

# Expiring Certificate

Cloud Execution Environment

OPERATING INSTRUCTIONS

**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.

**Trademark List**

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



# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Alarm Description	1
1.2	Prerequisites	3
<b>2</b>	<b>Procedure</b>	<b>4</b>
2.1	Replace NBI Certificate on vCIC	4
2.2	Replace NBI Certificate on Atlas	6
2.3	Replace CA Certificate on Atlas	8
2.4	Replace CA and NBI Certificates on vCIC	9
2.5	Replace CA and Client NeLS Certificates	11
2.6	Post Actions	11
<b>3</b>	<b>Additional Information</b>	<b>12</b>
	<b>Reference List</b>	<b>13</b>



Expiring Certificate



# 1 Introduction

This instruction concerns the handling of an alarm that requires intervention.

For more information about Certification Authority (CA) and Northbound Interface (NBI) certificates required for secure HTTPS access to the Cloud Execution Environment (CEE), refer to *SW Installation in Single Server Deployment* and *SW Installation in Multi-Server Deployment*.

## 1.1 Alarm Description

The Expiring Certificate alarm is issued by the Managed Object (MO) Certificate when one or more of the following certificates are about to expire:

- CA certificate (or chain of certificates) of the organization issuing the Atlas Northbound Interface (NBI) certificate
- CA certificate (or chain of certificates) of the organization issuing the virtual CIC (vCIC) NBI certificate
- Ericsson CA certificate issued for the Network License Server (NeLS)
- Atlas NBI certificate
- vCIC NBI certificate
- NeLS client certificate

**Note:** Atlas and vCIC certificates can be issued by the same CA or by two separate CAs. NeLS certificates are issued by Ericsson. For more information about NeLS certificates, refer to section *Configure License Management* in the *Runtime Configuration Guide*.

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



Table 1 Alarm Causes

Alarm Cause	Description	Fault Reason	Fault Location	Impact
CA or NBI certificate or certificates will expire within 30 days of current date.	The Expiring Certificate alarm is issued when one or more of the CA or NBI certificates are about to expire.	One or more of the CA or NBI certificates will expire within 30 days of current date.	OpenStack endpoints on the vCICs	Access to the NBI will be lost on the given date, leading to undefined behavior of CEE.
NeLS CA or client certificate will expire within 30 days of current date.	The Expiring Certificate alarm is issued when one or both of the NeLS certificates are about to expire.	One or both NeLS certificates will expire within 30 days of current date.	vCICs	Connection to the NeLS server will be lost on the given date. The alarm remains until the NeLS certificates are replaced.

**Note:** If a CA certificate is expired, the related NBI or NeLS certificate must also be replaced.

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

**For Atlas or vCIC certificates**

External connection (access to the NBI) will be lost on the given date.

**For NeLS certificates**

Connection to the NeLS server will be lost on the given date. NBI connection will remain, as NeLS connection is not mandatory in CEE 6.

The alarm remains active until the NeLS certificates are replaced.

The alarm attributes are listed in Table 2.

Table 2 Alarm Attributes

Attribute Name	Attribute Value
Major Type	193
Minor Type	2031712
Managed Object Class	Certificate



Attribute Name	Attribute Value
Managed Object Instance	Region=<name_of_the_region>, CeeFunction=1, CtrlDomain=1, Certificate=<filename>_<index>
Specific Problem	Expiring Certificate
Event Type	OTHER
Probable Cause	m3100Indeterminate
Additional Text	Expiration date of certificate <filename>_<index>: <expiration_date>
Severity	<ul style="list-style-type: none"> <li>• MINOR (5): 30 days before expiration date</li> <li>• MAJOR (4): 15 days before expiration date</li> <li>• CRITICAL (3): 7 days before expiration date</li> </ul>

## 1.2 Prerequisites

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

### 1.2.1 Documents

Ensure that the following documents have been read:

- CEE document [SW Installation in Single Server Deployment or SW Installation in Multi-Server Deployment](#)
- CEE document [Runtime Configuration Guide](#)
- NeLS document [Certificate Management, Reference \[1\]](#)

### 1.2.2 Tools

No tools are required.

### 1.2.3 Conditions

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

- Valid CA and NBI certificates are available. For more information, refer to the [SW Installation in Single Server Deployment](#) and [SW Installation in Multi-Server Deployment](#).



