

vMRF Backup and Restore Guideline

Virtual Multimedia Resource Function

User Guide

Copyright

© Ericsson AB 2016–2018. 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	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





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 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 Managed Object Management (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.

To export configuration data, perform the following steps:



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 process must be started when the node cannot retain the normal operational mode by using normal Operation and Maintenance (O&M) procedures, or the node must be restored to an earlier state. It is also 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 without Re-Deployment

This procedure describes how to restore a VNF without re-deployment, even if configuration data has been loaded into the VNF.

Prerequisites

- The file containing vMRF configuration data is available on the 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.
- Root (sudo) privileges are granted for the user performing the procedure.

Steps

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

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

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. Overwrite the configuration file /cluster/storage/configurationsbackup/mrsv_config.tar.gz with the file copied in [Step 1](#), and change configuration file permissions with the following commands:

```
for i in `cluster list | awk '/STANDBY|/QUIESCED/{print $1}'` ; do scp <configuration_file_to_be_restored>.tar.gz $i;; done
```

```
cluster run "sudo cp <configuration_file_to_be_restored>.tar.gz /cluster/storage/configurationbackups/mrsv_config.tar.gz"
```

```
cluster run "sudo chown <administrative_user>:com-emergency /cluster/storage/configurationbackups/mrsv_config.tar.gz"
```

```
cluster run "sudo chmod 660 /cluster/storage/configurationbackups/mrsv_config.tar.gz"
```

4. Disable persistent back-end service with the following command:

```
cluster run "sudo immcfg -m -a saImmRepositoryInit=2 safRdn=immManagement,safApp=safImmService"
```



5. Delete the persistent configuration database from all VMs with the following command:

```
cluster run sudo rm /cluster/storage/clear/coremw/etc/imm.db
```

Note: It is normal that this command responds `Failed to run command` on specific VMs, since the file does not necessarily exist in all VMs. Check the existence of the file with command `cluster run ls /cluster/storage/clear/coremw/etc/` and repeat the `rm` command if necessary.

6. Reboot the cluster with the following command:

```
cluster run sudo shutdown -r +<Shutdown_timer_in_minutes>
```

Note: The value of `<Shutdown_timer_in_minutes>` must be at least 1 to make sure that the active SC VM is not restarted before the shutdown command is issued on every PL VMs.

Results

The VNF cluster is restarted with the newly added configuration file, retaining normal VNF operation.

2.4.2 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.

2.4.3 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, refer to the 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. 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. 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.

3. Run the following command:

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

2.4.4

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
```