

vMRF Troubleshooting Guideline

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	Introduction	1
1.1	Documents	1
2	Troubleshooting Procedures	2
2.1	Manual Recovery Flow	2
2.2	Common Procedures	3
3	Trouble Cases	5
3.1	Deployment Related Trouble Cases	5
3.2	Scaling Related Trouble Cases	9
3.3	Signaling Related Trouble Cases	10
3.4	Media Related Trouble Cases	13
3.5	Load Related Trouble Cases	15
3.6	Announcement Related Trouble Cases	17





1 Introduction

This document describes how to perform the troubleshooting procedure in the vMRF.

1.1 Documents

Before starting this procedure, ensure that the following documents have been read:

- *Data Collection Guideline for vMRF*
- *vMRF Backup and Restore Guideline*

1.1.1 Conditions

Certain troubleshooting activities can have an impact on the node performance. For example, trace or log activation can be disturbing traffic and is not recommended without first consulting next level of maintenance support.



2 Troubleshooting Procedures

This section describes troubleshooting information for vMRF.

Problems identified that cannot be solved by using this document must be reported to the next level of maintenance support. This is to result in a Customer Service Report (CSR).

The details of the trouble reporting process is outside the scope of this document.

A manual recovery flow in [Manual Recovery Flow](#) on page 2 presents a generic workflow to identify and solve problems if possible, or to collect useful data.

[Trouble Cases](#) on page 5 describes specific trouble cases for various scenarios. These cases often utilize the manual recovery flow as well.

Log files of access and authorization events in the system can be collected by using the `journalctl` command. For more information, refer to *vMRF Security Management*.

It is recommended to periodically export and store the configuration of the node outside the VNF as a backup for a possible re-deployment. For more information, refer to *vMRF Backup and Restore Guideline*.

2.1 Manual Recovery Flow

This section describes the recommended manual recovery flow for troubleshooting purposes.

Steps

1. Log in to the vMRF instance.
2. Collect troubleshooting data regarding the incident in case next level support needs to be contacted. For more information on how to collect information, refer to *Data Collection Guideline for vMRF*.
3. Check vMRF status, identify the faulty VM if needed. See [vMRF Status Check](#) on page 3 for the procedure.
4. Consider performing a backup. For more information refer to *vMRF Backup and Restore Guideline*.
5. Force lock the faulty VM. If the VM is not available or accessible, continue with [Step 7](#).



Note: In this case the VM is locked immediately and all ongoing traffic from the VM is lost. For more information on locking a VM, refer to *vMRF Configuration Management*.

6. Restart the VM from the cloud management tool.

Note: If the *MrflInstance* MO that represents the VM is in locked state after the restart, it must be unlocked by setting the `administrativeState` attribute of the MO to UNLOCKED.

7. If the problem is not solved, remove the VM from the cluster using the cloud management tool and create a new VM.

2.2 Common Procedures

This section describes procedures used during troubleshooting.

2.2.1 vMRF Status Check

This procedure describes how to verify the vMRF deployment.

The status check shows the status of all VMs in the cluster. A VM can be identified by its `UUID`. The `UUID` is visible:

- in the `uuid` attribute of the *ComputeResource* MO, that is referenced from the *MrflInstance* MO, that represents the VM
- in the cloud management tool for each VM

2.2.1.1 vMRF Status Check on Openstack

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

```
ssh -A -i <private key .pem file> <user ID>@<O&M IP address>
```

2. Run the following command:

```
cluster run verify_vmrf_node_status.py
```

3. Check that all components are in the OK state.

The following example shows the printout of a successful status check:

```
Running command: "verify_vmrf_node_status.py" on localhost
eth0: OK
eth1: OK
eth2: OK
SC role: ACTIVE
CoreMW: OK
COM: OK, RUNNING
```



```
MrfDirector: OK, RUNNING
  CliDaemon: OK
  IpPipeline: OK
    TC-MPD: OK
    MrfAgent: OK
    CloudInit: OK
    SEC-CERT: OK
neighbourdetection: OK
```


3 Trouble Cases

This section describes trouble cases for vMRF.