- In case of vCIC and Atlas certificates, the new certificate has the same hostname as the old one. The hostname in the certificate cannot be changed with the current procedure.
- In case of single server deployment, vFuel is enabled.

## 2 Procedure

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

- If the vCIC NBI certificate expired, and the Managed Object Instance refers to the `ctrl.crt_<index>` file, see Section 2.1 on page 4.
- If the Atlas NBI certificate expired, and the Managed Object Instance refers to the `atlas.crt_<index>` file, see Section 2.2 on page 6.
- If the CA certificate for Atlas NBI expired, and the Managed Object Instance refers to the `atlas-ca.crt_<index>` file, see Section 2.3 on page 7.

In this case both the CA certificate and the NBI certificate must be replaced.

- If the CA certificate for the vCIC NBI expired, and the Managed Object Instance refers to the `ctrl-ca.crt_<index>` file, see Section 2.4 on page 9.

In this case both the CA certificate and the NBI certificate must be replaced.

- If the NeLS CA and client certificates expired, and the Managed Object Instance refers to the `tls_trusted_ca_certificate` or `tls_nels_client_certificate` files, see Section 2.5 on page 11.

Finish the procedure by carrying out the steps in Section 2.6 on page 11.

### 2.1 Replace NBI Certificate on vCIC

Perform the following:

1. If the CA certificate is also expired, replace it first, as described in Section 2.4 on page 9. Then continue with Step 2.
2. Check if there is an old, expired certificate file in `/mnt/cee_config` on vFuel.

If there is, delete it, as it is not referenced anymore in `/mnt/cee_config/config.yaml`. It is suggested to make a backup (a copy of the expired certificate file) before deleting.





**Note:** If the replacement is done before the expiration date, it is recommended to make a backup of the old certificate file.

3. Copy the new NBI certificate file to /mnt/cee\_config on vFuel.
4. If the file name is modified, update the config.yaml accordingly.
5. Install the certificate in the vFuel node by executing the below command in the Fuel master node:

```
fuel node --node <node_ids> --tasks eri_cert_copy_master =>
eri_copy_controller_certificates --force
```

Where <node\_ids> is the list of vCIC IDs from the `fuel2 node list` printout.

Example:

```
fuel node --node 1,2,3 --tasks eri_cert_copy_master =>
eri_copy_controller_certificates --force
```

6. Check that the installation was successful by using the `fuel2 task list` command.
  - a. Find the latest deployment task related to the certificate update and note down the task ID:

```
[root@fuel ~]# fuel2 task list |grep =>
deployment |tail -n1
```

An example of the output:

```
| 7 | ready | deployment | default | 1 | {} | False |
100 |
```

In the above example, the task ID is 7.

- b. Check task statuses and wait for tasks in running and pending state to complete.

If no tasks are in error state, the installation was successful.

```
[root@fuel ~]# fuel2 task history show =>
<task_id>--statuses running error pending
```

```
[root@fuel ~]#
```

An example of the command:

```
[root@fuel ~]# fuel2 task history show 7 =>
--statuses running error pending
```

7. Log in and restart the Apache service on all vCICs by executing the following command:



```
service apache2 restart
```

8. Log in to one of the vCICs and restart the haproxy service with the below command:

```
crm resource restart p_haproxy
```

9. Continue with Section 2.6 on page 11.

## 2.2 Replace NBI Certificate on Atlas

Perform the following:

1. If the vCIC NBI certificate is expired, replace it first, as described in Section 2.1 on page 4. Then continue with Step 2.
2. Check if there is an old, expired Atlas certificate file in `/mnt/cee_config` on vFuel.

If there is, delete it, as it is not referenced anymore in the `config.yaml`.

**Note:** If the replacement is done before the expiration date, it is recommended to make a backup of the old certificate file.

3. Copy the new NBI Atlas certificate file to `/mnt/cee_config` on vFuel.
4. If the file name is modified, update the `config.yaml` accordingly.
5. Install the certificates in the vFuel node by executing the below command in the Fuel master node:

```
fuel node --node <node_ids> --tasks eri_cert_⇒  
copy_master eri_copy_atlas_certificates --force
```

Where `<node_ids>` is the list of vCIC IDs from the `fuel2 node list` printout.

