ERICSSON

Security User Guide

Cloud Execution Environment

USER GUIDE

1/1553-CRA 119 1864/5 Uen C

Contents

1 Introduction

This document describes security management for the supported security services in the Cloud Execution Environment (CEE).

The supported security services are as follows:

- Identity and access management, as described in Section 2 on page 2
- Password policies, as described in Section 2.4 on page 12
- Privileged access, as described in Section 2.5 on page 12
- Audit and security logging and monitoring, as described in Section 3 on page 14
- Network security, as described in Section 4 on page 17
- Transport Layer Security for Atlas dashboard, as described in Section 5 on page 18
- Vulnerability management, as described in Section 6 on page 19

Note: Security management of EMC² ScaleIO as Cinder backend is out of the scope of this document. Refer to the section about security management of the document *EMC ScaleIO Version 2.0.x User Guide* and *EMC ScaleIO Version 2.0.x Security Configuration Guide* for more information.

2 Identity and Access Management

The purpose of Cloud Execution Environment Identity and Access Management (CEE IdAM) is to manage identities and credentials for cloud users, and to provide authentication and access control services for user accesses.

The IdAM architecture in CEE is shown in Figure 1.

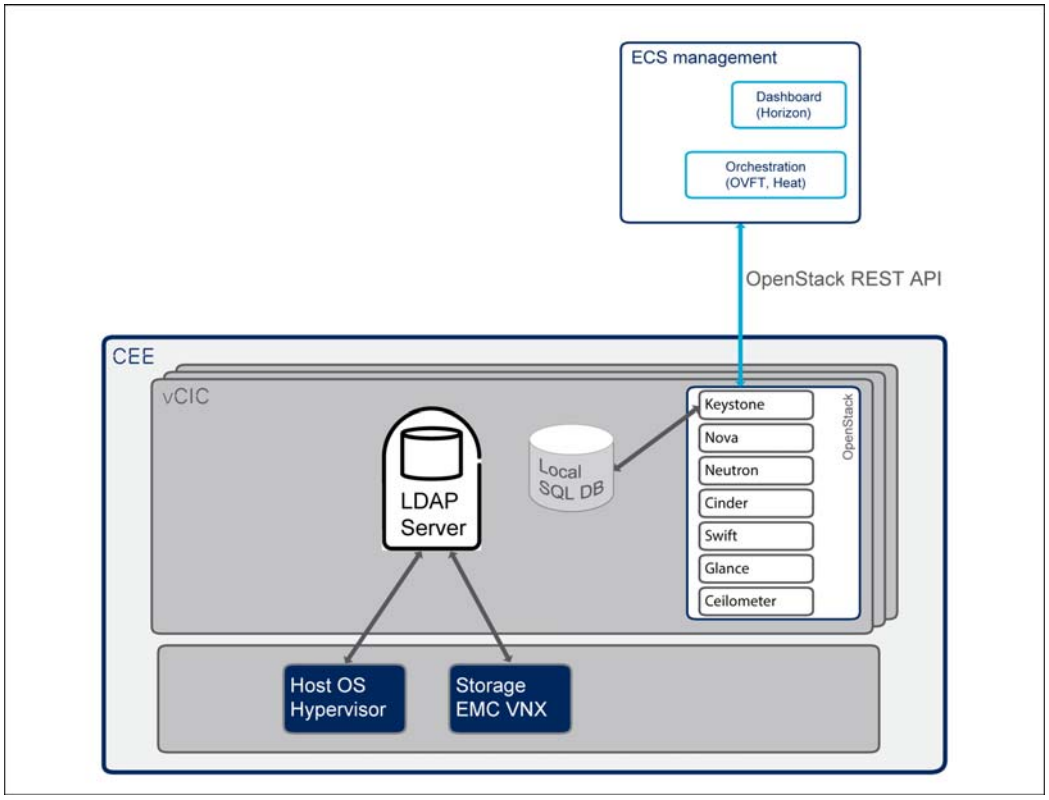

Figure 1 Identity and Access Management in the CEE

Managed Areas

CEE IdAM can be used to manage the following:

- Users, see Section 2.1 on page 3
- LDAP groups, see Section 2.2 on page 9
- Passwords, see Section 2.3 on page 10
- Password policies, see Section 2.4 on page 12
- Privileged access, see Section 2.5 on page 12

Configuration

The CEE IdAM tool uses internal default configuration options, or configuration parameters stored in the `cee-idam.conf` file under `/etc/cee-idam/`, or both. The initial configuration files are created during installation with parameter values collected from `config.yaml` file.

The IdAM section of the `config.yaml` file has the following main sections:

- `ldap`
- `userlist`
- `user`

For an example of the default configuration options of the `idam` section of `config.yaml` see Section 8 on page 25 in the Appendix.

For more information about IdAM configuration refer to *Configuration File Guide*.

For more information about the CEE IdAM tool refer to *Infrastructure Administrator Management Guide*.

