

# Emergency Recovery Procedure for vMRF

## 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

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Prerequisites	1
<b>2</b>	<b>Emergency Procedure</b>	<b>3</b>
2.1	Check Cloud Environment	5
2.2	Log in to the vMRF Instance	5
2.3	Check IP Configuration in the Active SC VM	6
2.4	Verify VNF Status	7
2.5	Recover the VNF by Deploying a New Instance	8
<b>3</b>	<b>Concluding Actions</b>	<b>9</b>
3.1	Problem Solved	9
3.2	Contact Cloud Administrator	9
3.3	Consult Next Level of Support	9





# 1 Introduction

This document gives an overview of the emergency recovery tasks to be performed on the Virtual Multimedia Resource Function (vMRF). Emergency in this document refers to the following situations:

- There is traffic disturbance without corresponding alarms.
- It is not possible to log in to the VNF using the O&M IP address.

This document does not describe what to do in case of traffic disruption or stoppage, or control signaling problems, such as H.248 control link problems. For these problems, refer to the *vMRF Troubleshooting Guideline*.

The system is assumed to have been in a fully working state before the problems started. Therefore no troubleshooting procedures that relate to faulty configuration are explained. For this type of information, refer to *Fault Management* and *vMRF Troubleshooting Guideline*.

The scope of the document is to cover vMRF-related issues in the virtualized environment. For virtualized infrastructure-related issues, contact the next level of support.

## 1.1 Prerequisites

This section provides information on the documents, tools, and conditions that apply to the procedures in this document.

### 1.1.1 Documents

Before starting this procedure, ensure that the following information or documents are available:

- Information about O&M IP address, username and password of the Operations, Administration, and Maintenance (OAM) user and emergency user. For more information, refer to *Security Management for ECLI, NETCONF, and SFTP Users*.
- Information on how to use the features of the Ericsson Command-Line Interface (ECLI), refer to *Ericsson Command-Line Interface User Guide*.
- Information about how to install the vMRF, refer to the relevant *deployment instructions*.
- Information about how to collect data and log files, refer to *Data Collection Guideline for vMRF*.



- Information about backup and restore procedures, refer to *vMRF Backup and Restore Guideline*.

### **1.1.2 Conditions**

Before starting this procedure, ensure that the following conditions are met:

- Information about the operation and architecture of vMRF is available
- Information about the virtualized infrastructure, such as, operating system, hypervisor, and hardware is available
- Site-specific information about the vMRF is available

### **1.1.3 Tools**

The following tools are required:

- SSH client
- Cloud management tool provided by virtualized infrastructure, including a console tool



## 2 Emergency Procedure

The procedure in this section describes the scenario used to find and resolve faults that can cause a vMRF emergency situation. [Figure 1](#) shows the recovery flow described in this document.

