. The dialog contains two tabs named “NEM License” and “CST1 License”. The <Refresh License Info> button allows the user to update the license information displayed on the currently selected license tab.

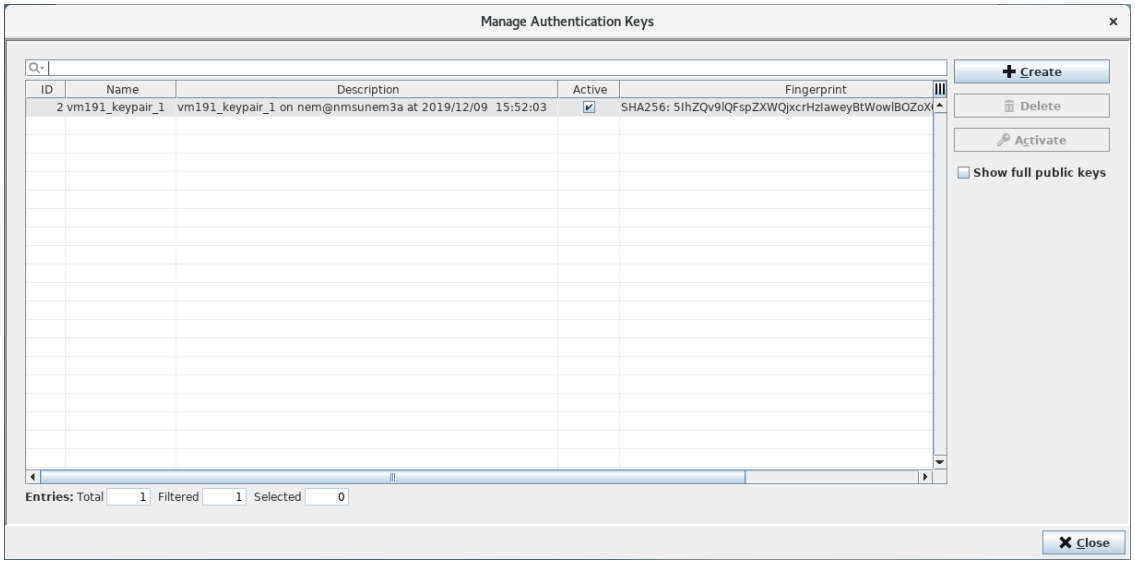
6.1.4.1 NEM License Tab

The <NEM License> tab shows information about the FOXMAN-UN license on the server to which the RAT is connected. Furthermore, it lists the workstation identification number and the Ethernet Interface for which the license was issued. An <Upload NEM License File…> button allows the user to upload a new license file to the server.



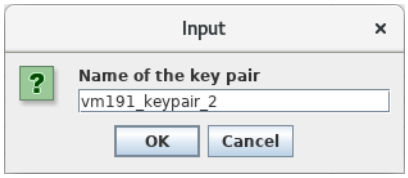
6.1.5 Manage Authentication Keys Dialog

Clicking on the <Manage Authentication Keys> button on the Main Window of the RAT will open its <Manage Authentication Keys> dialog. The button is only enabled if the server to which the RAT is connected is in state “Running”, which means all its base and core services are running. The dialog serves creation of public/private key pairs which are needed to establish SSH communication between FOX61x nodes and the FOXMAN-UN. The private key of a key pair always stays on the FOXMAN-UN server whereas for each node the corresponding public key can be uploaded via the FOXCST.

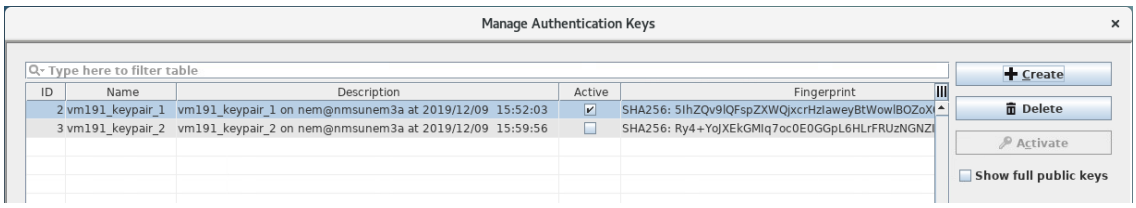


6.1.5.1 Creation of Key Pairs

A key pair can be created by clicking on the <Create> button on the dialog. An <Input> dialog will be shown where the user can enter an appropriate key pair name.



Upon clicking on the <OK> button the key pair will be created and added to the list of key pairs.



6.1.5.2 Deletion of Key Pairs

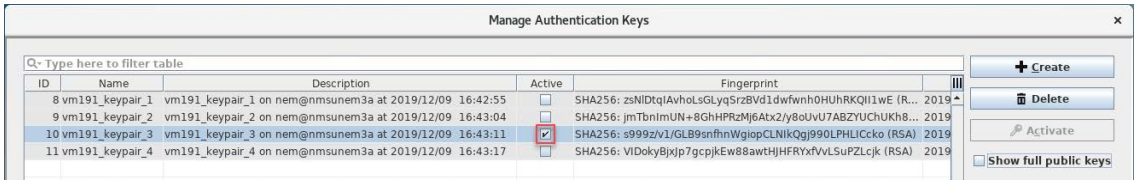
A key pair can be deleted by selecting it in the list of key pairs and then clicking on the <Delete> button on the dialog. A <Confirmation> dialog will be shown where the user must confirm deletion by clicking on the <Yes> button.

Upon clicking on the <Yes> button the key pair will be deleted and removed from the list of key pairs.

6.1.5.3 Activation of Key Pairs

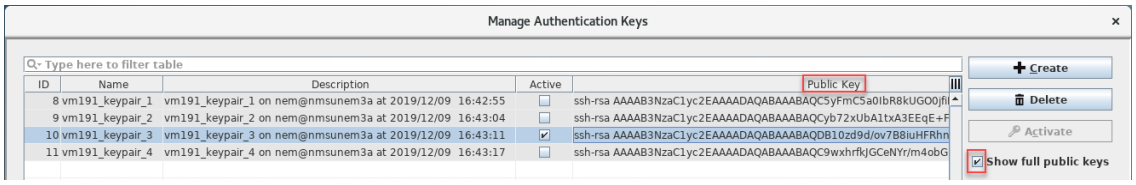
A key pair can be activated by selecting it in the list of key pairs and then clicking on the <Activate> button on the dialog. A <Confirmation> dialog will be shown where the user must confirm activation by clicking on the <Yes> button.

Upon clicking on the <Yes> button the key pair will be activated in the list of key pairs.



6.1.5.4 Display of Full Public Keys

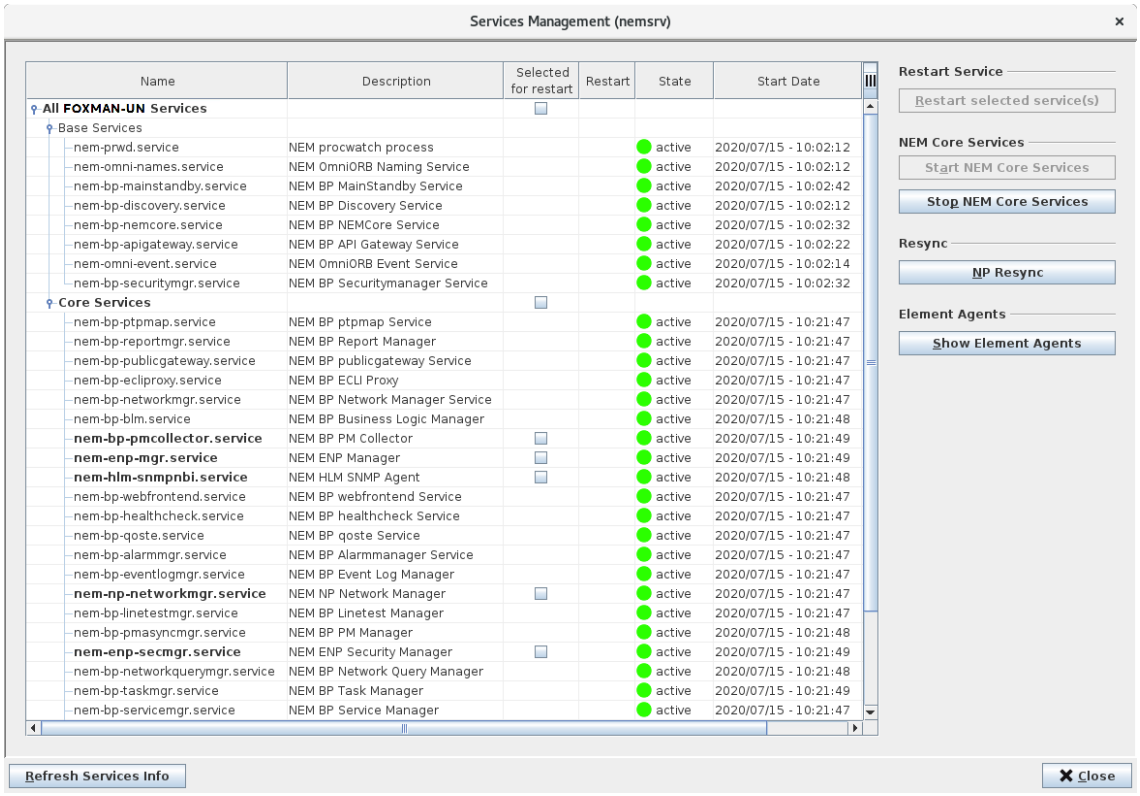
The <Manage Authentication Keys> dialog shows a list of all available public/private key pairs available on the server to which the RAT is connected. The <Fingerprint> column shows the SHA256 hash value of the public key of every public/private key pair in the list. If desired the full public keys can be shown instead. Thereto the <Show full public keys> checkbox must be ticked. Upon ticking the checkbox, the Column <Fingerprint> will be renamed to <Public Key> and will show the public key of every public/private key pair in the list.



