

Initial Configuration Guide

Virtual Multimedia Resource Function

User Guide

Copyright

© Ericsson AB 2016, 2017. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.



Contents

1	About This Document	1
2	vMRF Initial Configuration Tasks	2
3	Configure vMRF Application	3
3.1	Importing Configuration Data from NETCONF Template	4
3.2	Create and Import Configuration Data	4
3.3	Manual Configuration	5
3.4	Initial Configuration Data for the vMRF Application	8
4	Configure SNMP for Fault Management	10
5	Configure the networkManagedElementId Attribute	11





1 About This Document

This document describes the configuration that is a prerequisite for vMRF to process traffic. The configuration tasks in this document are performed after the vMRF VNF has been deployed using the relevant *deployment instructions*.

This document is written for vMRF operator personnel who are responsible for the deployment of vMRF. The vMRF operator is assumed to be a cloud service consumer on a cloud service.



2 vMRF Initial Configuration Tasks

Initial configuration includes the following tasks:

Steps

- vMRF application and security configuration. This is a mandatory configuration task. See [Configure vMRF Application](#) on page 3.
- SNMP configuration for fault management. This is a recommended configuration task. See [Configure SNMP for Fault Management](#) on page 10.
- Configuration of the `networkManagedElementId` attribute in the *ManagedElement* MO. This is a recommended configuration task. See [Configure the networkManagedElementId Attribute](#) on page 11.
- Performance management jobs configuration. This is a recommended configuration task, for more information refer to *Performance Management*.

3 Configure vMRF Application

Initial vMRF application configuration consists of configuring user plane networks and H.248 signaling links.

The following methods are available, as shown in [Figure 1](#):

- Importing configuration data using the deployment template during instantiation, as described in the relevant *deployment instructions* (the deployment template references the NETCONF template that contains the actual configuration data), and configuring security, as described in [Additional Security Configuration](#) on page 5.
- Importing configuration data using the deployment template and configuring security after instantiation, as described in [Importing Configuration Data from NETCONF Template](#) on page 4.
- Manual configuration after instantiation, as described in [Manual Configuration](#) on page 5.

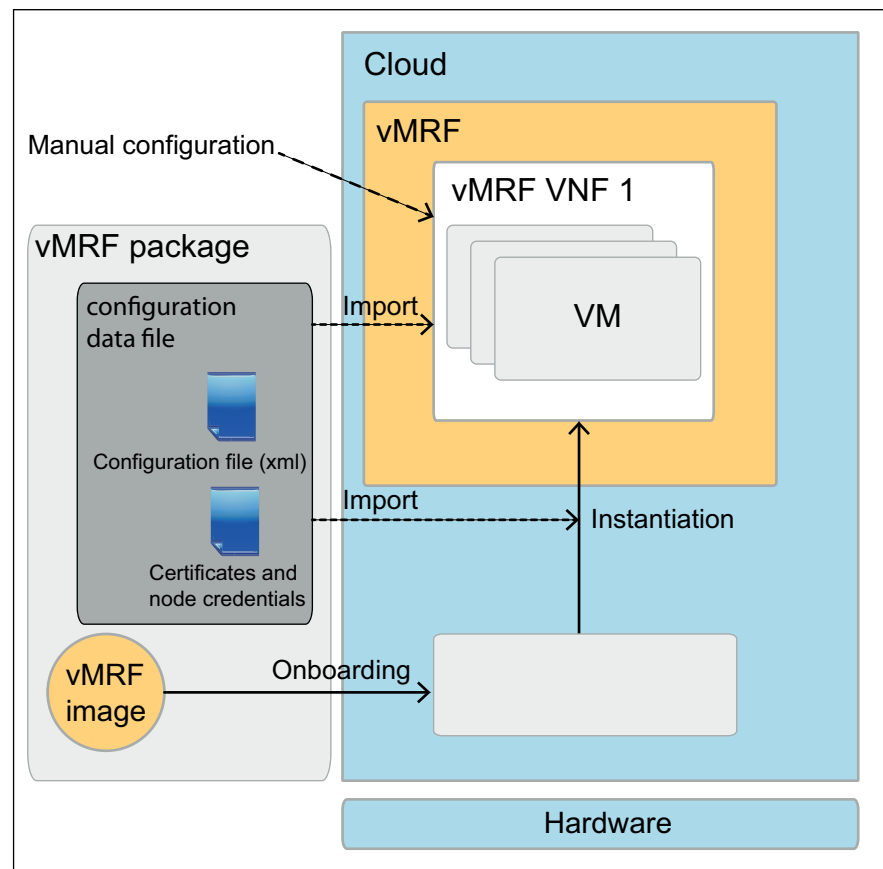


Figure 1 Options for Initial Configuration of vMRF Application



3.1 Importing Configuration Data from NETCONF Template

An example initial configuration file is part of the vMRF software delivery package, with the name `example_config.tar.gz`.

