ERICSSON

Expiring Certificate

Cloud Execution Environment

OPERATING INSTRUCTIONS

2/1543-CRA 119 1864/5 Uen C

Contents

1 Introduction

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

For more information on 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 NBI
- CA certificate (or chain of certificates) of the organization issuing the virtual CIC (vCIC) NBI
- Atlas NBI certificate
- vCIC NBI certificate

Note: Atlas and vCIC certificates can be issued by the same CA, or by two separate CAs.

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.

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

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

- The connection will be lost on the given date.

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`
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	• `MINOR (5)`: 30 days before expiration date • `MAJOR (4)`: 15 days before expiration date • `CRITICAL (3)`: 7 days before expiration date

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:

- 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 single server deployment, vFuel is enabled.

2 Procedure

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

- If the Atlas NBI certificate expired, see Section 2.1 on page 3.
- If the vCIC NBI certificate expired, see Section 2.2 on page 5.
- If the CA certificate for Atlas NBI expired, see Section 2.3 on page 5.

  In this case both the CA certificate and the NBI certificate must be replaced.
- If the CA certificate for the vCIC NBI expired, see Section 2.4 on page 6.

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

Finish the procedure by carrying out the steps in Section 2.5 on page 6.

2.1 Replace NBI Certificate on Atlas

Perform the following:

1. Log on to Atlas VM:
   ```
   <user@laptop>:~# ssh atlasadm@<atlas_ip_address
   > atlasadm@atlas:~$ sudo -i
   ```
2. Change the NBI certificate on Atlas by following the below procedure.

Note: The certificate and the private key are separated by delimiter lines:

```
-----BEGIN CERTIFICATE-----

<...>

-----END CERTIFICATE-----

-----BEGIN PRIVATE KEY-----

<...>

-----END PRIVATE KEY-----
```

Split the Atlas NBI certificate file in `/mnt/cee_config`, which is present on vFuel, into two parts (private key and NBI certificate) with the below commands:

```
sed -n '/BEGIN.*PRIVATE KEY/,/END.*PRIVATE KEY/p'
/mnt/cee_config/atlas-rsa.pem > atlas.key

sed -n '/BEGIN CERTIFICATE/,/END CERTIFICATE/p'
/mnt/cee_config/atlas-rsa.pem > atlas.pem
```

Copy the two files to the below locations in the Atlas VM:

a. Copy the private key (`atlas.key`) to `/etc/ssl/private/atlas.key`.

   In case the file already exists, overwrite it. Do not store multiple keys in this file.

   Verify that the permissions of `atlas.key` are as follows:

   ```
   rw-r----- 1 root ssl-cert
   ```

   If not, change the permissions using the following commands:

   ```
   root@atlas:~#chown root:ssl-cert⇒
    /etc/ssl/private/atlas.key
   root@atlas:~#chmod 640 /etc/ssl/private/atlas.key
   ```

b. Copy the Atlas NBI certificate (`atlas.pem`) to `/etc/ssl/certs/atlas.pem`

   In case the file already exists, overwrite it. Do not store multiple certificates in this file.

   Verify that the permissions of `atlas.pem` are as follows:

   ```
   -rw-r--r-- 1 root root
   ```

   If not, change the permissions using the following commands:

   ```
   root@atlas:~#chmod 644 /etc/ssl/certs/atlas.pem
   ```

3. If the CA certificate is also expired, continue with Section 2.3 on page 5.

   Else, continue with Step 4.

4. Reload the configuration by running the following commands:

   ```
   root@atlas:~#service apache2 reload
   service ovft-api restart
   service heat-api restart
   ```

5. Continue with Section 2.5 on page 6.

2.2 Replace NBI Certificate on vCIC

Perform the following:

1. If the CA certificate is also expired, continue with Section 2.4 on page 6.

   Else, continue with Step 3.

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 `config.yaml`.

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 on the vCIC with the below script:

   ```
   cd /usr/share/ericsson-orchestration/playbooks

   openstack-ansible infra-certificate-install.yml
   ```

6. Continue with Section 2.5 on page 6.

2.3 Replace CA Certificate on Atlas

Before you start the below procedure, make sure you are logged on to Atlas VM and the NBI certificate is already replaced.

1. Append the new CA certificate (or chain of certificates) to the `/etc/ssl/certs/ca-certificates.crt` file by following the below steps:

   a. Check if there is an old, expired certificate file in the system certific ate directory `/usr/share/ca-certificates/<cacert_file>`.

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

b. Copy the new CA certificate to the system certificate directory `/usr/share/ca-certificates/<cacert_file>`

c. Edit the `ca-certificates` configuration file `/etc/ca-certificates.conf`. Add the name of the file you copied to `/usr/share/ca-certificates` to the top of the list, after the final `#`.

d. Update the CA certificates database by executing the following command:
`root@atlas:~#update-ca-certificates`

The certificate is now imported into the `System CA Certificates` database.

2. Continue with Section 2.5 on page 6.

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 have to 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`.

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 on the vCIC with the below script:

   `cd /usr/share/ericsson-orchestration/playbooks`

   `openstack-ansible infra-certificate-install.yml`

5. Continue with Section 2.5 on page 6.

2.5 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*. For alarm-specific logs, refer to the Table *Data Collection for Alarms and Alerts* 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.