6.1.6 Services Management Dialog

Clicking on the <Start/Stop Services…> button on the Main Window of the RAT will open its <Services Management> dialog. The dialog offers the following functionalities:

- Overview over the operational state of individual FOXMAN-UN services listing state (active/ inactive), start date (time) and runtime (uptime) per individual service;
- Possibility to restart groups of services or individual services;
- Possibility to stop/start the NEM Core Services;
- Possibility to resynchronize the FOXMAN-UN Networking Package;
- Possibility to display the state of configured Network Element Agents.
- Possibility to refresh the services information displayed on the dialog.

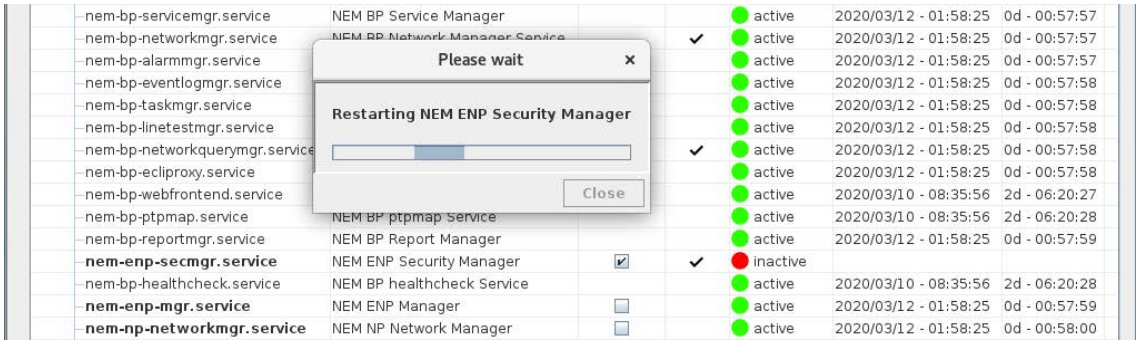


6.1.6.1 Operational state of services

The <Services Management> dialog displays the operational state of individual FOXMAN-UN services listing state (active/inactive), start date (time) and runtime (uptime) per individual service. The state of every service is queried at a regular interval from the server to which the RAT is connected and thus is periodically updated on the dialog.

6.1.6.2 Restart of groups of services or individual services

On the <Services Management> dialog the operator can restart groups of services or individual services. Groups of services or individual services that can be restarted are printed in bold in the <Name> column and can be selected (ticked) for restart in the <Select for restart> column. Once ticked, all services that depend on a ticked group of services or ticked individual service will be marked for restart in the <Restart> column. Once the user has done the selection, they can press the <Restart selected service(s)> button which will trigger the actual restart operation.



Please note:
For the operator a restart of a service will be noticeable through its new start time and a new runtime (after having pressed the <Refresh Services Info> button).

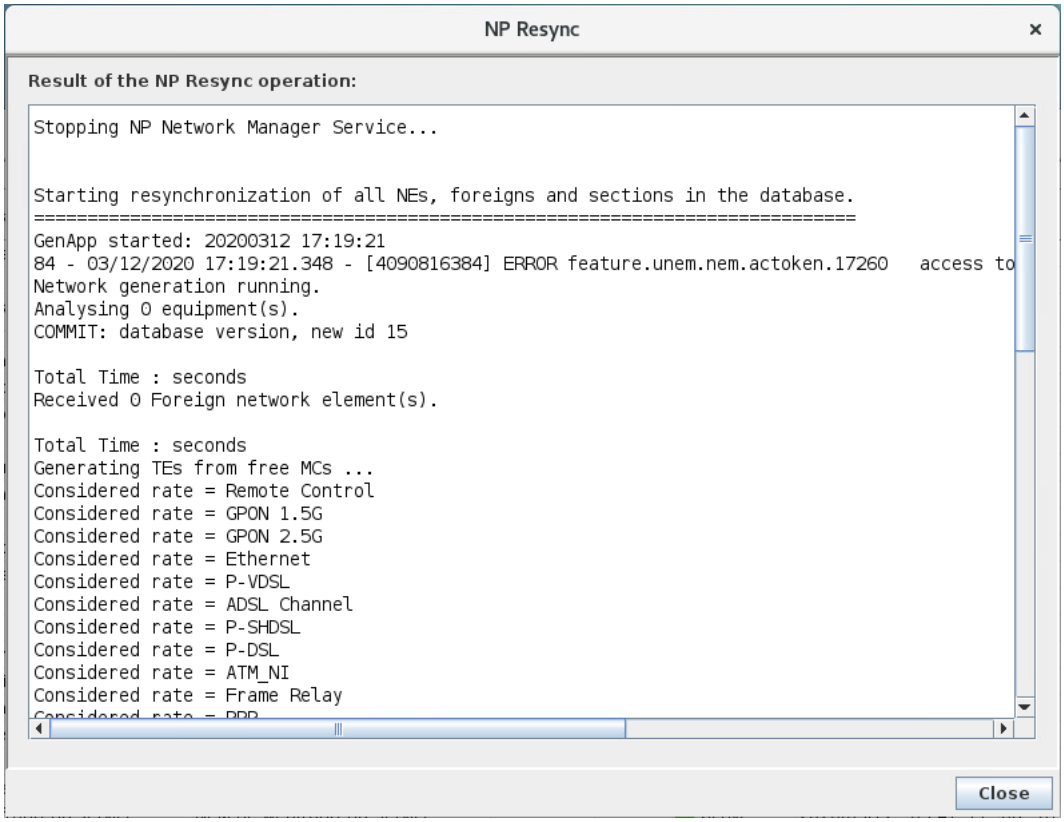
Restarting “All FOXMAN-UN Services” will disconnect the RAT from the server and the tool will be closed. A corresponding warning message will be displayed prior to execution of the command that needs to be confirmed by the operator. After the server’s Base Services have restarted, the user can connect again to the server with the RAT if desired.

6.1.6.3 Stop/Start of NEM Core Services

Services belonging to the “Core Services” group not only can be restarted but they can also be explicitly stopped or explicitly started via the corresponding buttons <Stop NEM Core Services> and <Start NEM Core Services>. This functionality is needed in connection with the Main/Standby solution where for various reasons the operator needs to be given the possibility to stop or start the core services on the Main or on the Standby Server.

6.1.6.4 Networking Package Resynchronization

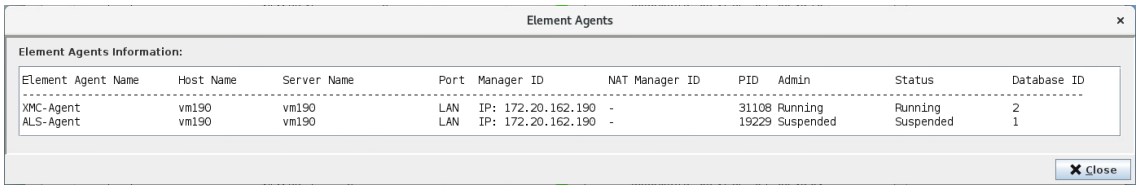
In rare cases, the FOXMAN-UN Networking Package might get out of synchronization with the FOXMAN-UN Base Package and thus will be in an inconsistent state. If the operator sees some indication for this case in the <Networking Package> window of the FOXMAN-UN they can trigger a resynchronization of the networking package with the base package by pressing the <NP Resync> button in the RAT. After having pressed the button, a dialog will open, listing the result of the NP resync operation.



