

# Security User Guide

Cloud Execution Environment

USER GUIDE

**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>
<b>2</b>	<b>Security Protocols, Algorithms, and Interfaces</b>	<b>2</b>
2.1	Interfaces	2
2.2	Algorithms	5
2.3	Protocols and Encryption	5
<b>3</b>	<b>Identity and Access Management</b>	<b>7</b>
3.1	Main User Types	8
3.1.1	Cloud Infrastructure Administrators	9
3.1.2	Local Administrators	9
3.1.3	Manage OpenStack Cloud Users	10
3.1.4	ScaleIO User Management	10
3.1.5	BSP User Management	10
3.1.6	NeLS User Management	10
3.2	LDAP Groups	10
3.3	Passwords	11
3.3.1	Change Password for root	11
3.3.2	Change Credentials for Predefined Users	12
3.3.3	Change Password for OpenStack Administrator	14
3.3.4	Change Password for CSC Administrator	18
3.3.5	Distribute SSH-keys for Personal Accounts	21
3.4	Password Policies	21
3.5	Privileged Access	21
<b>4</b>	<b>Security and Audit Trail Logging</b>	<b>23</b>
4.1	Logging Service Architecture	23
4.2	Log Types	24
4.3	Configure SIEM	25
<b>5</b>	<b>Network Security</b>	<b>27</b>
<b>6</b>	<b>Transport Layer Security</b>	<b>28</b>
<b>7</b>	<b>Vulnerability Management</b>	<b>29</b>
<b>8</b>	<b>Privacy</b>	<b>30</b>
<b>9</b>	<b>Services, Ports, and Protocols</b>	<b>31</b>
<b>10</b>	<b>Example Configuration for IdAM</b>	<b>47</b>



<b>Appendix</b>		
<b>11</b>	<b>Command Descriptions</b>	<b>48</b>
11.1	passwd	48
11.2	idamsetup	49
<b>Reference List</b>		<b>51</b>



# 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:

- Security protocols, algorithms and interfaces used in CEE, as described in Section 2 on page 2
- Identity and access management, as described in Section 3 on page 7
- Password policies, as described in Section 3.4 on page 21
- Privileged access, as described in Section 3.5 on page 21
- Audit and security logging and monitoring, as described in Section 4 on page 23
- Network security, as described in Section 5 on page 27
- Transport Layer Security (TLS) for Atlas dashboard, as described in Section 6 on page 28
- Vulnerability management, as described in Section 7 on page 29

**Note:** The security management of EMC<sup>2</sup> ScaleIO as Cinder back end is out of the scope of this document. Refer to the section about security management of the documents [Dell EMC ScaleIO Version 2.x User Guide](#) and [Dell EMC ScaleIO Version 2.x Security Configuration Guide](#) for more information.



## 2 Security Protocols, Algorithms, and Interfaces

CEE uses encryption on public facing interfaces to ensure that no eavesdropping or data alteration happens during transit. OpenStack REST APIs are reachable using HTTPS, data is encrypted on the virtual Cloud Infrastructure Controller (vCIC) nodes before it is sent out to the external network. Data is decrypted on the virtual CICs (vCICs), then the unencrypted data is sent to the internal management network. Low level cloud infrastructure management access uses Secure Shell (SSH) and SFTP protocols.

Atlas is an optional component of CEE. When installed, the Atlas virtual machine (VM) exposes OpenStack endpoints using HTTPS and provides management access through SSH to ensure that management sessions are encrypted.

Control and management interfaces with the relevant protocols are shown in Figure 1.