For a functional description of IdAM components, refer to *CEE Technical Description*.

2.1 Main User Types

The CEE IdAM solution differentiates between the following user types:

- Cloud Infrastructure Administrators, see Section 2.1.1 on page 3
- Local Administrators, see Section 2.1.2 on page 4

OpenStack Users are managed by default Keystone and Dashboard operations, not by the CEE IdAM tool, see Section 2.1.3 on page 4.

The VNX storage solution is managed by either LDAP users managed by the CEE IdAM tool or VNX global administrators, as described in Section 2.1.4 on page 5.

2.1.1 Cloud Infrastructure Administrators

Cloud infrastructure administrators (for example `ceeadm`) manage certain CEE infrastructure components, such as hypervisor blades, network switches, Cloud Infrastructure Controllers (CICs), and the storage system.

Note: Linux users, storage system users (EMC VNX), and network device users (Extreme switches) are considered to be infrastructure users.

The cloud infrastructure administrator accounts are stored on a Lightweight Directory Access Protocol (LDAP) server that acts as a centralized IdAM repository for the CEE. It supports the provisioning and authentication for `ceeadm`, ensuring that only authorized entities are allowed to access the resources, in line with the defined security policies. When trying to access an infrastructure component, the credentials of the user are verified against the credentials stored in the LDAP Server.

2.1.2 Local Administrators

In case the system needs to be accessed by either a user or a service when LDAP is not available, initial local accounts are predefined. For security and personal accountability reasons, the use of root must be limited.

In the scope of IdAM and CEE nodes the `atlasadm` and `cmha` users are created and SSH-keys are distributed for them.

These users belong to user groups that have sudo permissions without passwords, and access defined from each CIC to all other nodes. For more information about sudo user groups, refer to Section 2.5 on page 12.

On the vCICs the following users are created: `ceebackup` for backup and restore, and `ceecore` for crash and core management.

Predefined Local Administrators

atlasadm — The initial system user `atlasadm` with sudo rights is created during the prehardening. The password of the `atlasadm` user is set as part of the installation procedure. For more information refer to the Atlas documentation.

ceebackup — This administrator is used for backup and restore processes. `ceebackup` is only used on the vCICs.

ceecore — This administrator is used for crash and core management. `ceecore` is only used on the vCICs.

cmha — This is the administrator used by the CM-HA component.

2.1.3 Managing OpenStack Cloud Users

OpenStack users are managed by the default Keystone and Dashboard operations. For these operations refer to the corresponding OpenStack documentation, Reference [1].

OpenStack Cloud Administrators

OpenStack cloud administrators (`openstack-admin`) are consumers of CEE resources exposed through OpenStack services. OpenStack cloud

administrators manage OpenStack tenants, users, roles, services, and images. After installation the identity `admin` is automatically created and is a member of this group.

The `openstack-admin` identities are managed by the OpenStack component Keystone. Keystone acts as an authentication server for `openstack-admin`, using a local SQL database in the CEE as a back-end for the identities. For detailed information about the Atlas Dashboard from an administrator perspective refer to OpenStack documentation, Reference [1].

OpenStack Cloud Users

OpenStack users are able to provision their own resources within the limits set by the `openstack-admin`. For more information about OpenStack cloud users refer to OpenStack documentation, Reference [1].

Note: There is no automatically created OpenStack user after installation.

2.1.4 VNX User Management

In the CEE, the following user types are defined for the VNX storage solution:

LDAP User

LDAP users are to be used by system administrators to manage the VNX storage system unless the LDAP service is unavailable. For the predefined storage LDAP groups see Section 2.2 on page 9.

VNX Global Administrator User

VNX global administrator users are to be used in the following scenarios:

- During the installation of the system
- In case the LDAP service is not available
- When the VNX LDAP credentials have not yet been identified and implemented, but the operator needs to run commands for VNX
- When there is no LDAP user available with an administrator role, but the operator needs to run commands for VNX
- For services such as OpenStack Cinder and VNX log fetcher, which do not have dependency to the LDAP service

Note: The VNX global administrators are defined with scope global (0), which means that the user has the same permissions on all VNX systems within a domain.

For more information about VNX user management, refer to EMC documentation, Reference [3].

2.1.4.1 Managing LDAP Users

The user credentials of LDAP users are cross-checked with the registries in the LDAP server in the system. If the credentials are correct, the role of the user is set depending on the role mapping between the group of the user in LDAP and the role on the VNX.

In order to avoid hardcoded user names and passwords when running `naviseccli` commands towards the VNX, use security files. For the detailed description of the use of security files, see Section 2.1.4.3 on page 7.

The security files have to be recreated if the password has been changed. In order to ensure that `naviseccli` commands can be run without explicitly giving the user credentials, the security files have to be created for each CIC.