Example:

```
fuel node --node 1,2,3 --tasks eri_cert_copy⇒  
_master eri_copy_atlas_certificates --force
```

6. Check that the installation was successful by using the `fuel2 task list` command.
  - a. Find the latest deployment task related to the certificate update and note down the task ID:

```
[root@fuel ~]# fuel2 task list |grep ⇒  
deployment |tail -n1
```

An example of the output:



```
| 7 | ready | deployment | default | 1 | {} | False |
100 |
```

In the above example, the task ID is 7.

- b. Check task statuses and wait for tasks in running and pending state to complete.

If no tasks are in error state, the installation was successful.

```
[root@fuel ~]# fuel2 task history show =>
<task_id>--statuses running error pending
```

```
[root@fuel ~]#
```

An example of the command:

```
[root@fuel ~]# fuel2 task history show 7 =>
--statuses running error pending
```

7. In the Fuel node, transfer the certificate from the vCIC to the Atlas VM via the SBI:

```
[root@fuel ~]# scp cic-<index>:/etc/ssl/certs/CEE=>
/atlas.crt atlasadm@<atlas_sbi_ip_address>:
```

8. Login to the Atlas VM and switch to root user:

```
ssh atlasadm@<atlas_ip_address>
```

```
atlasadm@atlas:~$ sudo -i
```

9. Execute the below command to update the certificate:

```
root@atlas:~# atlas update-cert --atlas /home=>
/atlasadm/atlas.crt
```

10. Copy atlas.crt file to /etc/ssl/certs directory by executing the below command:

```
root@atlas:~# cp /home/atlasadm/atlas.crt =>
/etc/ssl/certs/atlas.crt
```

11. If the CA certificate is also expired, continue with Section 2.3 on page 7.

Else, continue with Step 12.

12. Reload the configuration by running the following commands:

```
root@atlas:~#service apache2 reload
service haproxy restart
```

13. Continue with Section 2.6 on page 11.



## 2.3 Replace CA Certificate on Atlas

In case the CA certificate for Atlas has expired, both the CA certificate and the NBI certificate must be replaced.

Perform the following:

1. If the vCIC CA certificate is expired, replace it first, as described in Section 2.4 on page 9. Then continue with Step 7.
2. Check if there is an old, expired Atlas CA certificate file in `/mnt/cee_config` on vFuel.

If there is, delete it, as it is not referenced anymore in the `config.yaml`.

**Note:** If the replacement is done before the expiration date, it is recommended to make a backup of the old certificate file.

3. Copy the new Atlas CA certificate file to `/mnt/cee_config` on vFuel.
4. If the file name is modified, update the `config.yaml` accordingly.
5. Install the certificates on the vCIC by running the below command:

```
fuel node --node <node_ids> --tasks eri_cert_copy⇒
_master eri_cert_create_dir eri_copy_controller⇒
_certificates eri_copy_ca_certificates eri_copy⇒
_atlas_certificates eri_copy_atlas_ca_certificates ⇒
eri_bundle_ca_certs --force
```

Where `<node_ids>` is the list of vCIC IDs from the `fuel2 node list` printout.

Example:

```
fuel node --node 1,2,3 --tasks eri_cert_copy⇒
_master eri_cert_create_dir eri_copy_controller⇒
_certificates eri_copy_ca_certificates eri_copy⇒
_atlas_certificates eri_copy_atlas_ca_certificates ⇒
eri_bundle_ca_certs --force
```

6. Check that the installation was successful by using the `fuel2 task list` command.
  - a. Find the latest deployment task related to the certificate update and note down the task ID:

```
[root@fuel ~]# fuel2 task list |grep ⇒
deployment |tail -n1
```

An example of the output:

```
| 7 | ready | deployment | default | 1 | {} | False |
100 |
```



In the above example, the task ID is 7.

- b. Check task statuses and wait for tasks in running and pending state to complete.