Follow the troubleshooting workflow as shown in [Figure 1](#).

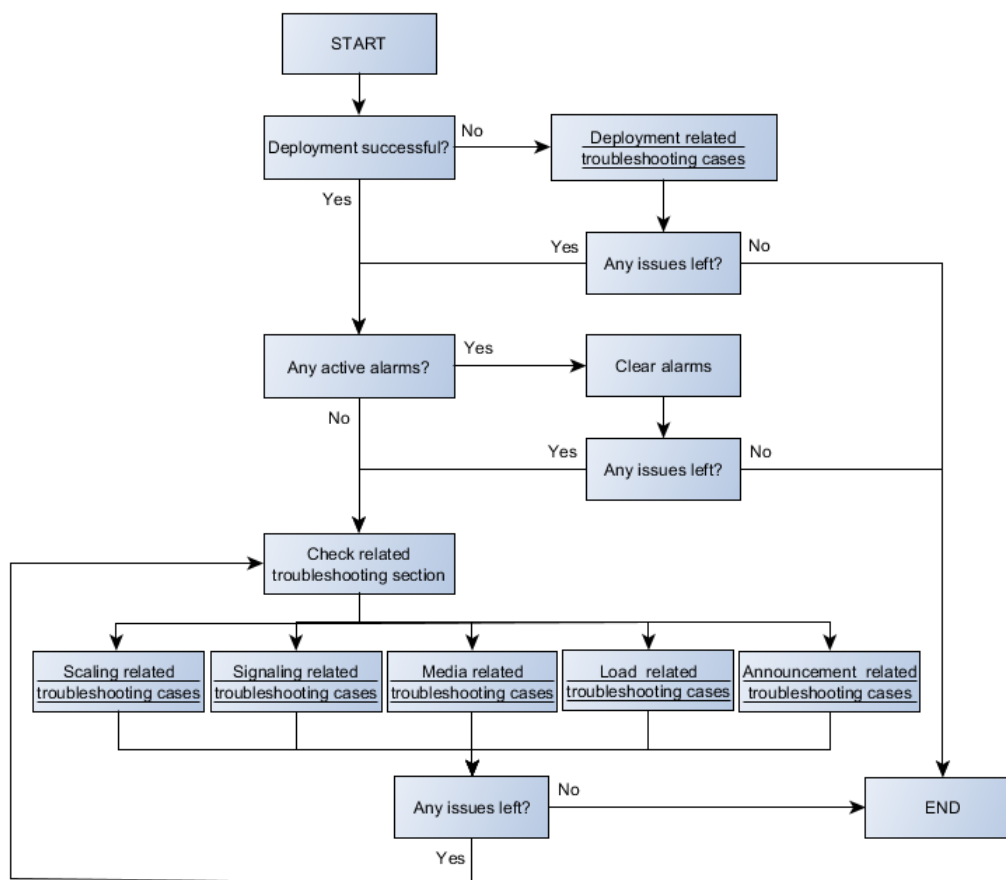


Figure 1 Troubleshooting Workflow

3.1 Deployment Related Trouble Cases

This section describes trouble cases related to deployment.

3.1.1 VNF Does not Start

3.1.1.1 Image Extraction Problem

Symptom:



Problem during image extraction.

Possible Cause:

Image is corrupted.

Procedure:

Do the following:

Steps

1. Verify the image using the MD5 checksum file that is provided by Ericsson.
2. If needed, repeat the download and extraction of the vMRF package as described in the corresponding *deployment guide*.
3. If the problem still exists, contact Ericsson support.

3.1.1.2

vMRF Instantiation not Possible in OpenStack

Symptom:

- Heat stack creation failed due to error: No valid host found. There are not enough hosts available.