2.1.4.2 Managing VNX Global Administrator Users

The installation scripts read the credentials of the VNX global administrator from the `config.yaml` file. It is strongly recommended to use site-specific credentials for the VNX global administrator. To set the credentials, the following values need to be configured in the `config.yaml` file, under "storage" > "centralized" > "emc_admin" as shown in Example 1.

```
storage:
       centralized:
         type: None
         hw_type: VNX5400
         storagepool_name: cinderpool
         mgmt_ip_A: 192.168.2.12
         mgmt_ip_B: 192.168.2.13
         emc_admin:
           user: <admin_name>
           passwd: <admin_password>
```

Example 1 VNX Global Administrator User Settings

Apart from the installation process, the VNX global administrator users have to be handled manually. This means that the credentials have to be given in the `naviseccli` command (`-user xxxx -password xxxx -scope 0`), unless a security file has been created.

For the predefined global administrator users the security files are automatically created during installation.

VNX Global Administrator for Cinder

OpenStack Cinder service has been configured to use the VNX global administrator user `cinder` with a security file. This user is created during the installation with a randomly generated password. The security file is created to avoid cleartext username and password in the following places:

- Cinder configuration files
- Cinder communication (naviseccli commands) to the VNX
- Logfiles

VNX Global Administrator for vnx-log-fetcher

The `vnx-log-fetcher` account has been configured to use a VNX global administrator user with a security file. This user is created during installation with a randomly generated password and a security file. This account is used by the `vnx-log-fetcher` component to periodically retrieve security related log files from the VNX storage system.

Listing VNX Global Administrators

List existing users with administrator rights and `global` scope with the following command:

```
/opt/Navisphere/bin/naviseccli -h <vnx-sp-ip> -user⇒
<user> -password <passwd> -scope 0 security -list |⇒
grep administrator

/opt/Navisphere/bin/naviseccli -h 192.168.2.12⇒
 -user admin -password ericsson -scope 0 security -list
Username:  admin
Role:      administrator
Scope:     global
```

Example 2 Listing VNX Global Users with Admin Rights

Changing Passwords for the VNX Global Administrator

Run the following command as the user for which the security files have been created (for example, to change the password for the ceeadm VNX global user, the command must be executed as ceeadm user):

```
/opt/Navisphere/bin/naviseccli -h <vnx-sp-ip> security⇒
-changepassword -newpassword <new password>
```

Note: The security files have to be recreated on all CICs after changing the password.

2.1.4.3 VNX Security Files

Using a Security File

If there is a valid security file created for the Linux user, the following credential parameters do not have to be given anymore when running a `naviseccli` command:

- User
- Password
- Scope

Run the `naviseccli` command as follows:

`/opt/Navisphere/bin/naviseccli -h <vnx-sp-ip> cmd`

Note: Security files contain information about the host where they have been created. It means that a security file must be created for each CIC.

Creating a Security File

Create a security file with the following command:

`/opt/Navisphere/bin/naviseccli -addusersecurity -user⇒ <username> -password <password> -scope 0 [-secfilepath⇒ <path>]`

Two encrypted files are created:

```
SecuredCLIXMLEncrypted.key
SecuredCLISecurityFile.xml
```

The `secfilepath` argument can be used to specify a different location for those two files than the home directory. If used, the parameter has to be used as well in each **`naviseccli`** command where the credentials are omitted.

```
<personal-user>@cic-1:~$ /opt/Navisphere/bin/naviseccli
-addusersecurity -user testusername -password⇒
 testpwd -scope 0 -secfilepath /temp
```

Example 3 Creating a Security File

```
<personal-user>@cic-1:~$ /opt/Navisphere/bin/naviseccli
 -h 192.168.2.12 -secfilepath /temp ntp -list -servers
address:  192.168.2.20
serverkey:  0
keyvalue:  ""
```

Example 4 Executing a naviseccli Command Without Specifying User Credentials

2.1.4.4 Synchronizing LDAP and VNX

After the password was successfully changed, the old security files still work for some time, as VNX synchronizes only every 24 hours. However, it is possible to trigger the synchronization manually as a global administrator user.

The advantage of this is that the running processes using the security files in the `naviseccli` commands are not interrupted between the password change and the creation of new security files.

Note: The security files must still be created immediately after the password change.

In order to manually synchronize LDAP and VNX, follow these steps:

1. Log into one of the CICs.

2. Run the following command as VNX Global Administrator User:

   /opt/Navisphere/bin/naviseccli -h *<vnx-sp-ip>* -user⇒ *<global-admin>* -password *<pwd>* -scope 0 security⇒ -ldap -synchronize

```
<personal-user>@cic-1:~$ /opt/Navisphere/bin/naviseccli⇒
 -h 192.168.2.12 -user admin -password ericsson -scope 0⇒
 security -ldap -synchronize
Confirm: You are about to synchronize with the following
LDAP server:
192.168.2.20

All users that are currently logged into this service⇒
 connection(s) and are affected by any changes will be⇒
 logged off!

Proceed?(y/n) y
```

Example 5 Manual LDAP Synchronization

Note: All affected users are logged off, for example, when connected to the system through the VNX Graphical User Interface (GUI).