Please note:
The NP Resync operation will only work if no user is editing any NP Application on the corresponding FOXMAN-UN server. If any editing session is active, the dialog displaying the result of the NP Resync operation will list a “NP resync stopped” error together with all connected users

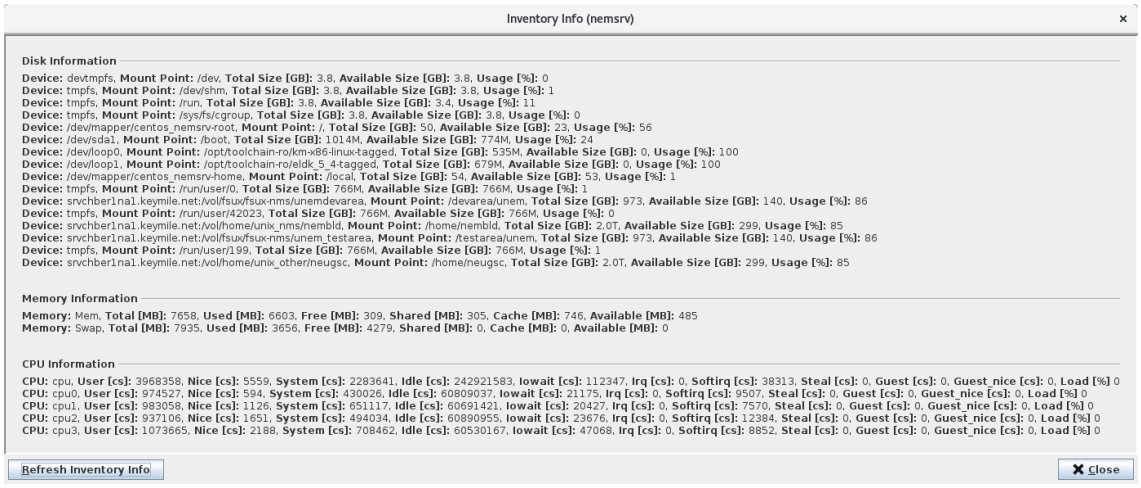
6.1.6.5 Display of Network Elements Agents

Pressing the <Show Element Agents> button will prompt a window that displays all configured Network Element Agents of the server to which the RAT is connected. For every agent a variety of related attributes such as Element Agent Name, Host Name, Status etc is shown.



6.1.7 Inventory Info Dialog

Clicking on the <Inventory Information> button on the Main Window of the RAT will open its <Inventory Info> dialog. The dialog shows the most important information about the server’s system such as disk, memory and CPU information. A <Refresh Inventory Info> button allows the user to update the displayed inventory information on the dialog.



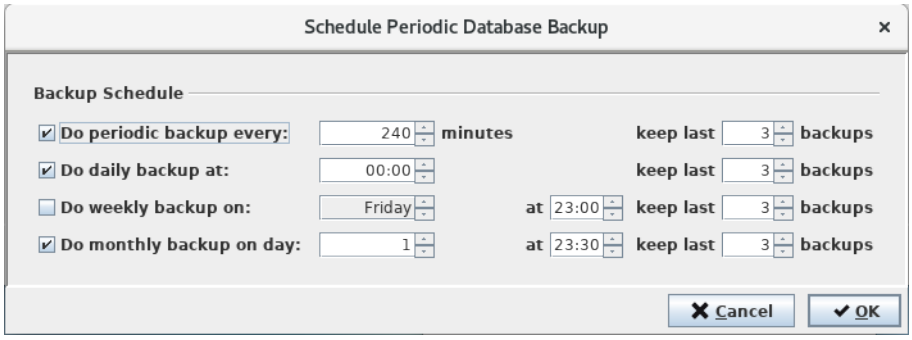
6.1.8 Schedule Periodic Database Backup Dialog

Clicking on the <Schedule Periodic Database Backup…> button on the Main Window of the RAT will open its <Schedule Periodic Database Backup> dialog. The dialog allows you to schedule a periodic database backup for the server to which the RAT is connected.

Backups can be scheduled:

- Every x minutes,
- Daily at a specific hour,
- Weekly on a specific weekday,
- Monthly on a specific day.

Any combination is possible as shown below.



For real Main/Standby Solution setups it is recommended to schedule at least one periodic backup a day.

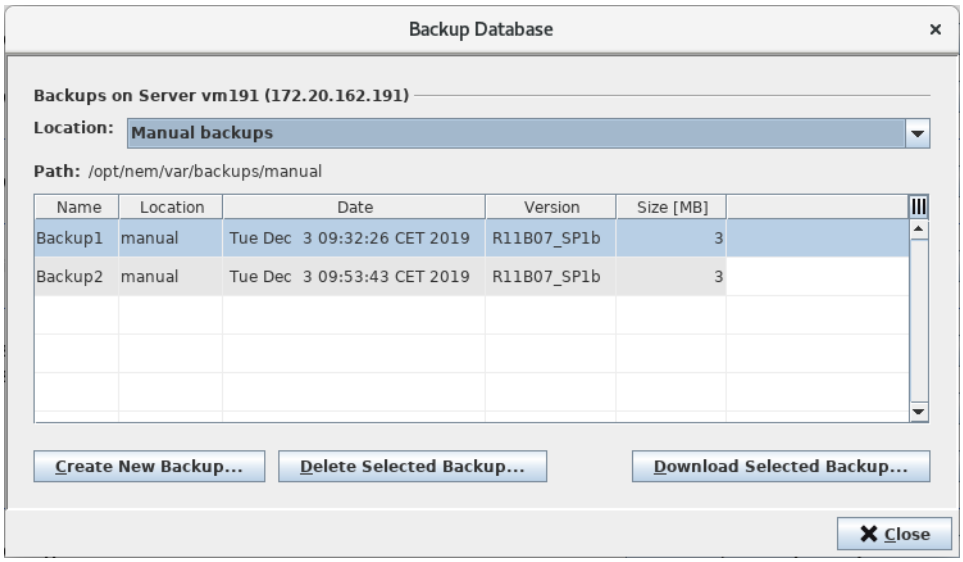
Please note:
If a monthly backup is scheduled for day 29, 30 or 31 and the month in which the backup shall be done does not have that many days, the backup will be done the last day of that month. Example: Monthly backup scheduled for day 31. In June the backup will be taken on day 30 as June only has 30 days.

6.1.9 Backup Database Dialog

Clicking on the <Backup Database Manually…> button on the Main Window of the RAT will open its <Backup Database> dialog. The dialog supports the following operations:

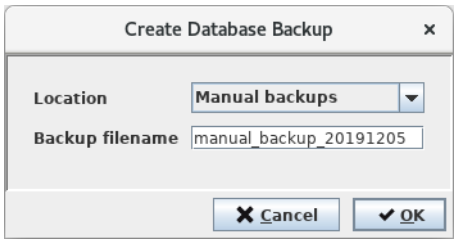
- display of available database backups in a specific location on the server to which the RAT is connected;
- manual database backup of the server to which the RAT is connected;

- deletion of an existing database backup on the server to which the RAT is connected;
- download of an existing database backup to the client machine from the server to which the RAT is connected.

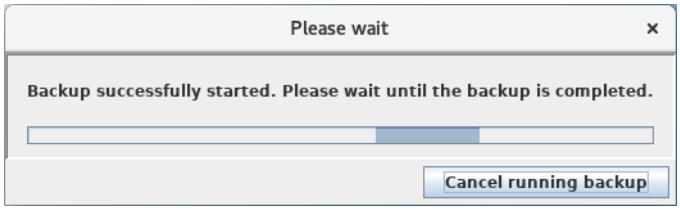


6.1.9.1 Create New Backup

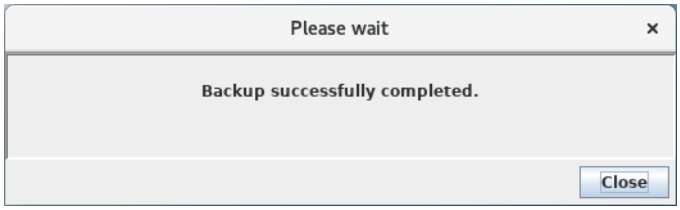
Clicking on the <Create New Backup> button on the <Backup Database> dialog will open the <Create Database Backup> dialog. It is aimed to do a manual database backup on the server to which the RAT is connected.



As a default, manual database backups got to the “Manual backups” location. Other available locations can be chosen as well except for the “Scheduled backups” location. However, it is recommended to use the “Manual backups” location for manual backups. Furthermore, a filename must be provided. Clicking on the <OK> button will start the backup operation.

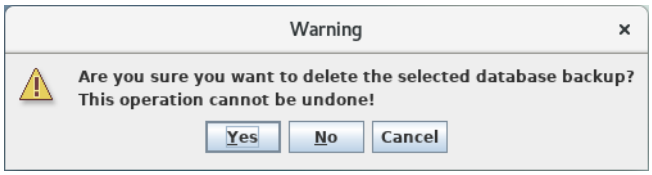


A successful backup will be confirmed upon completion.