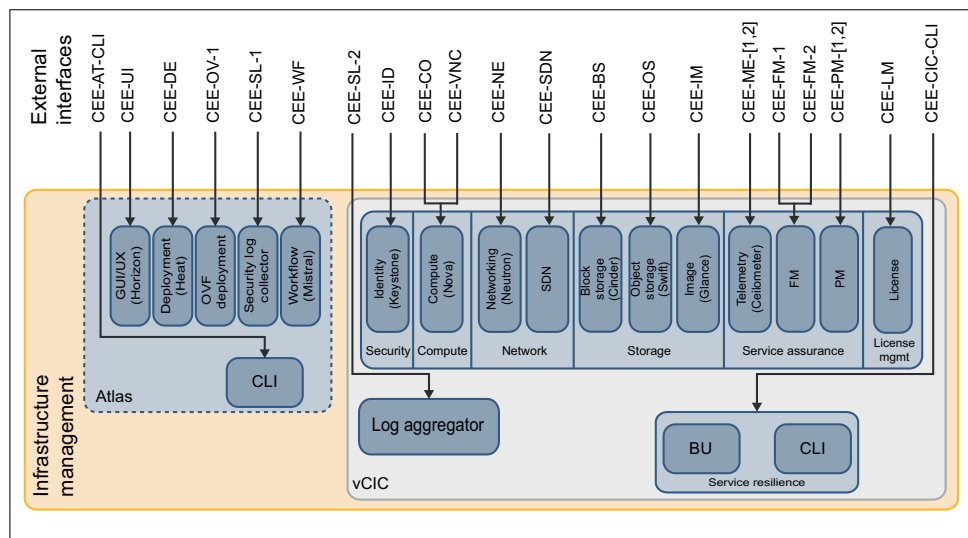


Figure 1 Security Protocols and Interfaces in CEE

### 2.1 Interfaces

External interfaces, including the OpenStack standard APIs and OpenStack REST APIs extended by Ericsson, are listed in Table 1.



Table 1 External Interfaces

Interface Type	Interface Name	Description
Atlas external interface	CEE-AT-CLI	[OpenSSH] Secure Shell (SSH) server providing a CLI and Secure File Transfer Protocol (SFTP) capabilities
	CEE-UI	[Ericsson] Hypertext Transfer Protocol (HTTP) GUI for the management of CEE
	CEE-DE	[OpenStack] Heat REST APIs for orchestrating application installation using the Heat engine. Refer to the section OpenStack Orchestration API v1 in <a href="#">OpenStack API Complete Reference</a> for details.
	CEE-OV-1	[Ericsson] Interface provided by the Open Virtualization Format (OVF) to Heat Orchestration Template (HOT) translation service. For more information, refer to the Distributed Management Task Force (DMTF) document <a href="#">Open Virtualization Format Specification</a> , Reference [6], and OpenStack Heat.
	CEE-SL-1	[Ericsson] Service used to send security-related logs to external Security Information and Event Manager (SIEM) systems
	CEE-WF	[OpenStack] Mistral is a workflow service that consists of a set of tasks and task relations. This workflow can be uploaded to Mistral so that it takes care of state management, correct execution order, parallelism, synchronization and high availability.



Interface Type	Interface Name	Description
vCIC external interface	CEE-SL-2	[OpenStack] If configured, logs are forwarded from both vCIC and compute host to an external log server
	CEE-ID	[OpenStack] Identity service (Keystone) security service used for authentications of all externally initiated calls
	CEE-CO	[OpenStack] Compute service (Nova) interface towards the CEE infrastructure for VM management
	CEE-VNC	[OpenStack] Virtual Network Control (VNC) HTTP proxy
	CEE-NE	[OpenStack] Networking service (Neutron) providing networking control, including both L2 and L3
	CEE-SDN	[Ericsson] Service used for software defined networking
	CEE-BS	[OpenStack] Block Storage service (Cinder), for creation and management of block storage volumes used by the tenant VMs
	CEE-OS	[OpenStack] Object Storage service (Swift) for CEE infrastructure storage only
	CEE-IM	[OpenStack] Image service (Glance) to upload, discover, register, and retrieve VM images and metadata definitions
	CEE-ME-1	[OpenStack] Telemetry service (Ceilometer) used for the collection of various counters throughout the system to provide the cloud provider and the tenants with statistics about the virtual infrastructure
	CEE-ME-2	[Ericsson] 3GPP compliant Extensible Markup Language (XML) API for data measurement
	CEE-FM-1	[Ericsson] Simple Network Management Protocol (SNMP) traps compliant with Ericsson Management Information Base (MIB) for Fault Management (FM)
	CEE-FM-2	[Ericsson] FM service providing a REST API for viewing the active alarms (faults) in the virtual and physical infrastructure
	CEE-PM-1	[Ericsson] SNMP providing Performance Management (PM) data in accordance with Ericsson PM MIB
	CEE-PM-2	[Ericsson] 3GPP compliant XML API for PM data
	CEE-LM	[Ericsson] License Management service used for communicating with the Network License Server (NeLS).
	CEE-CIC-CLI	[OpenSSH] SSH server providing CLI and SFTP capabilities





Internal interfaces are exposed to internal components, and do not have any external network connection.