Possible Causes:

- Low vCPU resources
- Low memory
- Problem in network allocation. Compute nova log shows: Failed to allocate the network(s)

Procedure:

Do the following:

Steps

1. In case of network allocation problem, check the neutron logs and configuration. Correct the network configuration.
2. Ensure that the environment fulfills hardware, software, and network requirements. The main requirements are listed in *vMRF Infrastructure Requirements*.
3. Follow the deployment instruction described in *Deployment Guide for OpenStack*.



4. If the problem still exists, contact Ericsson support.

3.1.2 Cyclic Kernel Restart

Symptom:

- Cyclic kernel restart.

Procedure:

Do the following:

Steps

1. Perform the manual recovery flow procedure, as described in [Manual Recovery Flow](#) on page 2.
2. If the problem still exists, contact Ericsson support.

3.1.3 VM Stuck

Symptoms:

- ssh connection to VM is not possible:

```
ssh mrsv-admin@192.160.112.15
ssh: connect to host 192.160.112.15 port 22: No route to host
```

- vMRF is disabled in vMTAS:

```
>show ManagedElement=1,MtasFunction=MtasFunction,⇒
MtasMediaFramework=0,MtasMrf=0,MtasMpController=0,MtasMrfpNode=1
MtasMrfpNode=1
  mtasMrfpNodeAdministrativeState=UNLOCKED
  mtasMrfpNodeId="[10.52.58.222]:2944"
  mtasMrfpNodeOperationalState=DISABLED
```

- VM console is inaccessible or console shows problems

Procedure:

Steps

1. Perform the manual recovery flow procedure, as described in [Manual Recovery Flow](#) on page 2.
2. If the problem still exists, contact Ericsson support.

3.1.4 No Console Connection in Openstack

Symptoms:



- Console is not available.

Procedure:

Do the following:

Steps

1. Restart OpenStack nova services.

3.1.5 No ssh Connection into VM

3.1.5.1 OpenStack

Symptom:

- No route to host.

```
ssh mrsv-admin@192.160.112.15
ssh: connect to host 192.160.112.15 port 22: No route to host
```

Possible Causes:

- No IP available
- Floating IP problem
- Routing problem
- Security group problem

Procedure:

Steps

1. Check console connection.
2. Check if there is an IP address for eth1.
3. Check if the floating IP is associated with the VM.
4. Check if ssh is enabled in the security groups of the VM.
5. Check connectivity and routing firewalls towards the cloud environment.
6. Perform the manual recovery flow procedure, as described in [Manual Recovery Flow](#) on page 2.
7. If the problem still exists, contact Ericsson support.



3.1.6 Wrong cloud-init Syntax

Symptom:

- cloud-init process indicates problem.

Procedure:

Steps

1. Check the user-data.txt file delivered in the release package. Modify it if needed.
2. If the problem still exists, contact Ericsson support.

3.1.7 No Running MRF Processes on SC

Symptom:

- Status check shows following printout:

```
Running command: "verify_vmrf_node_status.py" on localhost
eth0: OK
eth1: OK
eth2: OK
SC role: not_available
CoreMW: ERROR
COM: OK, NOT RUNNING
MrfDirector: OK, NOT RUNNING
CliDaemon: OK
IpPipeline: OK
TC-MPD: OK
MrfAgent: ERROR
CloudInit: NOT RUN YET
SEC-CERT: OK
neighbourdetection: OK
```

Procedure:

Steps

1. Perform the manual recovery flow procedure, as described in [Manual Recovery Flow](#) on page 2.
2. If the problem still exists, contact Ericsson support.

3.2 Scaling Related Trouble Cases

This section describes trouble cases related to scaling.



