

vMRF Backup and Restore Guideline

Virtual Multimedia Resource Function

User Guide

Copyright

© Ericsson AB 2016–2019. 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.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document *Trademark Information*.



Contents

1	Automatic Backup and Restore	1
2	Manual Backup and Restore	2
2.1	When to Make a Backup	2
2.2	Backup Procedure	2
2.3	When to Restore	3
2.4	Restore Procedure	3
3	VM Snapshot	6
3.1	When to Take a Snapshot	6
3.2	Take a Snapshot in VMware vSphere	6
3.3	Take a Snapshot in VMware vCloud Director	7
3.4	When to Revert to a Snapshot	7
3.5	Revert to a Snapshot in VMware vSphere	8
3.6	Revert to a Snapshot in VMware vCloud Director	8





1 Automatic Backup and Restore

vMRF performs automatic configuration backup after configuration changes. To prevent unnecessary backup operations, a new configuration is saved after an 80-second wait period following the most recent change. The 10 latest configuration backups are stored in time-stamped files in `/cluster/storage/configurationbackups/`. The file naming convention is the following:

```
<YYYYMMDD>_<hhmmss>_mrf.tar.gz
```

The copy of the latest backup file is also saved as `mrvs_config.tar.gz` in the same directory. This file is synchronized across all VMs of a cluster to enable any new SC to restore configuration after cluster restart.

When the maximum number of backup files is reached, the oldest backup file is deleted before a new backup is stored.

vMRF can perform automatic configuration restore if all VMs in a cluster reboot simultaneously. In this case, the new SC VM looks for `mrvs_config.tar.gz` in `/cluster/storage/configurationbackups/` and imports the configuration to the VNF, if the file exists.



2 Manual Backup and Restore

It is possible to create system backups and recover the system manually. During the manual backup and restore procedure, node credentials, trusted certificates, and configurable data from the vMRF MOM are exported from and imported to the VNF.

2.1 When to Make a Backup

It is recommended to periodically make a backup allowing for recovery.

A system backup must be made in the following cases:

- A work order is received, or this instruction is referred to from another instruction.
- Before the manual vMRF upgrade process is started.
- After a successful vMRF upgrade process.
- Major changes occur in the system configuration due to modifications in the network.
- After a sequence of small modifications, when the configuration is considered to be stable.

2.2 Backup Procedure

The backup procedure covers all the steps to make a successful backup of the system. During backup, node credentials, trusted certificates, and configurable data from the vMRF MOM model is exported.

Prerequisites

- The external location where the backup is stored is agreed on.
- The user ID, password, and O&M IP address of the node are known.
- The network configuration is not changed during the backup.
- A configured and operational vMRF VNF is available and you can log in to it as emergency user, using SSH.

Steps

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



```
ssh <user_ID>@<O&M_IP_address>
```

2. Run the following command:

```
/opt/mrf_director/mrf_export_conf.py  
<file_name_without_extension>
```

The *<file_name_without_extension>* is the full path to the file into which you want to export the configuration data.

Result: The configuration data is exported into a `.tar.gz` archive file.

3. Copy the exported configuration file out of the file system of the VNF using, for example, `scp`:

```
scp <user_ID>@<O&M_IP_address>:/home/<user ID>/mrf_conf.tar.gz .
```

Result: The example configuration file `mrf_conf.tar.gz` is copied from the vMRF VNF to the current directory.

2.3 When to Restore

The restore procedure must be started in the following cases:

- The VNF cannot retain the normal operational mode by using normal O&M procedures.
- The VNF must be restored to an earlier state.

It is recommended to restore a VNF from a configuration backup when troubleshooting the existing VNF is too time-consuming.

2.4 Restore Procedure

The restore procedure described in this section covers all the steps to make a successful recovery of the system. During recovery, node credentials, trusted certificates, and configurable data of the vMRF MOM model is imported to a vMRF VNF. If the configuration file contains an MO attribute that does not exist in the VNF, the MO attribute of the configuration file is discarded. If the VNF contains an MO attribute that does not exist in the configuration file, the default value of the MO is used in the restored VNF.

During the backup procedure, announcement files stored in vMRF VMs are not exported, therefore they are deleted during redeployment. For availability reasons, it is recommended to store announcement files to an external server. For more information, refer to [vMRF Configuration Management](#).

2.4.1 Restore during Deployment

Configuration data can be restored during deployment, which means that the necessary configuration data is imported into the VNF during the instantiation



step. For more information on this restore method, refer to the relevant deployment instructions.

2.4.2 Restore after Deployment

This section describes the case when configuration data is restored to a newly deployed VNF.

Prerequisites

- The VNF is clean, that is, it does not contain for example network data. For more information, see relevant deployment instructions.
- The file containing vMRF configuration data is available on the external location from where the backup is restored.
- The user ID, password, and O&M IP address of the VNF to be restored are known.
- You can log in to vMRF VNF as emergency user, using SSH.