2.1.5 BSP User Management

BSP user management is described in BSP User Management, Reference [4].

2.2 LDAP Groups

Table 1 shows the predefined LDAP groups. These groups are automatically created during the installation.

Table 1 Predefined LDAP Groups

ID	Name	Purpose
10000	DirectoryAdmins	Members are allowed to manage LDAP content
10001	ldap_users	LDAP user group with no special privileges
20001	storage_admin	LDAP group mapped for VNX admin role
20002	storage_storageadmin	LDAP group mapped for VNX storageadmin role
20003	storage_sanadmin	LDAP group mapped for VNX sanadmin role
20004	storage_networkadmin	LDAP group mapped for VNX networkadmin role
20005	storage_operator	LDAP group mapped for VNX operator role
20006	storage_securityadmin	LDAP group mapped for VNX securityadmin role
27000	sudo	This is the default system sudo group. It prompts users for password when executing a **`sudo`** command.
27001	ceesudo	Members of the this group are allowed to issue **`sudo`** commands without being prompted for the password.
27002	ceestatus	The members of this group are allowed to query `crm` status with **`sudo`**, without being prompted for a password.
27003	ceeuseradmin	The members of this group are allowed to execute **`sudo cee-idam`** commands without being prompted for a password.

For more information about EMC VNX roles refer to the EMC documents web page, Reference [3]. The *Security Configuration Guide for VNX* can be found by clicking on **VNX Series**, **Related documentation: VNX for Block OE 5.33 and VNX for File OE 8.1**, and **Security Configuration Guide on VNX for File** under ‘‘Security and Compliance’’.

2.3 Passwords

2.3.1 Managing Password for Root User

Root user must not be used directly after the initial installation of the system. The nodes cannot be directly accessed with the root user, but passwordless

access to the node can be done with ssh from the Fuel node. The Fuel node is used for system deployment and upgrades, and it is strongly recommended to change the root password after installation, or whenever the current password has been used to access the system.

The root password in Fuel can be changed with the **passwd** command.

The root password in all deployed CEE nodes can be changed using the `idamsetup` script in the Fuel node. In order to change the root password, save the new password to a file and use it with a local account with sudo privileges or as root user if no other users exist:

```
idamsetup -u root -c <filename>
```

Note: The direct inclusion of the password in the command **idamsetup -u root -p** *<password>* is **not recommended** as this is visible in the history and the argument list.

2.3.2 Managing Password for Predefined Users

The command `passwd` has to be used to change the password of `ceeadm`. The password has to be changed both on Fuel and on one of the CICs.

Example:

Fuel:

```
[root@fuel ~]# passwd ceeadm
 Changing password for user ceeadm.
 New password:
 Retype new password:
 passwd: all authentication tokens updated successfully.
```

vCIC:

```
root@cic-1:~# passwd ceeadm
 New password:
 Retype new password:
 LDAP password information changed for ceeadm
 passwd: password updated successfully
```

Other passwords of predefined users in all deployed CEE nodes including the Fuel system can be changed using the `idamsetup` script in the Fuel node. This command must be executed as a local account with `sudo` privileges, or as root user if no other users exist.

Note: The password change **does not apply** to nodes, that are deployed (for example, because of expansion, or Upgrade and Rollback) after the password has been changed. For these nodes the password configured during the initial system installation is applied, and must be changed immediately after the nodes have been deployed.

2.3.3 Distributing SSH-keys for Personal Accounts

Individual users do not have any individual SSH-keys generated. Each user must create their own SSH-key pairs, and distribute the keys to any node they have access to, and to which they would like to use SSH-keys instead.

2.4 Password Policies

CEE supports the use of password policies for users provisioned in the LDAP user repository.

It is also possible to map policies to a user by using the CEE IdAM tool. The policy name to be used is provided either when the user is created or when the user is modified. By default, the Standard policy is applied, when no other policy is set.

For more information, refer to *Infrastructure Administrator Management Guide*.

2.5 Privileged Access

Users are granted privileged access through sudo. Sudo privileges are available for users who are members of one of the sudo groups. Users can be added to various sudo user groups.

Note: With the exception of `ceebackup` all these groups are stored on the LDAP server. Therefore in maintenance mode only `ceebackup` group exists.

These groups are the following:

- `ceebackup`

  The members of the this group are allowed to issue `sudo` commands without being prompted for the password.

- `ceestatus`

  The members of this group are allowed to query `crm` status with sudo, without being prompted for a password.

- `ceesudo`

  The members of the this group are allowed to issue `sudo` commands without being prompted for the password.

- `ceeuseradmin`

  The members of this group are allowed to execute `sudo cee-idam` commands without being prompted for a password.

- `sudo`

  This is the default system sudo group. It prompts users for password when executing a sudo command.