3.2.2 vMRF VM Joins Wrong Cluster

Symptoms:

- A vMRF VM joins a different network cluster

```
mrsv-admin@42198368-bedd-898f-0d15-533ee8ad7dc4:~$ sudo journalctl |  
Jan  9 00:42:18 kontron-am4024e kernel: [ 36.890082] tipc: Started  
Jan  9 00:42:18 kontron-am4024e kernel: [ 36.891668] tipc: Own node  
Jan  9 00:42:18 kontron-am4024e kernel: [ 36.893952] tipc: Enabled  
discovery domain <1.1.0>, priority 10  
Jan  9 00:42:18 kontron-am4024e kernel: [ 36.897451] tipc: Establish  
on network plane A  
Jan  9 00:42:18 kontron-am4024e kernel: [ 36.899559] tipc: Establish  
on network plane A
```

1.1.3:eth0-1.1.1:eth0 implies problem. Correct tipc connection in vMRF is from eth0 to eth0: <1.1.10:eth0-1.1.15:eth0>

Possible Cause:

- Problem in cloud networking, incorrect network configuration, open network.

Procedure:

Steps

1. Check and reconfigure cloud networking.

3.3 Signaling Related Trouble Cases

This section describes trouble cases related to signaling.

3.3.1 No IP Address Available for Signaling

Symptom:

- IP address not available. Status check shows the following printout:

```
Running command: "verify_vmrf_node_status.py" on localhost:  
eth0: OK  
eth1: OK  
eth2: NO IPv4 ADDRESS  
SC role: ACTIVE  
CoreMW: OK  
COM: OK, RUNNING  
MrfDirector: OK, RUNNING
```



```

CliDaemon: OK
IpPipeline: OK
  TC-MPD: OK
  MrfAgent: OK
CloudInit: OK
  SEC-CERT: OK
neighbourdetection: OK

```

Possible Causes:

- Hardware problem
- VLAN tagging problem
- OpenStack configuration problem

Procedure:

Steps

1. Check DHCP server.
2. Check connectivity to DHCP server, physical connectivity, vlan tagging.
3. Check OpenStack security groups.

3.3.2

No Connection to NextHop

Symptoms:

- SCTP operational state of MRF application is disabled:

```

mrsv-admin@fi2-vmrf-com-uplift-cl2:~$ cluster run cli_tool mrf_appl status
Running command: "cli_tool mrf_appl status" on host: 192.168.0.3 (fi2-vmrf-com-uplift-cl2)
[2017-01-09 11:50:55.383]

Signalling State:
=====

H248Interface-Id: 3 H248Interface-LDN: "MediaResourceFunction=1,MrfH248Control=1,MrfH248Inte
H248Interface Service Change state: NOT_STARTED
Sctp operational state: DISABLED
Remote IP Address: 10.52.60.8 Remote Port: 21614
=====

H248Interface-Id: 2 H248Interface-LDN: "MediaResourceFunction=1,MrfH248Control=1,MrfH248Inte
H248Interface Service Change state: NOT_STARTED
Sctp operational state: DISABLED
Remote IP Address: 10.52.60.8 Remote Port: 21613
=====

H248Interface-Id: 1 H248Interface-LDN: "MediaResourceFunction=1,MrfH248Control=1,MrfH248Inte
H248Interface Service Change state: COMPLETED
Sctp operational state: ENABLED
Remote IP Address: 10.52.60.8 Remote Port: 21612
=====

LocalEndpoint Id: 3
Dscp: 40
Local port: 2944
=====