Steps

1. If a configuration data file is not available in the file system of the VNF, copy a file to the VNF using, for example, the scp command:

```
scp mrf_conf.tar.gz <user_ID>@<O&M_IP_address>:/home/<user_ID>/
```

Result: The configuration file `mrf_conf.tar.gz` is copied from the current directory to the `/home/<user_ID>/` folder in the file system of the vMRF VNF.

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

```
ssh <user_ID>@<O&M_IP_address>
```

3. Run the following command:

```
/opt/mrf_director/mrf_import_conf.py /home/<user_ID>/  
mrf_conf.tar.gz
```

2.4.3 Post-restore Checks

Finish the restore procedure by issuing the following commands:

Steps

1. Check the status of the VMs in the VNF with the following command:



verify_vmrf_cluster_status.py

2. Check the VNF for IP address collisions with the following command:

cluster run cli_tool ipp conf

3. Check the operational state of the SCTP links with the following command:

cluster run cli_tool mrf_appl sctp-status

4. Check the signaling state of the VNF with the following command:

cluster run cli_tool mrf_appl status



3 VM Snapshot

vMRF supports VM snapshots on VMware vSphere and VMware vCloud.

This feature allows the creation of snapshots of the VMs to recover the system from snapshot manually. The snapshot contains the current virtual disk content, but it must not contain memory.

3.1 When to Take a Snapshot

It is recommended to take a snapshot allowing VM reversion in the following cases:

- A work order is received, or this instruction is referred to from another instruction.
- After successful vMRF deployment and configuration.
- After a successful vMRF upgrade process.
- After a successfully scale-out operation.
- Major changes occur in the system configuration due to modifications in the network.
- After a sequence of small modifications, when the configuration is considered to be stable.

3.2 Take a Snapshot in VMware vSphere

This procedure describes how to take a snapshot of the VMs in the vMRF cluster using VMware vSphere.

Prerequisites

- A configured and operational vMRF VNF is available and you can log in to it as emergency user, using SSH.

Steps

1. Take a snapshot of all VMs in the vMRF VNF based on the instructions described in the [VMware vSphere documentation](#).

Use the following options:

- Clear the **Snapshot the virtual machine's memory** check box.



- Clear the **Quiesce guest file system** check box.

Results

The snapshots are created for all the VMs in the vMRF vApp.

3.3 Take a Snapshot in VMware vCloud Director

This procedure describes how to take a snapshots of the vMRF vApp using VMware vCloud Director.

Prerequisites

- A configured and operational vMRF VNF is available and you can log in to it as emergency user, using SSH.

Steps

1. Take a snapshot of the vMRF vApp based on the instructions described in the [VMware vCloud Director documentation](#).

Use the following options:

- Clear the **Snapshot the virtual machine's memory** check box.
- Clear the **Quiesce guest file system** check box.

Results

The snapshots are created for all the VMs in the vMRF vApp.

3.4 When to Revert to a Snapshot

The reversion procedure must be started in the following cases:

- The VNF cannot retain the normal operational mode by using normal O&M procedures.
- The VNF must be restored to an earlier state.

Reversion from a snapshot must be done for all VMs in the vMRF VNF simultaneously. If the reversion of a VM is done in another transaction, the reverted VM receives the configuration from the active SC VM at the time of reversion. If the active SC VM is reverted, the active SC role moves to the standby SC VM, and the reverted VM receives the configuration from the new active SC VM at the time of reversion.

Note: Reverting VMs from a snapshot has traffic impact because all VMs are shut down for a short time.



3.5 Revert to a Snapshot in VMware vSphere

This procedure describes how to revert to a snapshot of the VMs in the vMRF cluster using VMware vSphere.

Prerequisites

- At least one snapshot is available for each VM of the VNF that are to be reverted.

Steps

1. Revert either to the latest snapshot or any other snapshot available for all VMs in the vMRF VNF based on the instructions in the [VMware documentation for the vSphere web client](#).

Note: If a snapshot is not available of all the VMs, shut down the VMs that do not have a snapshot taken.

2. Power on the vMRF vApp.
3. Perform post-restore checks.

Results

The vMRF VNF is running with the configuration at the time when the snapshot was taken.

— RELATED INFORMATION —

[2.4.3 Post-restore Checks on page 4](#)

3.6 Revert to a Snapshot in VMware vCloud Director

This procedure describes how to revert to a snapshot of the vMRF vApp using VMware vCloud Director.

Prerequisites

- A snapshot is available for the vMRF vApp.

Steps

1. Revert to the latest snapshot of the vMRF vApp based on the instructions in the [VMware documentation for the vCloud Director web client](#).
2. Start the vMRF vApp.



3. Perform post-restore checks.

Results

The vMRF VNF is running with the configuration at the time when the snapshot was taken.

— RELATED INFORMATION —

[2.4.3 Post-restore Checks on page 4](#)