## 2.2 Algorithms

Encryption algorithms are listed below.

Table 2 Encryption Algorithms

Protocol	Settings	Implementation
HTTPS	<ul style="list-style-type: none"> <li>• Key eXchange (KeX): ECDH</li> <li>• Authentication: RSA, ECDSA</li> <li>• Ciphers: AES128_GCM, AES256_GCM</li> <li>• MACs: SHA256, SHA384</li> </ul>	OpenSSL 1.0.1
SSH	<ul style="list-style-type: none"> <li>• KeX: curve25519-sha256@libssh.org, diffie-hellman-group-exchange-sha256</li> <li>• Ciphers: chacha20-poly1305@openssh.com, aes256-gcm@openssh.com, aes128-gcm@openssh.com, aes256-ctr, aes192-ctr, aes128-ctr</li> <li>• MACs: hmac-sha2-512-etm@openssh.com, hmac-sha2-256-etm@openssh.com, umac-128-etm@openssh.com, hmac-sha2-512, hmac-sha2-256, umac-128@openssh.com</li> </ul>	OpenSSH 6.4p

## 2.3 Protocols and Encryption

The following protocols are used in CEE:

- SSH2 (OpenSSH 6.4p): used for Atlas and vCIC CLIs (CEE-AT-CLI, CEE-CIC-CLI)
- SNMPv2: used for fault management (CEE-FM-1)
- RELP: used for log collection (CEE-SL)
- TCP: used for external logging
- HTTPS (HTTP over TLSv1.2; where TLS is implemented by OpenSSL 1.0.1): used for all other communication



- Network File System (NFS): used for the `cinder-backup` service
- TLS: used for license management

**Note:** Communication using LDAP, SNMP, NFS and RELP protocols is not encrypted in CEE.

For more information about RELP encryption, refer to section [SBI and SIEM Configuration in Audit and Security Logging](#).

The NFS protocol is recommended to be used only together with Kerberos v5 network authentication, which provides secure authentication and can be used for data integrity and encryption of the NFS traffic. However, this CEE release does not support Kerberos, thus CEE nodes cannot communicate with external Kerberos servers. For this reason, secure communication between the CEE region and external storage back ends (for example, NFS) requires system integration (SI) activity and is outside the scope of this document. Using NFSv3 (or NFSv4 without data encryption) is not recommended unless the communication channel is secured. In CEE, volumes are not encrypted. Encryption of the transferred data is the responsibility of the user.



### 3 Identity and Access Management

The purpose of the CEE Identity and Access Management (IdAM) tool 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 2.

**Note:** ScaleIO administrator users are not managed by IdAM. For more information, refer to the Dell EMC ScaleIO Version 2.x Security Configuration Guide.