```



```
Sctp socket state: INITIATED.
DHCP assigned IP: 10.52.61.219
=====

MRF instance administrative state: UNLOCKED
=====

Running command: "cli tool mrf_appl status" on host: 192.168.0.4 (fi2-vmrf-com-uplift-cl2-0)
[2017-01-09 11:50:54.517]

Signalling State:
=====

H248Interface-Id: 3 H248Interface-LDN: "MediaResourceFunction=1,MrfH248Control=1,MrfH248Interfa
H248Interface Service Change state: NOT_STARTED
Sctp operational state: DISABLED
Remote IP Address: 10.52.60.8 Remote Port: 21614
=====

H248Interface-Id: 2 H248Interface-LDN: "MediaResourceFunction=1,MrfH248Control=1,MrfH248Interfa
H248Interface Service Change state: NOT_STARTED
Sctp operational state: DISABLED
Remote IP Address: 10.52.60.8 Remote Port: 21613
=====

H248Interface-Id: 1 H248Interface-LDN: "MediaResourceFunction=1,MrfH248Control=1,MrfH248Interfa
H248Interface Service Change state: ONGOING_COLD_BOOT
Sctp operational state: DISABLED
Remote IP Address: 10.52.60.8 Remote Port: 21612
=====

LocalEndpoint Id: 4
Dscp: 40
Local port: 2944
=====

Sctp socket state: INITIATED.
DHCP assigned IP: 10.52.61.215
=====

MRF instance administrative state: UNLOCKED
=====
```

Possible Causes:

- VLAN tagging problem in cloud
- VLAN tagging problem in site switches or routers
- Physical connectivity problem
- Security group problem

Procedure:

Steps

1. Check if the MRF H.248 Link Unavailable alarm is active. Clear the alarm using the alarm instruction.
2. Check if VM has IP address for eth2.
3. Check that SCTP is enabled in the security groups of the VM.
4. Check connectivity and routing firewalls towards the cloud environment.



5. Restart mrf process from CLI: `sudo systemctl restart mrf_appl.service`
6. Perform the manual recovery flow procedure, as described in [Manual Recovery Flow](#) on page 2.
7. If the problem still exists, contact Ericsson support.

3.3.3

No Connection to O&M IP Address

Symptom:

- The remote host key for the SSH connection to the O&M IP address has changed.

```

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle)
It is also possible that the RSA host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
<fingerprint>.
Please contact your system administrator.
Add correct host key in ~/.ssh/known_hosts to get rid of this messa
Offending key in ~/.ssh/known_hosts: <line number of the offending
Permission denied (publickey,password).

```

Possible Cause:

- After manual VNF upgrade, a new VM takes the ACTIVE SC role but has a different remote host SSH key than the old VM.

Procedure:

Steps

1. Remove the offending key from `~/.ssh/known_hosts` using the following command:

```
sed -i '<line number of the offending key>d' ~/.ssh/known_hosts
```

Result

The offending key is deleted, the warning message will not be displayed as long as the ACTIVE SC role stays in the current VNF.

3.4

Media Related Trouble Cases

This section describes trouble cases related to media.



3.4.2 No Connection to Client

Symptom:

- Client is not reachable. Ping request from the IP address ends in timeout.

```
mrsv-admin@fil-vmrf:~$ cli_tool ipp conf
Configuration:
Network (id:1)                                default_network
  VLAN ID                                     -
  UDP Port Range                             1024..65535
  Media IP IF (id:1)
    Ethdev                                    em1 (id:0)
    MAC                                       FA:16:EE:FC:14:7A
    Link                                     UP
    IP                                       10.52.58.133
    Status                                   DHCP OK
  Media IP IF (id:2)
    Ethdev                                    em1 (id:0)
    MAC                                       FA:16:EE:FC:14:7A
    Link                                     UP
    IP                                       2001:1b70:8298:2038::5
    Status                                   DHCP OK
    Link local                              fe80::f816:eeff:fe11:db83
  Static Route (id:4)
    IP                                       0.0.0.0/0
    Nexthop (id:4)
      MAC                                    00:30:88:11:DB:83
      IP                                    10.52.58.129
  Static Route (id:6)
    IP                                       ::/0
    Nexthop (id:6)
      MAC                                    00:30:88:11:DB:83
      IP                                    fe80::230:88ff:fe11:db83
mrsv-admin@fil-vmrf:~$

mrsv-admin@fil-vmrf:~$ cli_tool ipp ping -m 1 10.52.45.129
PING 10.52.45.129 56 bytes of data
Timeout (3000 ms)
mrsv-admin@fil-vmrf:~$
```