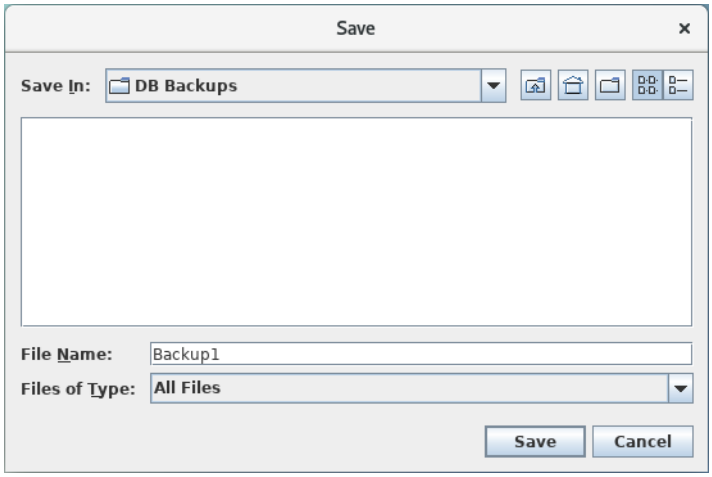
6.1.9.2 Delete Selected Backup

A selected database backup can also be deleted. Clicking on the <Delete Selected Backup> button on the <Backup Database> dialog will delete the backup after clicking on the <OK> button on the shown warning message.

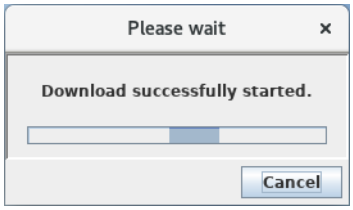


6.1.9.3 Download Selected Backup

If needed, a selected database backup can be downloaded to the client machine. Clicking on the <Download Selected Backup> button on the <Backup Database> dialog will open a <Save> dialog.



Entering an appropriate file name in the dialog and clicking on the <Save> button will start the download operation.



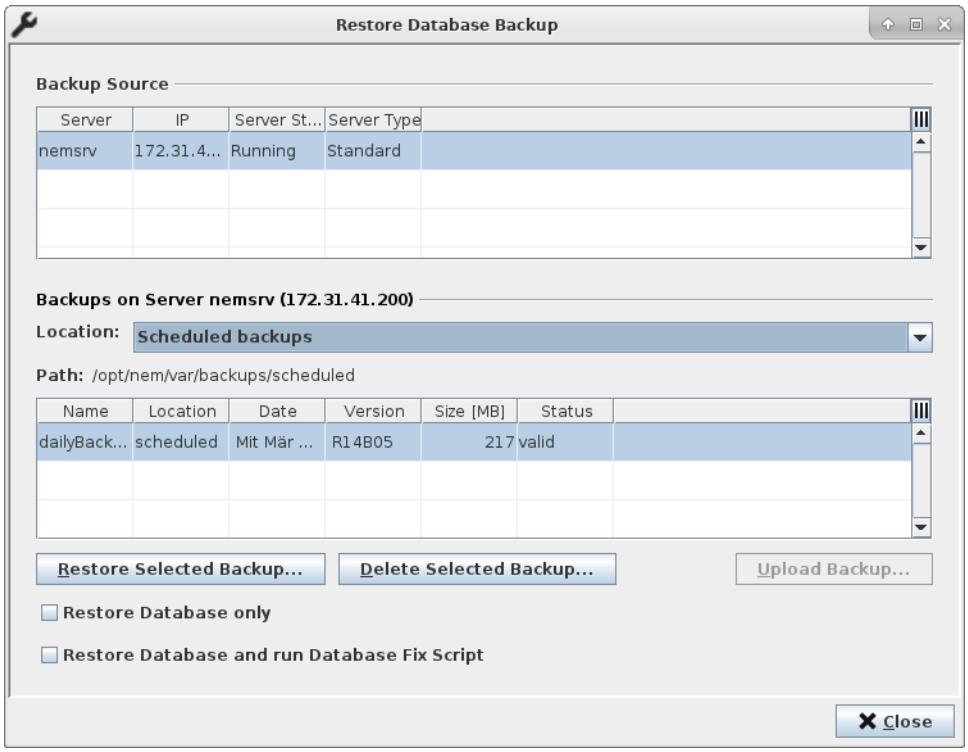
A successful download will be confirmed upon completion.

6.1.10 Restore Database Backup Dialog

Clicking on the <Restore Database Backup…> button on the Main Window of the RAT will open its <Restore Database Backup> dialog. The dialog supports the following operations:

- display of servers which can be chosen as a backup source;
- display of available database backups in a specific location on the server which has been chosen as a backup source;

- restoration of a selected database backup on the server which has been chosen as a backup source;
- deletion of an existing database backup on the server which has been chosen as a backup source;
- upload of an existing database backup from the client machine to the server to which the RAT is connected.



6.1.10.1 Restore Selected Backup

The <Restore Database Backup> dialog offers the restoration of a database backup on a server. Thereto the user must carry out the following steps:

1 Selection whether they want to restore the database only.

2 Selection whether they want to run the database fix script.

3 Selection of a backup source server.

4 Selection of a backup location on the source server.

5 Selection of a database backup in the backup location.

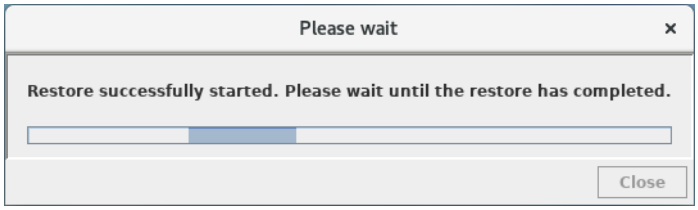
With step 1 the user decides whether they want to restore the database only. This option will only restore the NEM Database, the PM Database, the ALS Database, the alarm.txt and the events.txt file. Additional files will not be restored. This option corresponds to the command “edbrestore -n” executed in a terminal window on the server where the database shall be restored.

With step 2 the user decides whether they want to replace the Host Names and IP addresses of existing Element Agents in the selected backup through the ones of the FOXMAN-UN where the database restoration takes place (please refer to chapter 6.3 "IP Address Translation for FOX-MAN-UN Element Agents"). Restoration makes sense and thus running of the database fix script is highly recommended in case you import a database of a partner server (e.g. database of Main Server on Standby Server or vice versa).

Following steps 3 to 5, the user selects a database backup file that resides in a specific location on the source server and will be restored to the database of the source server.

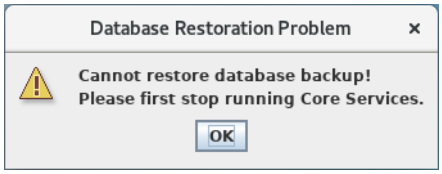
Clicking on the <Restore Selected Backup> button on the <Restore Backup Database> dialog will display a warning that the currently used database will be deleted.

Confirming the message by clicking on the <Yes> button will start the restoration operation.



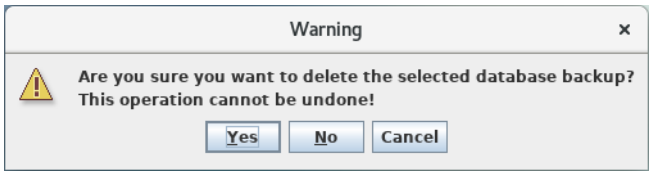
A successful restoration will be confirmed upon completion.

Please note:
Restoration of a backup is only possible if the core services of the server where the backup shall be restored are stopped. If this is not the case the RAT will display a dialog informing the user that there is problem restoring the backup due to running core services.



6.1.10.2 Delete Selected Backup

A selected database backup can also be deleted. Clicking on the <Delete Selected Backup> button on the <Restore Database Backup> dialog will delete the backup after clicking on the <Yes> button on the shown warning message.



6.1.10.3 Upload Backup

The <Restore Database Backup> dialog offers to upload a database backup to a server. Thereto the user must carry out the following steps:

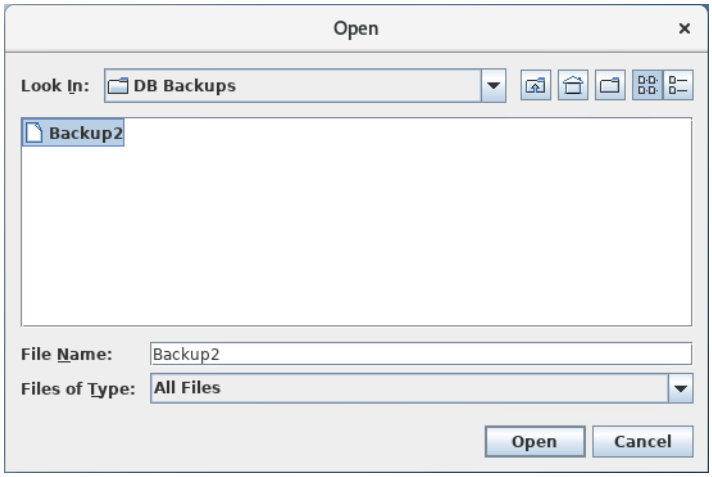
1 Selection of a backup source server.