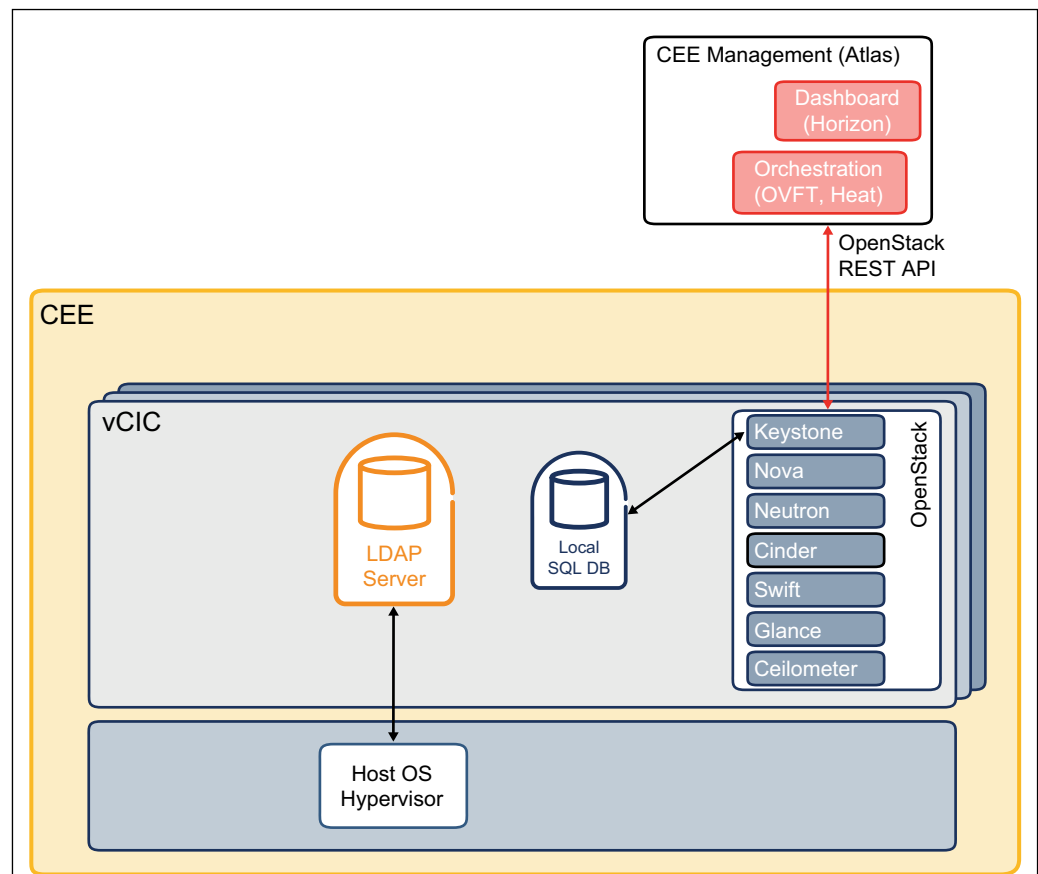


Figure 2 Identity and Access Management in CEE

#### Managed Areas

CEE IdAM can be used to manage the following:

- Users, see Section 3.1 on page 8
- LDAP groups, see Section 3.2 on page 10



- Passwords, see Section 3.3 on page 11
- Password policies, see Section 3.4 on page 21
- Privileged access, see Section 3.5 on page 21

## Configuration

CEE IdAM 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 the `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 10 on page 47.

For more information about IdAM configuration, refer to the [Configuration File Guide](#).

For more information about the CEE IdAM tool, refer to the [Infrastructure Administrator Management Guide](#).

For a functional description of IdAM components, refer to [CEE Technical Description](#).

## 3.1 Main User Types

The CEE IdAM tool differentiates between the following user types:

- Cloud Infrastructure administrators, see Section 3.1.1 on page 9
- Local administrators, see Section 3.1.2 on page 9

**Note:** Extreme switches do not support the Lightweight Directory Access Protocol (LDAP), so local users are used for administrative purposes.

CSC users are not integrated with IdAM. For more information about these users, refer to the below Software Defined Networking (SDN) documents:

- [Security User Guide, Reference \[3\]](#)
- [Cloud SDN Hardening Guideline, Reference \[2\]](#)



OpenStack users are managed by default Keystone and Dashboard operations, not by the CEE IdAM tool, see Section 3.1.3 on page 9.

### 3.1.1 Cloud Infrastructure Administrators

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

**Note:** Linux users and network device users (Extreme switches) are considered to be infrastructure users.

The cloud infrastructure administrator accounts are stored on a LDAP server that acts as a centralized IdAM repository for CEE. It supports the provisioning and authentication for `ceedadm`, 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.

### 3.1.2 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.

On CEE nodes `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 vCIC to all other nodes. For more information about sudo user groups, see Section 3.5 on page 21.

On vCICs `ceebackup` user is created for backup and restore, and `ceecore` for crash and core management.

#### Predefined Local Administrators

<b>atlasadm</b>	The initial system user <code>atlasadm</code> with sudo rights is created during the prehardening. The password of the <code>atlasadm</code> user is set as part of the installation procedure. For more information refer to the Atlas documentation.
<b>ceebackup</b>	This administrator is used for backup and restore processes. <code>ceebackup</code> is only used on the vCICs.
<b>ceecore</b>	This administrator is used for crash and core management. <code>ceecore</code> is only used on the vCICs.
<b>cmha</b>	This is the administrator used by the CM-HA component.