Possible Causes:

- Problem in static route
- Problem in client

Procedure:



Steps

1. Check static route in vMRF.
2. Check routing on site.
3. Check client using Wireshark.
4. Check that connection is OK:

```
mrsv-admin@fil-vmrf:~$ cli_tool ipp ping -m 1 10.52.45.129
PING 10.52.45.129 56 bytes of data
56 bytes from 10.52.45.129: icmp_seq=0 ttl=62 time=0 ms
mrsv-admin@fil-vmrf:~$
```

3.5 Load Related Trouble Cases

This section describes trouble cases related to load.

3.5.1 Disturbances in Traffic

Symptoms:

- Temporary or permanent stoppage of traffic

Possible Cause:

- Software problem

Procedure:

Do the following:

Steps

1. Check crash dumps.
2. Collect related data and contact Ericsson support. For more information on how to collect information, refer to *Data Collection Guideline for vMRF*.

3.5.2 Speech Quality Problem

3.5.2.1 Bandwidth Limitation

Symptom:

- Bad speech quality



Bandwidth limitation can be checked by using the `ipp discard-counters` command:

```
mrsv-admin@fi8-mrs:~$ cluster run cli_tool ipp discard-counters
RX_BANDWIDTH_POLICING_DROP_TRAFFIC : 6286
```

Possible Cause:

- Bandwidth limitation

Procedure:

Steps

1. Check that needed bandwidth is not limited.

3.5.2.3

Packet Loss in vSwitch

Symptom:

Bad speech quality.

Possible Cause:

- Packet loss in vSwitch.

Procedure:

Steps

1. Check packet loss in vSwitch by using the `ipp internals` command:

```
cluster run cli_tool ipp internals -l 1
portname dir max burst total discards lost
em1 out 64 3168760208 0 300455
vswitch lost: 390124
```

2. Check packet loss in vSwitch by using the cloud management tool.
3. Add more VMs to the cluster if needed.

3.5.2.4

Packet Loss on Site

Symptom:

Bad speech quality.

Possible Causes:

- Packet loss on site.



- Packet loss/error counters are incremented in site switches or routers and cloud server switches.

Procedure:

Steps

1. Check connectivity, configuration, VLANs, routing firewalls towards cloud environment.

3.6 Announcement Related Trouble Cases

This section describes trouble cases related to announcements.

3.6.1 vMRF Cannot Play Announcement

Symptoms:

- vMRF cannot play announcement

```
mrsv-admin@fi2-vmrf-20170116-084636-cl1:~$ cli_tool mrf_appl h248-c
[2017-01-17 09:36:08.190]
```

```
Modify Request total: 1472180 (Emergency: 0 IEPS: 0 Priority: 0)
    Pendings: 0
    Pending limit exceeded: 0
    Retransmissions: 0
    Retransmission limit exceeded: 0
```

```
24 (Emergency: 0 IEPS: 0 Priority: 0) replied with error 51
    Originated from CRH at location 66 (visible as ERR_LOC_0006)
```

Possible Causes:

- File caching failure
- Missing *BasicAnnouncement* or *VariableAnnouncement* MO configuration
- Variable announcement logic execution error

Procedure:

Steps

1. Run the following command:

```
cli_tool mrf_appl announcement-status --status
```



Example

```
mrsv-admin@fi2-vmrf-20170116-084636-cl1:~$ cli_tool mrf_appl announcement-status --status
-----
ANNOUNCEMENT FAULTS
-----
time                                faultId  category                announcementId  language
-----
2017-01-17T09:34:48+00:00          1        CONFIGURATION FAULT      27              en-GB
-----
```

2. Depending on the problem cause indicated in the `description` column, add missing MO configuration or correct the faulty logic file.

For more information on announcement MO configuration and logic files, refer to *vMRF Configuration Management*.