Please note:
Only the server to which the Remote Admin Tool is connected can be selected for this operation.

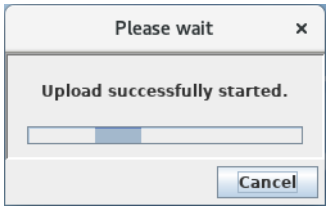
2 Selection of a backup location on the source server

Following above steps, the user selects a specific location on the source server to which the database backup file will be uploaded.

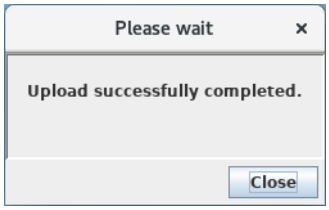
Clicking on the <Upload Backup> button on the <Restore Database Backup> dialog will show an <Open> dialog.



Selecting an appropriate database backup file on the client machine and clicking on the <Open> button will start the upload operation.



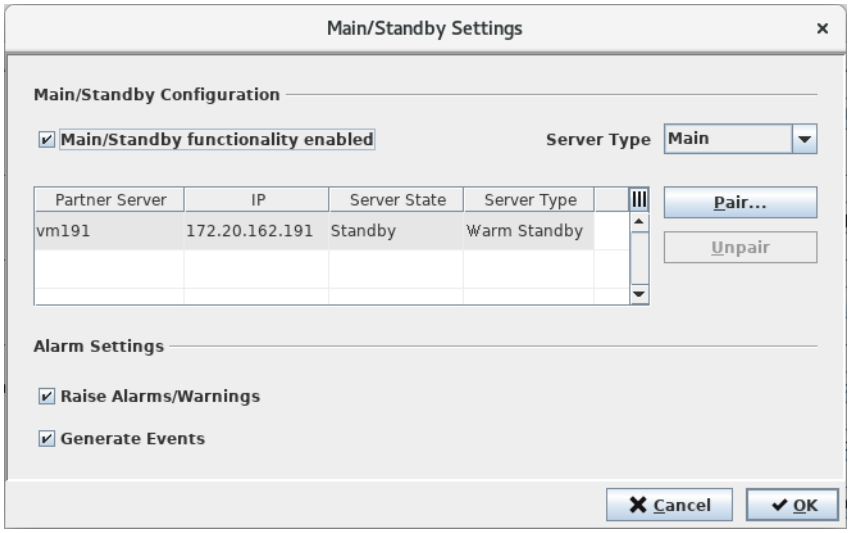
A successful upload will be confirmed upon completion.



6.1.11 Main/Standby Settings Dialog

6.1.11.1 Overview

Clicking on the <Main/Standby Configuration…> button on the Main Window of the RAT will open its <Main/Standby Settings> dialog.



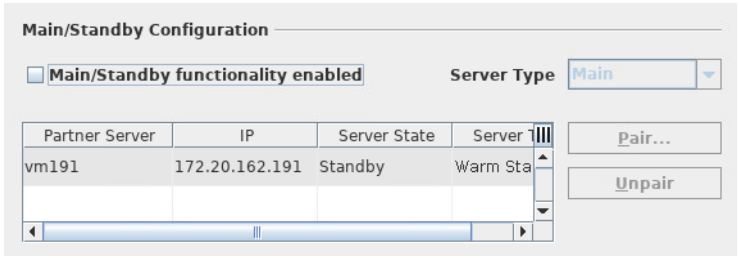
The dialog allows the following settings on the server to which the RAT is connected:

- activation of the Main/Standby functionality
- definition of the Server Type
- pairing or unpairing of a partner server
- activation of alarm/event generation

To save all settings done on the dialog, the <OK> button must be clicked. This will write all settings permanently to the server to which the RAT is connected and close the dialog.

6.1.11.2 Activation of Main/Standby functionality and definition of Server Type

The Main/Standby functionality of the server to which the RAT is connected can be enabled via the corresponding check box on the dialog. As soon as the check box is ticked, the user can select a server type and pair a partner server. If the check box stays unticked, both <Server Type> combo box and <Pair…> button are disabled and the server automatically is set to type “Standard”, what becomes visible on the RAT’s Main Window.



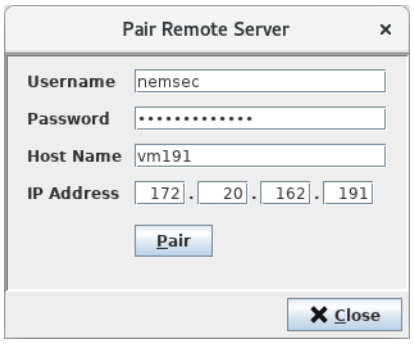
The <Main/Standby functionality> check box can only be ticked if at least a periodic database backup every n minutes, and/or a daily backup has been scheduled in the <Schedule Periodic Database Backup> dialog. If not, a configuration inconsistency message will be shown.

6.1.11.3 Pairing and unpairing of partner server(s)

Clicking on the <Pair…> button will allow the user to pair the server to which the RAT is connected with a partner server. In order the pairing operation be possible, the following conditions must be fulfilled:

- A server of type “Main” can be paired with one or several servers of type “Cold Standby” or “Warm Standby”.
- A server of type “Cold Standby” or “Warm Standby” can be paired with exactly one server of type “Main”.
- The Main/Standby functionality of the remote server that shall be paired must be enabled.
- The remote server that shall be paired must be in state “Not Running” or “Running” in case of a Main Server or in state “Standby” or “Running” in case of a Standby Server.

In the displayed <Pair Remote Server> dialog, NEM security administrator username and password, hostname, and IP address of the remote server must be provided.



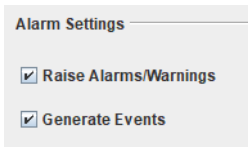
Clicking the <Pair> button on this dialog will finally perform the pairing operation. Successful pairing will be confirmed through a message box.

An existing pairing of two servers can also be undone. The <Unpair> button does offer this functionality. Again, some conditions must be fulfilled:

- The remote server that shall be unpaired must be in state “Not Running” or “Running” in case of a Main Server or in state “Standby” or “Running” in case of a Standby Server.

6.1.11.4 Activation of Alarm and Event generation

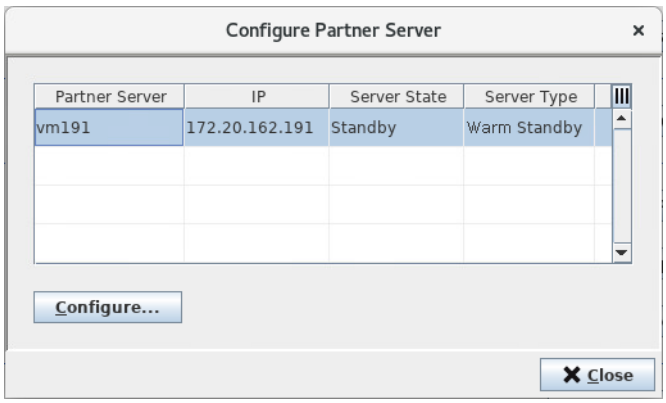
The <Main/Standby Configuration> dialog also allows activation or deactivation of alarm and event generation.



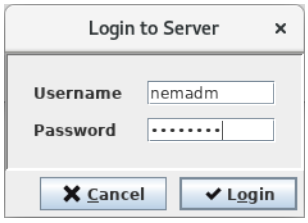
If ticked alarms and events will be generated on the server to which the RAT is connected according to the table shown in chapter 4.7.1 "Alarm and Event Types". If not ticked, no alarms and events will be generated.

6.1.12 Configure Partner Server Dialog

Clicking on the <Configure Partner Server…> button on the Main Window of the RAT will open its <Configure Partner Server> dialog.



The dialog allows launching a new instance of the Remote Admin Tool for a partner server of the server to which the RAT is currently connected. Selecting a server in the shown list and clicking on the <Configure…> button will open a login dialog for the selected server.



Providing the correct credentials and clicking on the <Login> button will launch a separate instance of the Remote Admin Tool for the selected server. The primary Remote Admin Tool stays open and its <Configure Partner Server> dialog closes automatically.

