

Fencing Failed

Cloud Execution Environment

OPERATING INSTRUCTIONS

Copyright

© Ericsson AB 2016. 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	Introduction	1
1.1	Alarm Description	1
1.2	Prerequisites	2
2	Procedure	3
2.1	Actions	3
3	Additional Information	5



Fencing Failed



1 Introduction

This instruction concerns alarm handling.

1.1 Alarm Description

The alarm is issued by the Managed Object (MO) `Node` when the periodic supervision algorithm detects that the compute host has failed the availability test three consecutive times, and `fence_compute_before_evacuation` was set to `true` (meaning that the compute will be fenced down), but fencing was not successful.

The severity of the alarm is `CRITICAL` or `CLEARED`.

The possible alarm causes and fault locations are explained in Table 1.

Table 1 Alarm Causes

Alarm Cause	Description	Fault Reason	Fault Location	Impact
Out-of-band management password has been changed	The out-of-band management of the compute node has been changed	Due to security reasons the out-of-band management password has been changed for the compute node, but fencing configuration has not been updated	Controller nodes	Fencing will not be successful due to password change
Compute malfunction	The affected compute is malfunctioning	The compute cannot be fenced due to a hardware related error (and out-of-band management is unable to switch off the server or blade)	Compute node	Fencing will not be successful due to hardware error
Network issue between controller and out-of-band management system	The fencing solution on the controllers is not able to communicate to the out-of-band management of the compute	Network issue prevents the communication from the controller node to the out-of-band management system	Network between controller and out of band management	Fencing will not be successful due to network error

The following is the consequence for the node if the alarm is not solved:

- The virtual machines (VMs) running on the affected compute node cannot be evacuated, as evacuation will only happen after a successful fencing



action. This causes unnecessary downtime for VMs that should be evacuated (VMs that have their `ha-policy` set to `ha-offline`).

- Failed fencing prevents the automatic recovery of the compute host, reducing resource availability and the availability of the managed-on-host VMs, until the compute host is manually restarted or replaced by the operator.

The alarm attributes are listed in Table 2.

Table 2 Alarm Attributes

Attribute Name	Attribute Value
Major Type	193
Minor Type	2031716
Managed Object Class	Node
Managed Object Instance	Region=<name_of_the_region>, CeeFunction=1, Node=<hostname_of_the_node>
Specific Problem	Fencing failed
Event Type	communicationsAlarm (2)
Probable Cause	protectionMechanismFailure (81)
Additional Text	;uuid=<HW_UUID_of_corresponding_server> (1)
Severity	CRITICAL or CLEARED

(1) The format of this field is expected to change in CEE R6.

Note: The alarm does not specify which VMs are affected. Separate VM Unavailable alarms are issued for each one.

For more information about the VM Unavailable alarm, refer to *VM Unavailable*.

1.2 Prerequisites

This section provides information on the documents, tools, and conditions that apply to the procedure.

1.2.1 Documents

Not applicable.

1.2.2 Tools

No tools are required.



1.2.3 Conditions

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

- Information about how to connect and use out-of-band management is available.
- Information whether an out-of-band management password was changed since the last reconfiguration of the fencing system is available.

2 Procedure

This section describes the procedure to follow when this alarm is received.

2.1 Actions

Perform the following:

1. Use the unqualified part of the hostname to find out the number of the corresponding shelf and server.

The unqualified hostname is displayed in the following format:

```
compute-<shelf_id>-<blade_id>
```

The first value shows the number of the shelf, while the second value shows the number of the server or blade.

2. Check where CM-HA is running and note the controller. You can get the information by issuing the following command on an arbitrary controller:

```
crm resource status p_cmha
```

3. Check the password in the `/etc/fencing_config/fencing.yaml` file on the vCICs, if it contains the right password for the out-of-band management of the affected compute.

The following scenarios are possible:

- If the password in the file does not match the actual password, reconfigure the fencing subsystem. For more information, refer to the *Runtime Configuration Guide*.

Wait for 10 minutes after reconfiguring the fencing subsystem to see if the alarm ceases. If the alarm ceases, exit this procedure.



- Or the password in the file matches the actual password. In this case, proceed to Step 4.
4. Check the network connectivity from the controller towards the out-of-band management by using SSH.

The following scenarios are possible:

- The connection attempt is not successful from the controller to the out-of-band management. Make sure that the out-of-band management system is available and restart it, if needed. For more information on how to restart the out-of-band management system, refer to the product documentation of the out-of-band management solution.

After the restart of the out-of-band management system, restart CM-HA service by issuing the following command on a controller:

```
crm resource restart p_cmha
```

If the alarm ceases, exit this procedure.

- Or the restart of out-of-band management did not solve the problem. In this case, proceed to Step 5.
5. Check the network connectivity from the controller towards other network addresses.

The following scenarios are possible:

- The connection attempt is not successful from the controller to other network addresses. Reboot the controller.

```
reboot -f
```

If the alarm ceases, exit this procedure.

- Or the restart of the controller did not solve the problem. In this case, proceed to Step 6.
6. Check the compute node via out-of-band management. If it's not available, replace the server as described in *Server Replacement*.

The following scenarios are possible:

- The replacement process was successful, the server was fenced down successfully, and the alarm ceases. If the alarm ceases, exit this procedure.
- Or the replacement did not solve the problem. In this case, proceed to Step 7.



7. Collect troubleshooting data as described in the *Data Collection Guideline*. For alarm-specific logs, refer to the table *Data Collection for Alarms and Alerts* in the *Data Collection Guideline*.
8. Contact the next level of maintenance support.

Further actions are outside the scope of this instruction.
9. The job is completed.

3 Additional Information

The alarm is ceased for a compute host in the below cases:

- The compute host is fenced down successfully by its out-of-band management.
- The compute host is recovered.