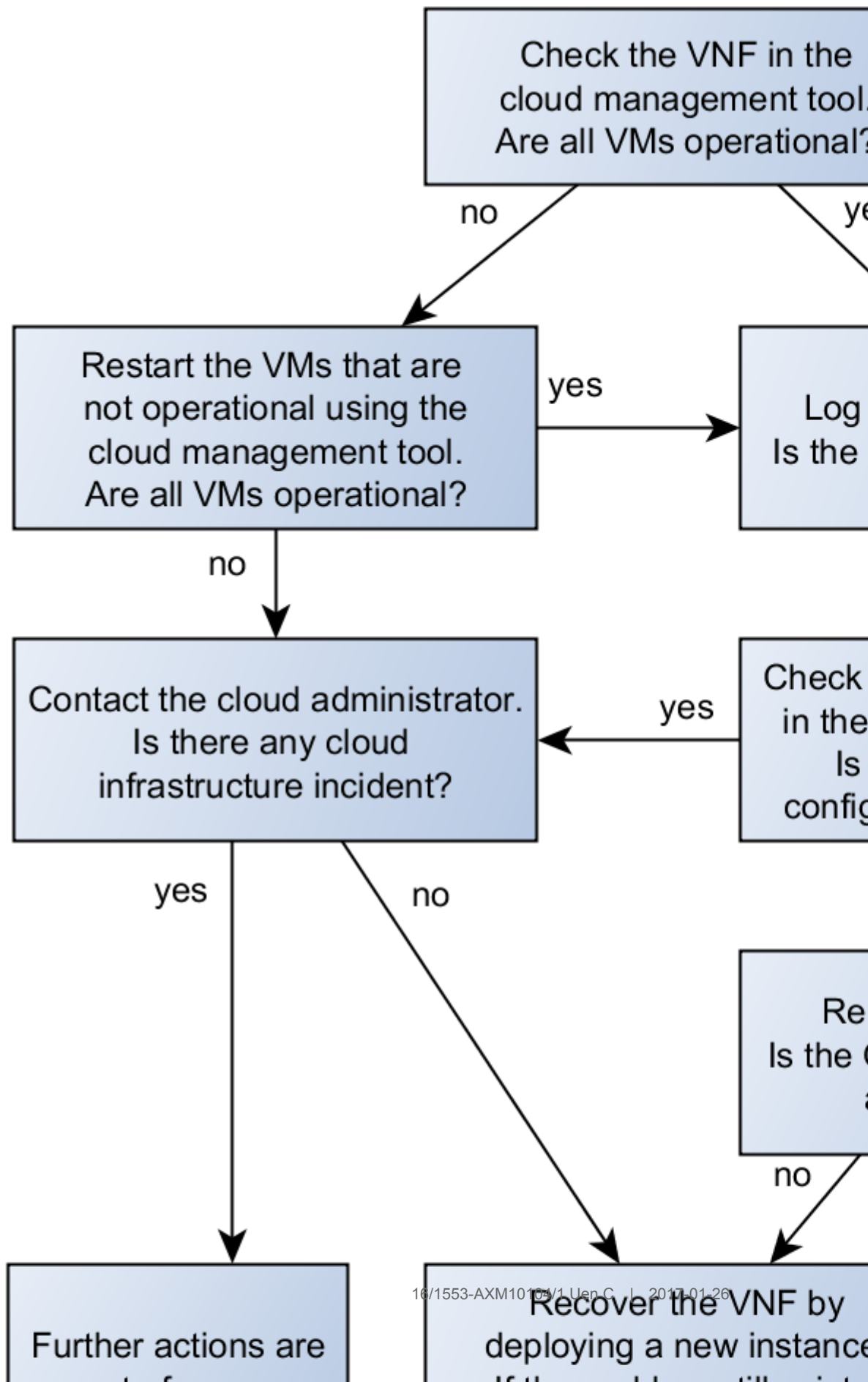






Figure 1 vMRF Recovery Flow

## 2.1 Check Cloud Environment

This procedure describes how to check the cloud environment for problems with the VNF.

### Steps

1. Check the VMs belonging to the vMRF VNF in the cloud management tool.
  - If all the VMs are operational, continue with [Log in to the vMRF Instance](#) on page 5.
  - If any of the VMs is not running, continue with the next step.
2. Restart the VMs that are not running, using the cloud management tool.
  - If the VMs recovered after the restart, continue with [Log in to the vMRF Instance](#) on page 5.
  - If the VMs did not recover, continue with the next step.
3. Contact the cloud administrator to check if there are any incidents affecting the cloud infrastructure.
  - If there are any cloud infrastructure incidents that can be related to the vMRF problem, further actions are out of scope of this procedure, continue with [Contact Cloud Administrator](#) on page 9.
  - If there are no cloud infrastructure incidents that can be related to the vMRF problem, continue with [Recover the VNF by Deploying a New Instance](#) on page 8.

## 2.2 Log in to the vMRF Instance

1. Log in to the vMRF instance by opening an SSH connection to the O&M IP address of the vMRF VNF using the following command, then continue with [Verify VNF Status](#) on page 7:

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

If the vMRF O&M IP address is not accessible, connect to any VM of the vMRF VNF from the console tool, and continue with [Check IP Configuration in the Active SC VM](#) on page 6.



## 2.3 Check IP Configuration in the Active SC VM

This procedure describes how to check the IP configuration of the active SC VM.

The procedure includes checking if the Moveable IP (MIP) address stored in `/mip/oam/address` is configured correctly. The MIP address is configured as the primary IP address on the `eth1` interface of the active SC.

### Prerequisites

- You have logged in to the VNF using the console tool.
- The IP address of the active SC VM from the `verify_vmrf_cluster_status.py` script output.

### Steps

1. Open an SSH connection to the SC VM using the following command:

```
ssh <user ID>@<SC VM IP address>
```

2. Check the MIP address, using the following command:

```
$ sudo cat /mip/oam/address
```

```
192.168.1.4
```

3. Check the IP configuration on the active SC with the following command:

```
$ ip a s eth1
```

```
2: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fa
    link/ether fa:16:ee:14:ec:8e brd ff:ff:ff:ff:ff:ff
    inet <MIP address>/24 brd 192.168.1.255 scope global eth1
        valid_lft forever preferred_lft forever
    inet 192.168.1.5/24 scope global secondary eth1:0
        valid_lft forever preferred_lft forever
```

The O&M IP is configured in the SC, if the `<MIP address>` is the same as the output of the command in [Step 2](#).