If no tasks are in error state, the installation was successful.

```
[root@fuel ~]# fuel2 task history show =>
<task_id>--statuses running error pending
```

```
[root@fuel ~]#
```

An example of the command:

```
[root@fuel ~]# fuel2 task history show 7 =>
--statuses running error pending
```

7. Transfer the CA certificate from the vCIC to the Atlas VM via the SBI by executing the below command in vFuel:

```
[root@fuel ~]# scp cic-x:/etc/ssl/certs/CEE=>
/atlas-ca.crt atlasadm@atlas_ SBI:
```

8. Login to the Atlas VM and switch to root user:

```
ssh atlasadm@<atlas_ip_address>
```

```
atlasadm@atlas:~$ sudo -i
```

9. Execute the below command to update the certificate:

```
root@atlas:~# atlas update-cert --cee /home=>
/atlasadm/atlas-ca.crt
```

10. Continue with Section 2.6 on page 11.

## 2.4 Replace CA and NBI Certificates on vCIC

In case the CA certificate for the vCIC has expired, both the CA certificate and the NBI certificate must be replaced.

Perform the following:

1. Check if there is an old, expired certificate file in /mnt/cee\_config on vFuel.

If there is, delete it, as it is not referenced anymore in config.yaml.

**Note:** If the replacement is done before the expiration date, it is recommended to make a backup of the old certificate file.

2. Copy the new NBI certificate file and the CA authority certificate (or chain of certificates) to /mnt/cee\_config on vFuel.



3. If any of the file names are modified, update the `config.yaml` accordingly.
4. Install the certificates in the vFuel node by executing the below command in the Fuel master node:

```
fuel node --node <node_ids> --tasks eri_cert_copy⇒  
_master eri_copy_controller_certificates eri_copy⇒  
_ca_certificates eri_copy_atlas_certificates eri_copy⇒  
_atlas_ca_certificates eri_bundle_ca_certs --force
```

Where `<node_ids>` is the list of vCIC IDs from the `fuel2 node list` printout.

Example:

```
fuel node --node 1,2,3 --tasks eri_cert_copy⇒  
_master eri_copy_controller_certificates eri_copy⇒  
_ca_certificates eri_copy_atlas_certificates eri_copy⇒  
_atlas_ca_certificates eri_bundle_ca_certs --force
```

5. Check that the installation was successful by using the `fuel2 task list` command.
  - a. Find the latest deployment task related to the certificate update and note down the task ID:

```
[root@fuel ~]# fuel2 task list |grep ⇒  
deployment |tail -n1
```

An example of the output:

```
| 7 | ready | deployment | default | 1 | {} | False |  
100 |
```

In the above example, the task ID is 7.

- b. Check task statuses and wait for tasks in running and pending state to complete.

If no tasks are in error state, the installation was successful.

```
[root@fuel ~]# [ fuel2 task history show ⇒  
<task_id>--statuses running error pending
```

```
[root@fuel ~]#
```

An example of the command:

```
[root@fuel ~]# fuel2 task history show 7 ⇒  
--statuses running error pending
```

6. Restart the Apache service on all vCICs by executing the following command:  
  
**service apache2 restart**



7. Log in to one of the vCICs and restart the haproxy service with the below command:

```
crm resource restart p_haproxy
```

8. Continue with Section 2.6 on page 11.

## 2.5 Replace CA and Client NeLS Certificates

If one or both of the NeLS certificates are expired, perform the procedure described in section [Configure License Management in the Runtime Configuration Guide](#).

## 2.6 Post Actions

After replacing the certificate, do the following:

1. Check that the certificate is working by doing the following steps:

- For vCIC certificates: execute at least one OpenStack command from the vCIC.

For example, execute the below command:

```
nova list
```

- For Atlas certificates: open Atlas GUI.

In case Atlas GUI was opened before the procedure started, close the browser and launch it again. Clicking **Refresh** is not sufficient.

2. Wait for the alarm to cease. This can take up to one hour.

The following scenarios are possible:

- The procedure was successful, the alarm ceases.

If the alarm ceases, exit this procedure.

- Or the procedure did not solve the problem.

In this case, proceed to Step 3.

3. Collect troubleshooting data as described in the [Data Collection Guideline](#).
4. Contact the next level of maintenance support. Further actions are outside the scope of this instruction.
5. The job is completed.



### 3 Additional Information

The alarm is ceased when the expired certificate or certificates are replaced. This can take up to one hour.





## Reference List

- [1] Certificate Management, 1551-CRA 119 1933