6.1.13 Switchover Settings Dialog

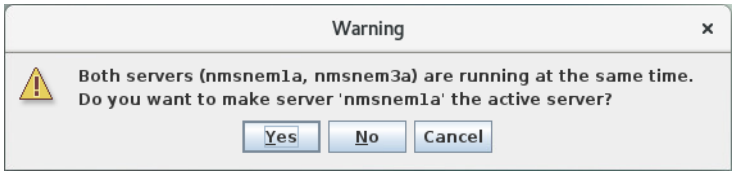
The <Make This Server Active …> button is intended for activation of the server to which the RAT is connected. The operation is also called “Easy Switchover”. The button is only enabled if the server is paired with at least one partner server.

6.1.13.1 Switchover with one Partner Server

If the button <Make This Server Active …> is clicked and the server is already active (its core services are already running) and the partner server is not active (its core services are not running) this will be indicated through a corresponding message box.

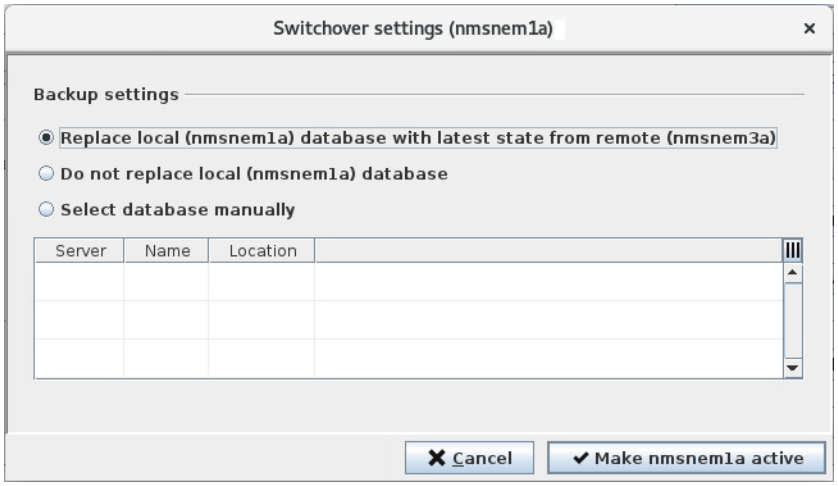
Clicking the <OK> button will terminate the activation operation (nothing to be done).

If the <Make This Server Active …> button is clicked and the server is already active (its core services are already running) and the partner server is also active (its core services are also running) this will be indicated through a corresponding message box.



Clicking the <Yes> button will open the <Switchover settings> dialog.

If the <Make This Server Active …> button is clicked and the server is not yet active (its core services are not running) the <Switchover settings> dialog will open.



The <Switchover settings> dialog allows for easy activation of the server to which the RAT is connected. Activation on the one hand signifies to start up the server's core services if they are not yet running and on the other hand to shut down the core services of the partner server if they are running.

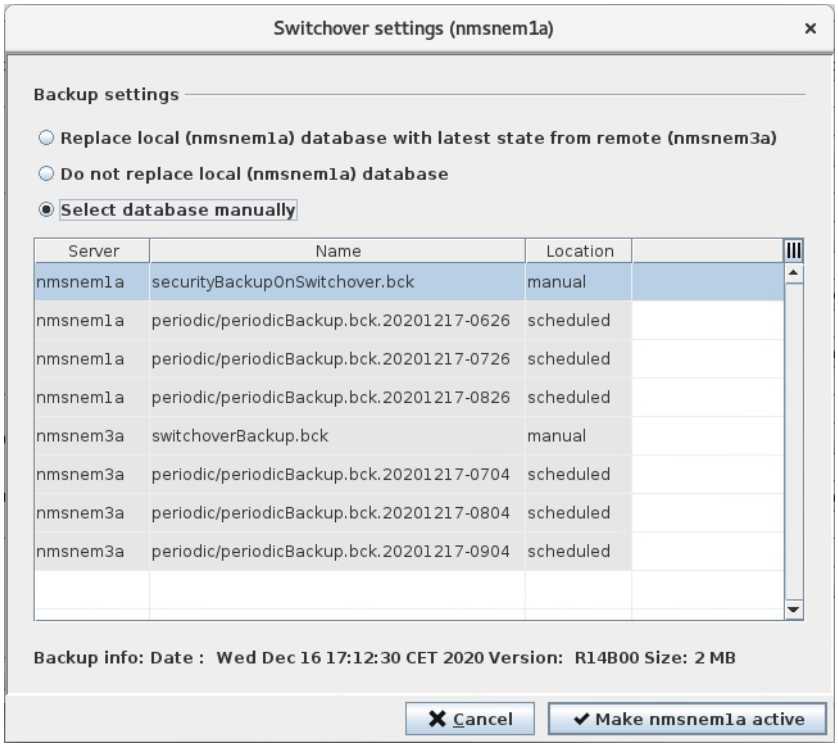
Before the actual activation procedure can take place, the user must decide how to cope with the local database. Three options are available for selection:

- Replace local database with latest state from remote

  The database of the server that shall be activated will be replaced with the latest one from the partner server.
- Do not replace local database

  The database of the server that shall be activated will not be replaced at all.
- Select database to replace local database with manually.

  The database of the server that shall be activated will be replaced by one chosen by the user. Databases available on the server to be activated or on its partner server are at offer.

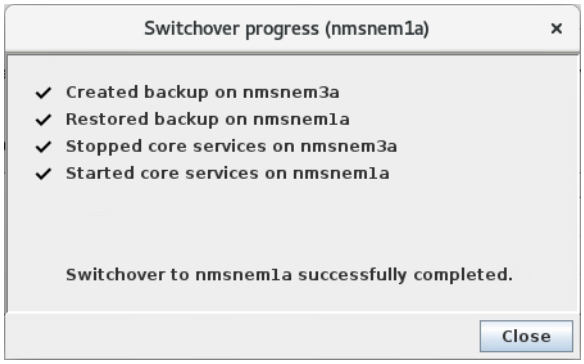


After the user has decided upon what shall happen with the local database, they can press the <Make xyz active> button on the <Switchover Settings> dialog. In case the local database will be replaced, a warning dialog, stating that the currently used local database will be overwritten, must be confirmed. Then the following steps will be carried out for the activation of the server depending on the different scenarios how to treat the local database.

	Activation (switchover) steps on Local Server (server to be activated) and Partner Server	**Remark**
Option "Replace local database with latest state from remote"	1 Backup database on the partner server. 2 Transfer partner database backup from the partner to the local server. 3 Take a security backup of the local database. 4 Restore the partner database backup on the local server. 5 Stop the core services on the partner server if they are running. 6 Start the core services on the local server if they are not already running.	Step 1: This database backup can be found on the partner server under /opt/nem/var/backups/manual/switchoverBackup.bck Step 3: This database backup can be found on the local server under /opt/nem/var/backups/manual/securityBackupOnSwitchover.bck REMARK! Only one backup of each type will be kept (backups will be overwritten).
Option "Do not replace local database"	1 Stop the core services on the partner server if they are running. 2 Start the core services on the local server if they are not already running.	

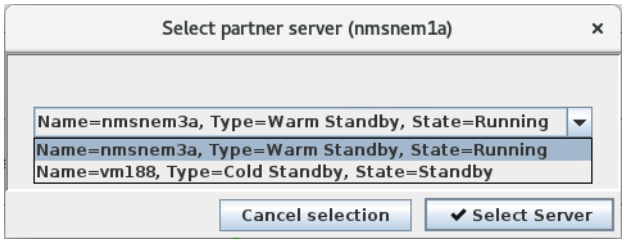
	Activation (switchover) steps on Local Server (server to be activated) and Partner Server	Remark
Option "Select database manually"	1 Take a security backup of the local database. 2 Restore the database backup selected by the user on the local server. 3 Stop the core services on the partner server if they are running. 4 Start the core services on the local server if they are not already running.	Step 1: This database backup can be found on the local server under /opt/nem/var/backups/manual/securityBackupOnSwitchover.bck REMARK! Only one backup will be kept (backup will be overwritten).

The switchover progress is shown in a corresponding dialog where most important steps according to above table are listed and a successful switchover operation is finally indicated.



6.1.13.2 Switchover with more than one partner server

The switchover operation with more than one partner server in principal works like the one with only one partner server. The only difference is that the user first has to select the partner server for which the switchover operation shall be carried out as the operation always applies for one main/standby server pair. As a main server can have many standby servers (one to many relation) but every standby server can only have one main server (one to one relation) this use case can only occur if the user wants to activate a main server that has more than one standby server as partners. In this case, after pressing the <Make This Server Active …> button on the <Switchover settings> dialog, the <Select partner server> dialog will be shown.



Once the partner server is selected, the further operation steps will simply follow the switchover scenario with one partner server.

6.2 Configuration File

Settings done in the <Schedule Periodic Database Backup> and <Main/Standby Settings> dialogs of the Remote Admin Tool (refer to chapters 6.1.8 "Schedule Periodic Database Backup Dialog" and 6.1.11 "Main/Standby Settings Dialog") are stored in the mainstandby.conf file which resides in folder /opt/nem/etc of the corresponding FOXMAN-UN server.