The `tar.gz` file contains the following:

- An XML file that contains MO configuration values. The example `tar.gz` file contains an example XML file with the name `config.xml`. You must edit the XML file with values that match your environment, as described in the procedure below. As an optional service, Ericsson can provide a file that is already edited to match your environment.
- Node credentials: You must add the node credentials to the `tar.gz` file, as described in the procedure below.
- Trusted certificates: You must add the trusted certificates to the `tar.gz` file, as described in the procedure below.
- `manifest.yaml`: The file contains configuration metadata for the import and the contents of `/usr/share/image/package_build_data` for troubleshooting.

Note: You must manage the content of the `tar.gz` file using a Python script that is also delivered in the vMRF software delivery package. To run the script, you need Python installed on a Linux computer.

3.2 Create and Import Configuration Data

This procedure describes how to create and import the initial configuration data.

Steps

1. Extract the XML file from the tar file for editing using the `vmrs_config_update.py` script:

```
vmrs_config_update.py -c example_config.tar.gz -gxf config.xml
```
2. Edit the XML file with specific values for your environment, as described in the relevant *deployment instruction*. For a list of MOs and attributes to configure, see [Initial Configuration Data for the vMRF Application](#) on page 8.

Note: The XML document is case-sensitive, pay attention when editing MO names and attributes.



3. Pack the XML file back into the `tar.gz` file, using the `vmrs_config_update.py` script:

```
vmrs_config_update.py -c example_config.tar.gz -sxf
config.xml
```

4. Add the node credentials and trusted certificates to the tar file, and set the LDAP password using the `vmrs_config_update.py` script:

```
vmrs_config_update.py -c example_config.tar.gz -anc
key.pem cert.pem -atc <trusted_certificate>.pem ldap
<password>
```

5. Open an SSH connection to the O&M IP address of the vMRF VNF using the following command:

```
ssh <user ID>@<O&M IP address>
```

6. Copy the modified `tar.gz` file to the VNF using, for example, `scp`:

```
scp example_config.tar.gz <user ID>@<O&M IP address>:/
home/<user ID>
```

Result

The configuration file is copied from the current directory to the `/home/<user ID>` folder in the file system of the vMRF VNF.

7. Run the following command:

```
/opt/mrf_director/mrf_import_conf.py /home/<user ID>/
example_config.tar.gz
```

Emergency user credentials are needed to perform this step.

Result

The configuration data is imported and vMRF connects to the user plane and signaling networks.

3.2.1 Additional Security Configuration

Configure security as described in *vMRF Security Management*. Skip the installing node credentials and trusted certificates configuration steps, as they were already performed during the configuration data import procedure.

3.3 Manual Configuration

Manual configuration means configuring each MO and MO attribute using the ECLI or a NETCONF client. Manual configuration requires emergency user credentials.

If ECLI is used, do the following:



Steps

1. Connect to the O&M IP address of the vMRF VNF by issuing the following command:

```
ssh <user ID>@<O&M IP address>
```

2. Start a session by issuing the `cliss` command

If a NETCONF client is used, connect to the O&M IP address of the vMRF VNF using the client.

3.3.1 Configure vMRF User Plane

Do the following:

Steps

1. In the MOM, navigate to `ManagedElement=1,MediaResourceFunction=1`. Check that the `mediaIpVersion` attribute is configured correctly. `mediaIpVersion` is visible only in configure mode.

Note: The `mediaIpVersion` attribute is only visible in configure mode.

See [Table 1](#) for the details.

3.3.2 Configure vMRF Signaling

Do the following:

Steps

1. In the MOM, navigate to `ManagedElement=1,MediaResourceFunction=1,MrfH248Control=1`, and create a *MrfH248Interface* MO for the H.248 connection.

In the created *MrfH248Interface* MO, configure the following attributes:

- `mrFH248InterfaceId`
- `remoteIpAddress`
- `remotePortNumber`

2. To activate the H.248 link towards the MTAS, set the administrative state of the given *MrfH248Interface* MO to `UNLOCKED`.

See [Table 2](#) for the details.



3.3.3 Create a Basic Announcement

This procedure describes how to create a *BasicAnnouncement* MO, that represents a single audio announcement file.