### 3.1.3 Manage OpenStack Cloud Users

OpenStack users are managed by the default Keystone and dashboard operations.

**Note:** OpenStack services (apart from Cinder) are only configured with internal management VIP addresses. Therefore, Keystone returns the internal OS\_AUTH\_URL address in case of external authentication requests.

OpenStack **administrators** (openstack-admin) are consumers of CEE resources exposed through OpenStack services. OpenStack administrators manage OpenStack domains, tenants (projects), users, roles, services, and images. After installation, the identity admin is automatically created and is a member of this group. Keystone acts as an authentication server for openstack-admin, using a local SQL database in CEE as a back end for the identities.

OpenStack **users** are able to provision their own resources within the limits set by the openstack-admin.

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

For more information about OpenStack cloud users, refer to the [OpenStack Identity API](#) and the [OpenStack Administrator Guide](#).

### 3.1.4 ScaleIO User Management

ScaleIO user management is described in section [ScaleIO Access Control](#) in the [System Hardening Guideline](#).

### 3.1.5 BSP User Management

BSP user management is described in [BSP User Management, Reference \[1\]](#).

### 3.1.6 NeLS User Management

Network License Server (NeLS) user management is described in the [System Hardening Guideline](#).

## 3.2 LDAP Groups

Table 3 shows the predefined LDAP groups. These groups are automatically created during the installation.

**Note:** For more information about CSC users, refer to the below SDN documents:

- [Security User Guide, Reference \[3\]](#)
- [Cloud SDN Hardening Guideline, Reference \[2\]](#)



Table 3 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
27000	sudo	This is the default system sudo group. It prompts users for password when executing a <b>sudo</b> command.
27001	ceesudo	Members of the this group are allowed to issue <b>sudo</b> commands without being prompted for the password.
27002	ceestatus	The members of this group are allowed to query <b>crm</b> status with <b>sudo</b> , without being prompted for a password.
27003	ceeuseradmin	The members of this group are allowed to execute <b>sudo cee-idam</b> commands without being prompted for a password.

## 3.3 Passwords

### 3.3.1 Change Password for root

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 vFuel node. The vFuel 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.

**Note:** The password of local users can remain unchanged on nodes which are offline during the password change.

The root password in all deployed CEE nodes can be changed using the following methods:

#### Using **passwd**

For setting the root password locally on vFuel, the **passwd** CLI command can also be used.

If the **passwd** command is used, the root password in vFuel does not propagate to other nodes and so must be changed manually for each node.



### Using idamsetup

If idamsetup is used, the root password is set for each newly deployed node.

Passwordless sudo privileges are required, see Section 11.2 on page 48.

Do the following on vFuel:

1. Create a new password that fulfills the strong password conditions described in the [System Hardening Guideline](#)
2. Write the new password to a file set with restricted permissions so that it is not readable to other users (for example, 0600)
3. Change the password:

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

where <credentials\_file> is the name of the new password file.

**Note:** The direct inclusion of the password in the command (`idamsetup -u root -p <password>`) is not recommended. For more information, see Section 11.2 on page 48

### 3.3.2 Change Credentials for Predefined Users

Credentials for predefined users can be changed using the following commands:

- `passwd`
- `idamsetup`

The command `passwd` has to be used to change the password of `ceeadm` and additional accounts created with the `cee-idam` tool. For more information on `passwd`, see Section 11.1 on page 48.

Other passwords and SSH keys of local predefined users in all deployed CEE nodes including the Fuel system can be changed using the `idamsetup` script in the vFuel node. For more information on `idamsetup`, see Section 11.2 on page 48.

Use `idamsetup` to manage the SSH key and passwords of the following predefined users:

- `ceeadm`, see Section 3.3.2.4 on page 13
- `ceebakup`, see Section 3.3.2.1 on page 12
- `ceecore` Section 3.3.2.2 on page 13
- `cmha` Section 3.3.2.3 on page 13





### 3.3.2.1 Changing SSH Keypair and Password for cebackup

This procedure changes the password of the cebackup user on vFuel and on the vCICs. Also, a new SSH keypair is created. The private key is distributed to the vCICs, and the public key is installed on all nodes of the region.