For a typical Main/Standby installation the file does not need manual adaptation, however in some situations the user might want to change some individual parameters. Following an overview of the file contents and its meaning:

```
{
  "serviceEnabled": true,                       Main/Standby service enabled/disabled
  "alarmsEnabled": true,                        Alarm generation enabled/disabled
  "eventsEnabled": true,                        Event generation enabled/disabled
  "skipSecurityBackup": false,                  Skipping of database security backup at server
                                                activation (easy switchover) enabled/disabled
  "serverType": {
    "serverType": "MAIN"                        Server type [MAIN, WARMSTANDBY, COLDSTANDBY]
  },
  "partnerServers": [                           A list of partner servers
    {
      "localServer": {                          The server on which this file resides (local
        "ip": "172.20.162.190",                 server) with its IP address, host name and
        "name": "vm190",                        server type
        "serverType": "MAIN"
      },
      "remoteServer": {                         The first partner server of the local server with
        "ip": "172.20.162.191",                 its IP address, host name and server type
        "name": "vm191",                        Other remote servers might be specified in case
        "serverType": "WARMSTANDBY"             the local server is of type "MAIN"
      }
    }
  ],
  "backupLocationList": [                       A list of backup locations on the local server
    {
      "location": "manual",                     Identifier of the manual backup location
      "name": "Manual backups",                 Name of manual backup location shown in RAT
      "folder": "/opt/nem/var/backups/manual",  Storage location of manual backups on server
      "visible": true                           If this location shall be visible in RAT or not
    },                                          REMARK! Do not modify this section!

    {
      "location": "scheduled",                  Identifier of the scheduled backup location
      "name": "Scheduled backups",              Name of scheduled backup location shown in RAT
      "folder": "/opt/nem/var/backups/scheduled",    Storage location of scheduled backups on server
      "visible": true                           If this location shall be visible in RAT or not
    },                                          REMARK! Do not modify this section!
    {
      "location": "fromRemote",                 Identifier of the remote backup location[1]
      "name": "Cache copy of remote backups",   Name of remote backup location shown in RAT
      "folder": "/opt/nem/var/backups/remote",  Storage location of remote backups on server
      "visible": false                          If this location shall be visible in RAT or not
    }                                           REMARK! Do not modify this section!
  ],                                            Additional backup sections might be
                                                added if desired.

  "backupLocation": {                           Definition of which location all scheduled
    "location": "scheduled"                     backups on the local server shall be stored to
  },
  "cacheLocation": {                            Definition of which location all remote backups
    "location": "fromRemote"                    on the local server shall be stored to
  },
  "backupSchedule": {                           Database backup schedule
    "periodicBackup": true,                     For the meaning of the individual
    "periodicBackupMinutes": 240,               parameters refer to chapter section 6.1.8
    "periodicBackupKeepLast": 3,
    "dailyBackup": true,
    "dailyBackupHour": "00:00",
    "dailyBackupKeepLast": 3,
    "weeklyBackup": false,
    "weeklyBackupWeekDay": "Friday",
    "weeklyBackupHour": "23:00",
    "weeklyBackupKeepLast": 3,
    "monthlyBackup": false,
```

1. The backup location where the local server stores copied over backups from the remote server(s).

```
    "monthlyBackupDay": 1,
    "monthlyBackupHour": "23:30",
    "monthlyBackupKeepLast": 3
  },
  "pingSettings": {                          Ping settings for local server pinging remote one
    "interval": 30,                          Ping interval in seconds
    "maxMissingPings": 2                     How many pings can be missed
  },
  "copyOverSettings": {                      Interval settings for local server copying over
                                             database backups from remote server
    "interval": 2                            Interval in minutes
  }
  "backupSettings": {                        Backup timeout settings
    "timeoutMin": 30,                        Backup timeout duration in minutes
    "killOnTimeout": true
  }
}
```

Ping Settings and Copy Over Interval are not configurable via Remote Admin Tool.

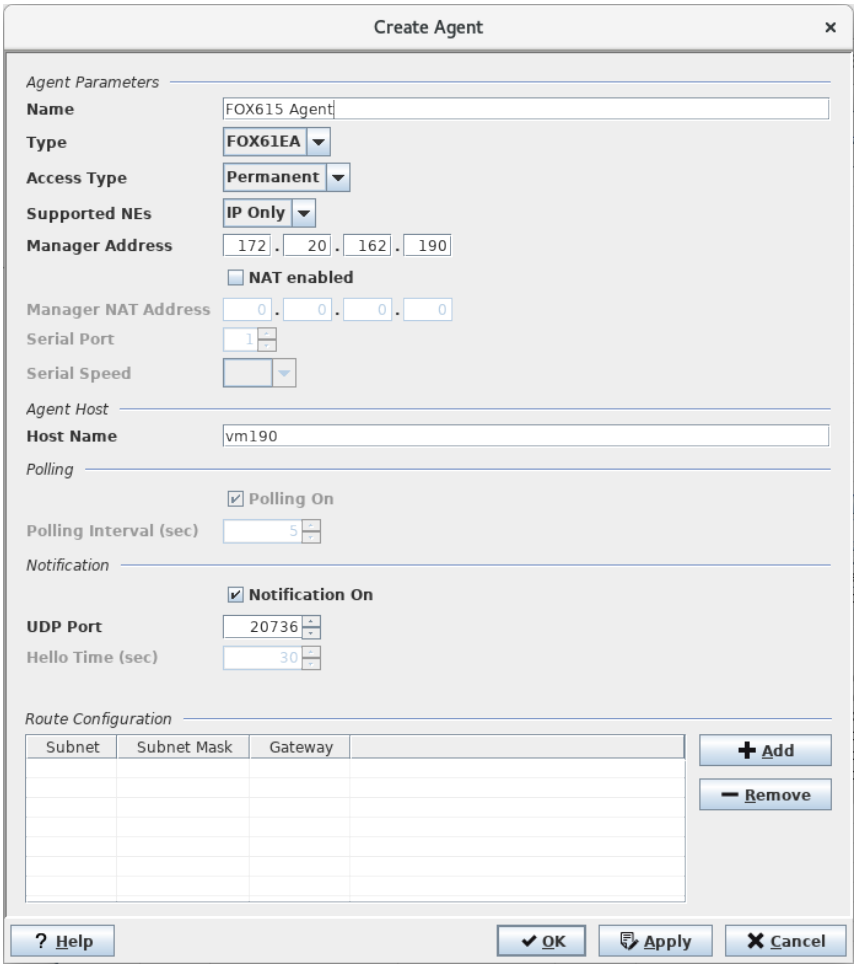
6.3 IP Address Translation for FOXMAN-UN Element Agents

6.3.1 Initial Situation

In order FOXMAN-UN be capable of managing equipment so called Element Agents must be defined in its NEM Configurator. An Element Agent basically defines a Gateway from FOXMAN-UN to equipment of a certain type and vice versa. The most important parameters of such an Agent are:

- Name
- Type
- Manager Address
- Host Name
- UDP Port

Following as an example the parameters of an Element Agent of type FOX61EA as defined in FOXMAN-UN:



Agent parameters are stored in the FOXMAN-UN database and thus are part of the database copy over operation from Main to Standby and vis versa in case the Main/Standby Solution is used. As Main and Standby Servers must have different Host Names and IP addresses for its network interface cards it becomes obvious that Host Names and IP addresses of Element Agents must be exchanged after the database copy over operation has occurred.

Taking the Network Setup of chapter 3.1 "Network Setup" as an example imagine that we have two servers with to Element Agents defined as follows:

Main Server		**Standby Server**	
Hostname	nmsMain	Hostname	nmsStandby
Network C IP	172.20.162.223	Network D IP	192.168.32.148

FOX61x Agent in FOXMAN-UN of Main Server		**FOX61x Agent in FOXMAN-UN of Standby Server**	
Name	FOX61x Agent	Name	FOX61x Agent
Manager Address	172.20.162.223	Manager Address	192.168.32.148
Host Name	nmsMain	Host Name	nmsStandby

It becomes obvious that after the database of the Main Server, containing the FOX61x Agent data, has been copied over to the Standby Server must be adapted to reflect the corresponding FOX61x Agent data on the Standby Server. Meaning IP address 172.20.162.223 must be replaced through 192.168.32.148 and hostname “nmsMain” must be replaced by “nmsStandby”. The same of course also applies for the opposite operation, namely when copying the Standby Server database to the Main Server. Thereafter, IP address 192.168.32.148 must be replaced through 172.20.162.223 and hostname “nmsStandby” must be replaced by “nmsMain”.