For information about how to manage sudo groups, refer to *Infrastructure Administrator Management Guide*.

3 Security and Audit Trail Logging

CEE offers a logging service by which security- and audit trail-related events are logged into a central log collector residing inside the Atlas VM, using Reliable Event Logging Protocol (RELP).

3.1 Logging Service Architecture

The logging service architecture is shown in Figure 2.

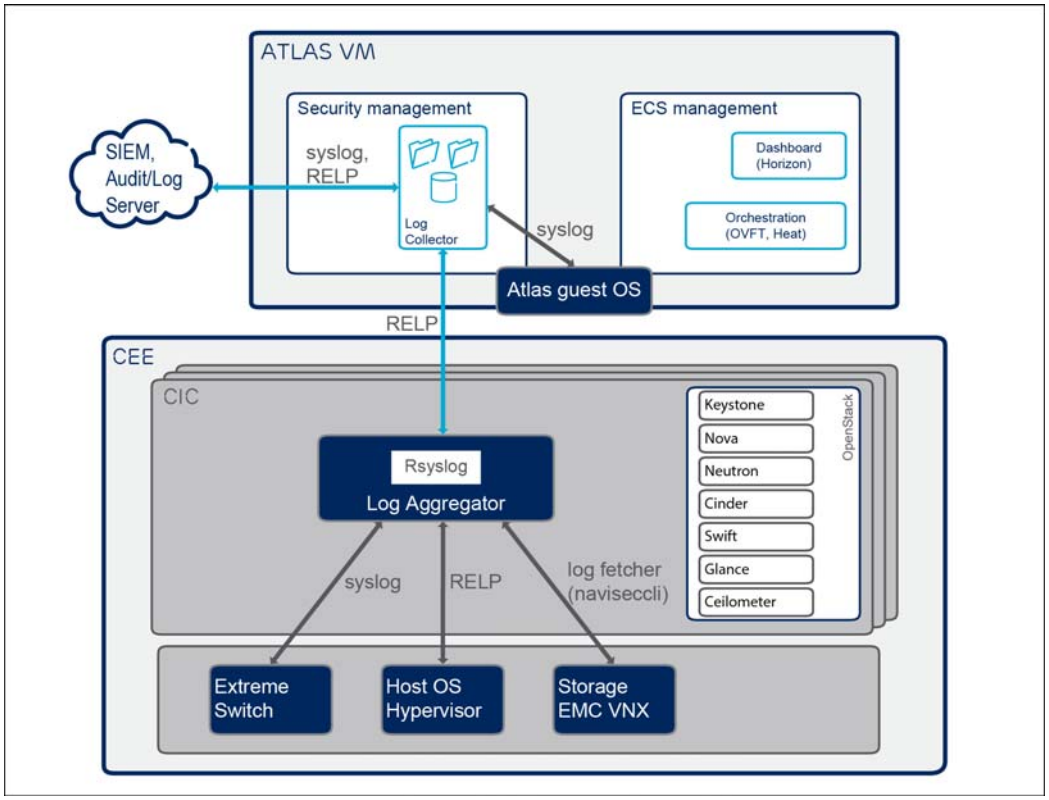

Figure 2 Logging Service Architecture

The logging service consists of the following components:

Logging Clients

Client components send security and audit log events to the log aggregator server as follows:

- EMC VNX

  Audit and security log records are fetched periodically by `naviseccli` and forwarded by the VNX log fetcher to the log aggregator.

- Extreme switch

  Audit and log records are pushed asynchronously towards the log aggregator using the `syslog` protocol.

- Host OS, Hypervisor

  Audit and log records are pushed asynchronously towards the log aggregator over RELP.

Log Aggregator

The log aggregator receives logs from clients, and sends the logs to the southbound interface of Atlas over RELP to the log collector. If the log collector is not available, the log aggregator stores the logs in a buffer. The stored logs are transmitted to the log collector when it becomes available again.

Log Collector

The log collector receives the logs from the `rsyslog` instance of the log aggregator over RELP protocol.

SIEM

The external Security Information and Event Management (SIEM) systems provide the possibility for real-time data analysis. Audit log events can be transferred without data loss from the log collector over RELP protocol and `syslog` over TCP to one or multiple SIEMs.

3.2 Log Types

The following logs are created by the logging service:

Audit Trail Log

The audit trail log contains detailed information about system configuration changes. This audit tool enables the service provider to check who carried out specific operations in the system, and when.

The configuration of the Linux audit subsystem is generated during the execution of the `eri_audit` playbook. There is no API or CLI for changing the configuration, so when changes are needed, use the following procedure:

Update the `/usr/share/ericsson-orchestration/ansible/playbooks/roles/eri_audit_logging/templates/auditd/audit.rules.j2` template file on the vFuel node. Execute the below command to apply the changes:

```
cd /usr/share/ericsson-orchestration/playbooks && openstack-ansible eri-audit-logging-install.yml
```

Security Log

The security log records security events on the node. The purpose of this is to record security events, for example, failed logins and attempts to access the node with valid or invalid credentials.