Prerequisites

- An Ericsson Command-Line Interface (ECLI) session in Exec mode is open.
- The announcement files are available on the announcement storage server or in the local storage.

Steps

1. In the MOM, navigate to **ManagedElement=1,MediaResourceFunction=1,Announcements=1,BasicAnnouncements=1** and create a *BasicAnnouncement* MO for each audio announcement file.
2. For each created *BasicAnnouncement* MO, define values for the following attributes:
 - **announcementId**

An identity for the basic announcement. The combination of the **announcementId** and **languageCode** attributes form a unique identity for the basic announcement.
 - **basicAnnouncementId**

The value component of the RDN.
 - **fileName**

The name of the announcement file.
 - **filePath**

The relative file path to the directory where the announcement file is stored. The value of this attribute is relative to the **announcement_storage_server_path** attribute in the deployment template. In case of local storage the value of the attribute is relative to **/cluster/storage/announcements**.

Example: **basic/en-GB/**
 - **languageCode**



Language code of the basic announcement. The combination of the `announcementId` and `languageCode` attributes form a unique identity for the basic announcement.

Language code has the format of an RFC 5646 language tag.

Example: en-GB

The following attributes are optional:

- `duration`

The amount of time the announcement is to be played in milliseconds. If the specified duration is greater than the overall length of the announcement, the announcement is repeated until the duration is elapsed. The playing time is also dependent on the value of the `iteration` attribute. The selected playing time is always the shortest possible alternative.

- `iteration`

The number of times the announcement is repeated when played to the user.

- `userLabel`

Label for free use.

3.3.4 Configure Security

For information on security configuration, refer to *vMRF Security Management*.

3.4 Initial Configuration Data for the vMRF Application

Table 1 vMRF Network Attributes

ManagedElement=1,MediaResourceFunction=1	
mediaIpVersion	Possible values: <ul style="list-style-type: none">• IPV4 (default)• IPV4_IPV6• IPV6



Table 2 vMRF Controlling Server Attributes

ManagedElement=1,MediaResourceFunction=1, MrfH248Control=1, MrfH248Interface=<interface ID>	
remoteIpAddress	IP address of the controlling server
administrativeState	State of H.248 link
remotePortNumber	Remote port of the controlling server

Table 3 SCTP Profile Attributes

ManagedElement=1,Transport=1,SctpProfile=1	
dscp	
heartbeatInterval	
initRto	
maxBurst	
maxRto	
maxInitRt	
minRto	
sackTimer	
assocMaxRtx	
pathMaxRtx	
primaryPathMaxRtx	
alphaIndex	
betaIndex	
cookieLife	



4 Configure SNMP for Fault Management

The Simple Network Management Protocol (SNMP) provides alarm notifications.

The used SNMP version must be consistent with the SNMP targets used in the network fault management system. The recommended SNMP version is SNMPv3.

Do the following:

Steps

1. Create SNMP targets using one of the following instructions:

- *Create SNMPv1 Target*
- *Create SNMPv2C Target*
- *Create SNMPv3 Target*

Note: To prevent modification of the management information base (MIB) files through SNMP, the `isMibWritable` attribute of the SNMP target MOs is recommended to be set to `false` during the creation of the target.

2. SNMP views can be created to restrict read/write access to SNMP MIBs. It is recommended to grant SNMP access only to the ERICSSON-ALARM-MIB, that is needed for fault management purposes. This can be done by creating an SNMP view with `readOids` attribute set to 1.3.6.1.4.1.193.183 using the instruction *Create SNMP View*.

For the default SNMP settings, refer to the *Snmp* MO in the MOM.

For more information on fault management, refer to *Fault Management*.



5 Configure the networkManagedElementId Attribute

This procedure describes how to configure the `networkManagedElementId` attribute of the *ManagedElement* MO. The attribute changes the RDN visible in, for example, NETCONF transactions and PM files. This task is required for the OSS-RC interworking.

Prerequisites

An Ericsson Command-Line Interface (ECLI) session in Exec mode is in progress.

Steps

1. In the MOM, navigate to the *ManagedElement* MO and enter configure mode:

```
>ManagedElement=1
```

```
(ManagedElement=1)>configure
```

2. Modify the value of the `networkManagedElementId` attribute:

```
(config-ManagedElement=1)>networkManagedElementId=<value>
```

Note: The value must be unique within the network namespace.

3. Commit the changes:

```
(config-ManagedElement=1)>commit
```

Result

The job is completed.