6.3.2 Implementation IP Address Translation

6.3.2.1 Standard Implementation

The Standard implementation of IP Address Translation for the Main/Standby Solution has been implemented the following way:

- Any database imported on the Main Server or the Standby Server is not altered through the actual database import operation.
- After the import has taken place, hostname and IP address of any Element Agent in the database will be replaced according to the following rules:
  - the IP address assigned to the hostname of the server where the database import has occurred is taken from the server's host file. After this step, the server hostname and its IP address are known as "server_hostname" and "server_ip".
  - all IP addresses of Element Agents in the imported database that do not equal to 127.0.0.1 are replaced by "server_ip".
  - all hostnames of Element Agents in the imported database that do not equal to "localhost" are replaced by "server_hostname".

This standard implementation is sufficient for simple network setups where Main and Standby Server each just have one network interface to the equipment network whose IP address is assigned to the server's hostname.

6.3.2.2 Customization

For more complex network setups with several network interfaces and IP addresses to the equipment the user can customize the IP translation for Element Agents as follows:

- On every Server there is file named "iptranslate.conf.template" in the folder /opt/nem/etc.
- Change the file name to "iptranslate.conf". This will activate the customization.
- Open the file with an editor. Its content will look as follows:

```
# replace manager ip's in NEM database
# Format is <FromIP>=<ToIP>
# eg. 172.20.162.99=172.20.162.206
```

- Add all Element Agent IP addresses from a remote server (or remote servers) that need to be replaced through a specific IP address of the local server to the file (taking the example of chapter 6.3.1 "Initial Situation" the entry "172.20.162.223=192.168.32.148" must be added to the file on the Standby Server, and the entry "192.168.32.148=172.20.162.223" must be added to the file on the Main Server).
- Save the file.

After a database import has taken place, hostname and IP address of any Element Agent in the database will now be replaced according to the following rules:

- If for a specific Element Agent IP address, no IP assignment entry can be found in the "iptranslate.conf" file, this IP address will not be replaced at all.
- If for a specific Element Agent IP address, an IP assignment entry in the form IP1=IP2 can be found in the "iptranslate.conf" file, IP1 will be replaced by IP2 unless IP1 is equal 127.0.0.1. (in other words, entries in the form 127.0.0.1=IP2 will be neglected).
- The hostname of every Element Agent in the imported database that does not equal to "localhost" is replaced by the server's hostname in case also the Agent's IP address has been replaced in the previous steps.

6.4 IP Address Translation for ALS Equipment Managers

If ALS is used together with FOXMAN-UN the same problem with IP address translation of Equipment Managers applies as for native FOXMAN-UN Element Agents. Some Equipment Managers offered by ALS listen for SNMP alarm traps on specific IP addresses and ports. The

corresponding parameters can be specified per Manager in the ALS Configurator on the respective Manager's SNMP tab. The parameters are named as follows:

- Manager SNMP Trap Reception IP
- Manager SNMP Trap Reception Port

These two parameters are stored in the ALS database which is part of any database dump taken on the Main Server. After transfer of the dump to the Standby Server there is no mechanism in place that replaces a defined Manager SNMP Trap Reception IP valid for the Main Server with the corresponding one on the Standby Server. That means, after import of the database dump on the Standby Server, ALS would not be able to start the corresponding Manager's trap handler (listener) due to an incorrect IP address in the ALS database.

In order to solve this issue, the ALS on the Standby Server must make use of a specific file where a mapping between trap reception IPs of the Main Server and trap reception IPs of the Standby Server can be defined. The file does not exist and must be created by the user on the Standby Server as follows:

`/var/lib/ABB/FOXMAN/ALS28/config/TrapIpTranslation.properties`

On the Main Server the file is not needed and thus does not need to be created.

After creation of the file on the Standby Server, entries in the form IP1=IP2 can be added, e.g. “172.20.162.223=192.168.32.148”.

Every line in the file signifies that on the Standby Server ALS starts all trap handlers (listeners) on IP2 whose parameter “Manager SNMP Trap Reception IP” equals to IP1 on the Main Server. Additional entries can be appended to the file in order to consider additional SNMP Trap Reception IPs. For instance, if there is an Equipment Manager in ALS that listens for traps on IP 172.20.162.112 on the Main Server and shall listen for traps on IP 192.168.32.112 on the Standby Server, the following entry must be appended to the file:

```
172.20.162.112=192.168.32.112
```

The entire file then would read as follows:

```
172.20.162.223=192.168.32.148
172.20.162.112=192.168.32.112
```

Please note:
It is also possible to specify 0.0.0.0 as SNMP Trap Reception IP for an ALS Equipment Manager signifying that the corresponding trap receiver listens on all available Ethernet Interfaces (IP addresses) of the system for incoming traps. This address of course does not need an entry in the file TrapIpTranslation.properties as 0.0.0.0=0.0.0.0 becomes superfluous. The problem with specifying 0.0.0.0 as trap reception IP is that it cannot be used for automatic trap subscription through ALS as every equipment needs configuration of a specific Trap Reception IP in order to know where to send its traps to[1].

1. ALS offers automatic SNMP Trap Subscription for some of its Equipment Mangers. This means that it registers the corresponding Equipment Manager's SNMP Trap Reception IP and SNMP Trap Reception Port on every respective equipment that it supervises.

7 Troubleshooting

7.1 Log Files

The FOXMAN-UN Main/Standby Solution offers log files to investigate on possibly occurring problems. Various log files can be found as listed below:

Component	File Name	Location	Remark
FOXMAN-UN Voyager - Main/Standby Service	nem-bp-mainstandby.log	/opt/nem/var/log	
Remote Admin Tool	remoteadmintool.log	/opt/nem/var/log	Linux Client
	remoteadmintool.log	c:\Program Files (x86)\FOXMAN-UN_UI_R$\var\log	Windows Client

Property files to control the logging level and logged packages or classes can be found as follows:

Component	File Name	Location	Remark
FOXMAN-UN Voyager - Main/ Standby Service	mainstandby.properties	/opt/nem/voyager/etc	
Remote Admin Tool	remoteadmintool_log.properties	/opt/nem/client/etc	Linux Client
	remoteadmintool_log.properties	C:\Program Files (x86)\FOXMAN-UN_UI_R$\etc	Windows Client

8 Important Notes

Initially both systems, Main and Standby, have been equally configured with regard to managed devices. However, configuration might change over time as parameters of existing devices are changed, new devices are added, or existing devices removed. The following rules must be applied when such changes occur.

Rules:

- If new native devices (e.g. FOX515, FOX61x) are added/removed on/from the Main System, the devices do not need to be added/removed on/from the Standby System too.
- If new devices are added/removed to/from an existing ALS Manager on the Main System, the devices do not need to be added/removed on/from the Standby System too.
- IP routes to equipment networks must be configured both on the Main and the Standby System.
- If a new ALS Manager is added or an existing one's parameters changed on the Main System, the corresponding changes do not need to be applied to the Standby System.
- If a new cross-launch type for ALS-managed equipment is added or an existing one's parameters changed on the Main System, the same changes must also be applied on the Standby system.

9 Document History

Date	Release	Rev.	Comments
2019-09-02	FOXMAN-UN R11B	A	First version.
2019-12-11	FOXMAN-UN R11B	B	Revised version for release R11B.
2020-03-04	FOXMAN-UN R11B SP01	C	Added cross reference in section 5.1 referring to section 6.3.
2020-07-15	FOXMAN-UN R14A	A	Updated section 6.1.1 "Overview" and reworked section 6.1.6 "Services Management Dialog" for new major release. Corrected standby server type terminology.
2021-01-15	FOXMAN-UN R14B	A	Updated for current system release. Added section 6.1.13 "Switchover Settings Dialog".
2021-03-15	FOXMAN-UN R14B	B	Revised database restore options (6.1.10 "Restore Database Backup Dialog") and mainstandby.conf contents (6.2 "Configuration File").
2021-07-23	FOXMAN-UN R15A	A	Updated for current system release.
2022-02-02	FOXMAN-UN R15B	A	Updated for current system release. Updated document branding.
2022-09-02	FOXMAN-UN R16A	A	Updated for current system release.
2023-02-24	FOXMAN-UN R16B	A	Updated for current system release. Updated document branding.
2024-09-02	FOXMAN-UN R17A	A	Updated for current system release.
2025-09-30	FOXMAN-UN R17A	B	Updated note on NP Resync in 6.1.6.4 "Networking Package Resynchronization".
2025-10-10	FOXMAN-UN R18	A	Updated for current system release.

Hitachi Energy Ltd
Bruggerstrasse 72
5400 Baden - Switzerland

Phone: please refer to https://www.hitachienergy.com/contact-us/Customer-Connect-Center (Customer Connect Center)
Email: communication.networks@hitachienergy.com

www.hitachienergy.com/communication-networks

Document ID: 1KHW029097 R18 Rev. A