Besides the events included in the audit logging, many other system events are logged through the generic logging system. Based on the `config.yaml` logging settings, log records are stored locally or forwarded to remote hosts (computes, vFuel node, external log server). Logs stored within CEE will get rotated out of existence to reclaim storage space, so if the log records must be kept for a longer period of time it is recommended to enable the external logging feature in the `config.yaml`.

Note: There is no predefined filtering of security-related events, so enabling external logging could lead to transporting a large amount of logs, using up a significant network bandwidth.

3.3 Configuring SIEM

The audit events received by the Log Collector can be forwarded to an arbitrary number of SIEM systems for further analysis and correlation. The supported protocols for forwarding events are RELP and `syslog` over TCP.

For information about configuring SIEM refer to *Security Information and Event Management*.

4 Network Security

In CEE, the Data Center Firewall (DCFW) provides protection for the system. The DCFW also acts as an O&M firewall.

The DCFW is located outside the CEE.

The connectivity and network description of the DCFW is described in detail in the *DC Firewall Hardening Guide* and *System Hardening Guideline* documents.

5 Transport Layer Security

Transport Layer Security (TLS) provides the mechanisms to ensure authentication, non-repudiation, confidentiality, and integrity of user communications for the CEE services. Secure TLS communication is supported for the OpenStack service endpoints through the northbound interface.

For settings, refer to *SW Installation in Multi-Server Deployment*or *SW Installation in Single Server Deployment*, and *Configuration File Guide*.

6 Vulnerability Management

The Ericsson Product Security Incident Response Team (PSIRT) provides a vulnerability monitoring service in order to reduce the risk of system security incidents. PSIRT constantly monitors various vulnerability information sources to sustain an up-to-date understanding of current vulnerabilities. If a new vulnerability potentially affects Ericsson products or solutions, PSIRT notifies the impacted product responsible, who then can act on the reported vulnerabilities. Within CEE, security fixes are merged into the CEE software by normal software upgrade procedures. For more information about CEE software upgrade refer to *CEE SW Update and Rollback*, and for information about the upgrade of Atlas software, refer to *Atlas SW Upgrade*.

7 Services, Ports, and Protocols

All open ports and services running on the CEE nodes, that are, CICs, compute nodes with host OS, and Atlas Dashboard are listed in this section.

Note:

- The Process ID (PID) values listed are provided as an example only. The actual PID value is assigned when the process is created and varies over time and between systems.
- Some of these ports can be blocked by the DCFW, so although they are open, they might not be reachable from outside of the system.

Namespaces

The namespaces `global`, `haproxy`, and `vrouter` are used by applications. There are additional namespaces defined on the CICs. For the full list enter the command:

```
ip netns
```

IP allocation

Two distinct networks are used for OpenStack services:

- `br-ex` interface is used by the external network
- `br-mgmt` interface is used by the internal network

The IP allocation for these services is as follows:

```
# ip a s br-ex
14: br-ex: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc ⇒
noqueue state UNKNOWN group default
    link/ether ee:f6:ba:31:f4:46 brd ff:ff:ff:ff:ff:ff
    inet 10.20.100.4/24 brd 10.20.100.255 scope global br-ex
       valid_lft forever preferred_lft forever

# ip a s br-mgmt
20: br-mgmt: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc ⇒
noqueue state UNKNOWN group default
    link/ether c6:ad:eb:08:9a:42 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.23/25 brd 192.168.2.127 scope global br-mgmt
       valid_lft forever preferred_lft forever
```

Additionally, `pacemaker` also manages virtual IP (VIP) addresses. The list of VIPs and where they are defined can be listed as follows:

```
# crm status
```

```
vip__management         (ocf::fuel:ns_IPaddr2): Started ⇒
cic-1.domain.tld
vip__vrouter_pub        (ocf::fuel:ns_IPaddr2): Started ⇒
cic-1.domain.tld
vip__vrouter    (ocf::fuel:ns_IPaddr2): Started cic-1.⇒
domain.tld
vip__public     (ocf::fuel:ns_IPaddr2): Started cic-1.⇒
domain.tld
vip__zbx_vip_mgmt       (ocf::fuel:ns_IPaddr2): Started ⇒
cic-1.domain.tld
```