- If the O&M IP is configured, the problem is related to a virtualized network infrastructure issue. Continue with [Contact Cloud Administrator](#) on page 9.
  - If the O&M IP is not configured, continue with the next step.
4. Reboot the SC VM:

```
SC:$ reboot
```



5. Check the connectivity of the NBI:

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

- If the O&M IP address is accessible, continue with [Verify VNF Status](#) on page 7.
- If the O&M IP address is not accessible, continue with [Recover the VNF by Deploying a New Instance](#) on page 8.

## 2.4 Verify VNF Status

This procedure describes how to verify VNF status the after logging in to the VNF.

### Steps

1. Run the following command:

```
verify_vmrf_cluster_status.py
```

2. Check the components in the output of the `verify_vmrf_cluster_status.py` script.
  - If any of the components operate abnormally, restart the affected VMs or the VNF. To identify the faulty VMs, run the following command: `cluster run verify_vmrf_node_status.py`. If the problem still exists, continue with [Recover the VNF by Deploying a New Instance](#) on page 8.
  - If all components operate normally, continue with the next step.
3. Verify that there are no active alarms.
  - If there are active alarms, cease the alarms, and continue with the next step.

For more information on ceasing alarms, refer to the [relevant alarm OPI](#).

- If there are no active alarms, but traffic disturbance has not ceased, continue with the next step.
4. Verify that traffic is received by vMRF, and whether the emergency situation continues by checking traffic-related counters that indicate traffic disturbance.

**Note:** Counters can be checked on the VNF level by adding `cluster run` to the command.

- If the emergency situation has ceased, continue with [Problem Solved](#) on page 9.



- If the emergency situation persists, continue with [Recover the VNF by Deploying a New Instance](#) on page 8.

## 2.5 Recover the VNF by Deploying a New Instance

1. Using the proper *deployment instructions*, deploy a new VNF instance with one or two VMs, and check that it is running properly. Remove VMs from the old VNF, if there is not enough capacity for more than one VNF. Ensure that the new instance connects to the same external networks as the old instance. It is recommended to import the configuration data exported from the old VNF during deployment. Deploying a new VNF might require configuration changes in connected systems, for example, due to new O&M IP address.
  - If the new instance is operating normally, continue with the next step.
  - If the new instance has the same problems as the old one, continue with [Consult Next Level of Support](#) on page 9.
2. Scale out the new VNF instance to the full capacity as described in *vMRF Configuration Management*.

**Note:** If there are not enough resources to scale out the new instance while the old instance still exists, add one VM at a time to the new instance, and at the same time gracefully shut down, and remove another VM in the old instance. Always keep one VM in the old VNF.
3. Check that the new instance is fully operational, by using methods described in [Verify VNF Status](#) on page 7.
  - If the new instance is operating normally, continue with [Problem Solved](#) on page 9.
  - If the new instance has the same problems as the old one, continue with [Consult Next Level of Support](#) on page 9.



## 3 Concluding Actions

In general, all the described recovery situations must be seen as abnormal and must be reported to the next level of support.

It is therefore important to document the problematic situation and all the recovery steps that have been taken, for a Root Cause Analysis (RCA) to determine the source of the problem.

Log files in the system must be saved or copied to another place to prevent them from being overwritten with newer information. It is important that these logs are available for any future RCA. For more information on collecting logs, refer to *Data Collection Guideline for vMRF*.

### 3.1 Problem Solved

The recovery was successful. Keep vMRF and the affected functions under extra observation for a while to ensure that the fault does not reoccur.

#### Steps

1. Record the incident according to local procedures.
2. Create a CSR to the next level of support to have the root cause investigated, if needed.

### 3.2 Contact Cloud Administrator

The problem is related to a virtualized infrastructure network issue.

#### Steps

1. Provide the Cloud Administrator with the information needed to investigate incidents affecting the cloud infrastructure. Further actions are outside the scope of this instruction.

### 3.3 Consult Next Level of Support

Problems identified that cannot be solved by using this document must be reported to the next level of maintenance support.

1. Consult next level of maintenance support. Further actions are outside the scope of this instruction.