These VIP addresses are defined either in the `haproxy`or in the `vrouter` namespace as follows:

```
# ip netns exec haproxy ip a s
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state ⇒
UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
31: hapr-ns: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc ⇒
pfifo_fast state UP group default qlen 1000
    link/ether 4e:77:eb:d7:df:ba brd ff:ff:ff:ff:ff:ff
    inet 240.0.0.2/30 scope global hapr-ns
       valid_lft forever preferred_lft forever
    inet6 fe80::4c77:ebff:fed7:dfba/64 scope link
       valid_lft forever preferred_lft forever
35: b_public: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc ⇒
pfifo_fast state UP group default qlen 1000
    link/ether da:33:42:22:7e:73 brd ff:ff:ff:ff:ff:ff
    inet 10.20.100.3/24 scope global b_public
       valid_lft forever preferred_lft forever
    inet6 fe80::d833:42ff:fe22:7e73/64 scope link
       valid_lft forever preferred_lft forever
37: b_management: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 ⇒
qdisc pfifo_fast state UP group default qlen 1000
    link/ether 2a:60:b2:d7:73:a1 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.21/25 scope global b_management
       valid_lft forever preferred_lft forever
    inet6 fe80::2860:b2ff:fed7:73a1/64 scope link
       valid_lft forever preferred_lft forever
39: b_zbx_vip_mgmt: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 ⇒
qdisc pfifo_fast state UP group default qlen 1000
    link/ether 22:6e:f3:37:df:3a brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.22/25 scope global b_zbx_vip_mgmt
       valid_lft forever preferred_lft forever
    inet6 fe80::206e:f3ff:fe37:df3a/64 scope link
       valid_lft forever preferred_lft forever
```

```
# ip netns exec vrouter ip a s
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state ⇒
UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
23: vr-host-ns: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 ⇒
qdisc pfifo_fast state UP group default qlen 1000
    link/ether e2:46:cf:f5:d6:d9 brd ff:ff:ff:ff:ff:ff
    inet 240.0.0.6/30 scope global vr-host-ns
       valid_lft forever preferred_lft forever
    inet6 fe80::e046:cfff:fef5:d6d9/64 scope link
       valid_lft forever preferred_lft forever
33: conntrd: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc ⇒
pfifo_fast state UP group default qlen 1000
    link/ether 12:37:ce:a5:c1:c9 brd ff:ff:ff:ff:ff:ff
    inet 240.1.0.23/24 scope global conntrd
       valid_lft forever preferred_lft forever
    inet6 fe80::1037:ceff:fea5:c1c9/64 scope link
       valid_lft forever preferred_lft forever
45: b_vrouter: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc ⇒
pfifo_fast state UP group default qlen 1000
    link/ether 96:fb:c8:42:4f:0f brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.20/25 scope global b_vrouter
       valid_lft forever preferred_lft forever
    inet6 fe80::94fb:c8ff:fe42:4f0f/64 scope link
       valid_lft forever preferred_lft forever
47: b_vrouter_pub: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 ⇒
qdisc pfifo_fast state UP group default qlen 1000
    link/ether 12:ee:ca:b2:e2:4e brd ff:ff:ff:ff:ff:ff
    inet 10.20.100.2/24 scope global b_vrouter_pub
       valid_lft forever preferred_lft forever
    inet6 fe80::10ee:caff:feb2:e24e/64 scope link
       valid_lft forever preferred_lft forever
```

Refer to Table 2 for IP address allocation overview.

Table 2 IP address allocation

IPv4 address	Network namespace	Usage
10.20.100.2/24	`vrouter`	VIP address on the public network (`vip__vrouter_pub`)
10.20.100.3/24	`haproxy`	VIP address on the public network (`vip__public`)

IPv4 address	Network namespace	Usage
10.20.100.4 10.20.100.5 10.20.100.6	global	CIC individual NBI IP address
192.168.2.20/25	vrouter	VIP address on the management network (vip__vrouter)
192.168.2.21/25	haproxy	VIP address on the management network used for OpenStack services (vip__management)
192.168.2.22/25	haproxy	VIP address used for Zabbix web UI (vip__zbx_vip_mgmt)
192.168.2.23/25	global	private address on the management network

Reachable services

The tools netstat and lsof are used to report where services are bound.

The services reachable from the public network are divided into the following categories:

- Listening only on the vip__public address:

```
# ip netns exec haproxy lsof -nP -i @10.20.100.3

COMMAND     PID     USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
haproxy    9253  haproxy    9u  IPv4  58870      0t0  TCP 10.20.100.3:5000 (LISTEN)
haproxy    9253  haproxy   11u  IPv4  58872      0t0  TCP 10.20.100.3:35357 (LISTEN)
haproxy    9253  haproxy   13u  IPv4  58874      0t0  TCP 10.20.100.3:8773 (LISTEN)
haproxy    9253  haproxy   15u  IPv4  58876      0t0  TCP 10.20.100.3:8774 (LISTEN)
haproxy    9253  haproxy   18u  IPv4  58879      0t0  TCP 10.20.100.3:8776 (LISTEN)
haproxy    9253  haproxy   20u  IPv4  58881      0t0  TCP 10.20.100.3:9292 (LISTEN)
haproxy    9253  haproxy   22u  IPv4  58883      0t0  TCP 10.20.100.3:9696 (LISTEN)
haproxy    9253  haproxy   28u  IPv4  58889      0t0  TCP 10.20.100.3:8080 (LISTEN)
haproxy    9253  haproxy   30u  IPv4  58891      0t0  TCP 10.20.100.3:8777 (LISTEN)
haproxy    9253  haproxy   32u  IPv4  58893      0t0  TCP 10.20.100.3:6080 (LISTEN)
haproxy    9253  haproxy   34u  IPv4  58895      0t0  TCP 10.20.100.3:8052 (LISTEN)
haproxy    9253  haproxy   38u  IPv4  58899      0t0  TCP 10.20.100.3:7676 (LISTEN)
haproxy    9253  haproxy   40u  IPv4  58901      0t0  TCP 10.20.100.3:80 (LISTEN)
haproxy    9253  haproxy   43u  IPv4  58904      0t0  TCP 10.20.100.3:443 (LISTEN)
watchmen- 23111 watchmen    3u  IPv4 176697      0t0  UDP 10.20.100.3:30165
```

- Listening on the CIC individual NBI IP address:

```
root@cic-1:~# lsof -nP -i @10.20.100.4
COMMAND   PID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
ntpd    11982  ntp   22u  IPv4  70756      0t0  UDP 10.20.100.4:123
```

- Services bound to the wildcard (0.0.0.0) IPv4 address:

```
# netstat -ltunp| awk '{if ($4 ~ "0.0.0.0") { print $0 }}'
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      8198/apache2
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      6283/sshd
tcp        0      0 0.0.0.0:15672           0.0.0.0:*               LISTEN      12696/beam.smp
tcp        0      0 0.0.0.0:8888            0.0.0.0:*               LISTEN      8198/apache2
tcp        0      0 0.0.0.0:25              0.0.0.0:*               LISTEN      7104/master
tcp        0      0 0.0.0.0:35357           0.0.0.0:*               LISTEN      8198/apache2
tcp        0      0 0.0.0.0:41055           0.0.0.0:*               LISTEN      12696/beam.smp
tcp        0      0 0.0.0.0:10050           0.0.0.0:*               LISTEN      7977/zabbix_agentd
tcp        0      0 0.0.0.0:8514            0.0.0.0:*               LISTEN      485/rsyslogd
tcp        0      0 0.0.0.0:20514           0.0.0.0:*               LISTEN      485/rsyslogd
tcp        0      0 0.0.0.0:8997            0.0.0.0:*               LISTEN      25926/python
tcp        0      0 0.0.0.0:3333            0.0.0.0:*               LISTEN      6293/python
tcp        0      0 0.0.0.0:5000            0.0.0.0:*               LISTEN      8198/apache2
tcp        0      0 0.0.0.0:49000           0.0.0.0:*               LISTEN      6291/xinetd
tcp        0      0 0.0.0.0:49001           0.0.0.0:*               LISTEN      6291/xinetd
udp        0      0 0.0.0.0:40963           0.0.0.0:*                           25845/python
udp        0      0 0.0.0.0:123             0.0.0.0:*                           11955/ntpd
udp        0      0 0.0.0.0:8514            0.0.0.0:*                           485/rsyslogd
udp        0      0 0.0.0.0:514             0.0.0.0:*                           485/rsyslogd
udp        0      0 0.0.0.0:4952            0.0.0.0:*                           6320/python
udp        0      0 0.0.0.0:10514           0.0.0.0:*                           485/rsyslogd
```

For the mapping between port number and service name, refer to *System Hardening Guideline*.

8 Example Configuration for IdAM

This output is an example of an IdAM configuration in the `config.yaml` file.

Note: The content of the `config.yaml` file can be changed at installation time. For details about `config.yaml` refer to *Configuration File Guide*.

```
ericsson:
    idam:
      ldap:
        basedn: dc=cee,dc=ericsson,dc=com
        rootdn: cn=admin
        rootpw: ''
        anonymous_binddn: cn=anon
        anonymous_bindpwd: ''
        manager_binddn: cn=ldapadmin
        manager_bindpwd: ''
        sync_binddn: cn=repl
        sync_bindpwd: ''
      userlist:
      - ceeadm
      - cmha
      - ceebackup
      - ceecore
      users:
        ceebackup:
          idam_tag:
          - admin
          passwd: 'n}Z:1+#-=_$@'
        ceeadm:
          idam_tag:
          - none
          passwd: 'GT$dS4mEP\#E'
          openstack_access:
            os_tenant: admin
            os_create_account: false
            os_password: admin
            os_username: admin
            os_role: admin
        cmha:
          idam_tag:
          - none
        ceecore:
          idam_tag:
          - none
```

Reference List

[1] *OpenStack Documentation, http://docs.openstack.org, OpenStack Admin User Guide*

[2] *EMC Documentation web page, https://mydocuments.emc.com/*

[3] *EMC Documentation web page, https://mydocuments.emc.com/, Security Configuration Guide for VNX*

[4] *BSP User Management*, 6/1553-APR 901 0549/1