Do the following on vFuel:

1. Create a new password that fulfills the strong password conditions described in the [System Hardening Guideline](#)
2. Write the new password to a file set with restricted permissions so that it is not readable to other users (for example, 0600)
3. Execute the following command:

```
idamsetup -u cebackup -r root -c <credentials_file>
```

where <credentials\_file> is the name of the new password file.

### 3.3.2.2 Changing SSH Keypair for ceecore

This procedure creates a new SSH keypair for the cebackup user. The private key is distributed to the vCICs, and the public key is installed on all nodes of the region.

Passwordless sudo privileges are required, see Section 11.2 on page 48.

Execute the following command on vFuel:

```
idamsetup -u ceecore -r root
```

### 3.3.2.3 Changing SSH Keypair for cmha

This procedure creates a new SSH keypair for the cmha user. The private key is distributed to the vCICs, and the public key is installed on all nodes of the region.

Passwordless sudo privileges are required, see Section 11.2 on page 48.

Execute the following command on vFuel:

```
idamsetup -u cmha -r root
```

### 3.3.2.4 Changing SSH Keypair for ceeadm

This procedure creates a new SSH keypair for the cebackup user. The private key is distributed to the vCICs, and the public key is installed on all nodes of the region.

Passwordless sudo privileges are required, see Section 11.2 on page 48.

Execute the following command on vFuel:

```
idamsetup -u ceeadm -r root
```



### 3.3.3 Change Password for OpenStack Administrator

OpenStack identity (Keystone) is deployed in CEE as two separate instances, and both have their own admin users:

<b>vFuel admin</b>	User admin on vFuel, defined in the Keystone database running on vFuel.
<b>Cloud admin</b>	User admin on vCICs, defined in the Keystone database running on vCICs.

For detailed information on passwords refer to sections [Initial System and User Accounts](#) and [Strong Password Conditions in the System Hardening Guideline](#).

#### 3.3.3.1 Change vFuel Admin Password

To change the password of the vFuel admin:

1. Log on to the vFuel node and change the admin password:

```
fuel user change-password
```

2. Update the `/etc/fuel/astute.yaml` by changing `FUEL_ACCESS.password`:

```
"FUEL_ACCESS":  
  "password": "admin"  
  "user": "admin"
```

3. Update the tag `OS_PASSWORD` in `/root/.config/fuel/fuel_client.yaml` using a suitable editor, for example, vi:

```
OS_PASSWORD: "<new_password>"
```

Example:

```
# cat /root/.config/fuel/fuel_client.yaml  
  
SERVER_ADDRESS: "192.168.0.11"  
SERVER_PORT: "8000"  
OS_USERNAME: "admin"  
OS_PASSWORD: "admin"  
OS_TENANT_NAME: "admin"  
KEYSTONE_PORT: "5000"
```

#### 3.3.3.2 Change Cloud Admin Password

To change the password of the cloud (vCIC) admin:

1. Log on to the vFuel node and check the number of environments that are defined, using the command `fuel env`.



If there are multiple environments, note down the relevant environment ID (<environment\_number>).

**Note:** As vFuel manages one CEE deployment, the <environment\_number> value is set to 1 in most deployments.

2. Print a list of the current environment variables for the relevant environment:

```
fuel env --env <environment_number>⇒
--attributes --download
```

Example:

```
fuel env --env 1 --attributes --download
```

3. Update ./cluster\_<environment\_number>/attributes.yaml: change the cloud admin password in the editable.access.password field.

editable.access.password.value is used to describe the actual key in the YAML hierarchy, as shown below.

**Note:** Use single quotation marks, in the format '<password>', to allow special characters in the password.

```
./cluster_1/attributes.yaml
```

```
editable:
  access:
    email:
      description: Email address for Administrator
      label: Email
      regex:
        error: Invalid email
        source: ^\S+@\S+$
      type: text
      value: admin@localhost
      weight: 40
    metadata:
      group: general
      label: OpenStack Access
      weight: 10
    password:
      description: Password for Administrator
      label: Password
      regex:
        error: Empty password
        source: \S
      type: password
      value: 'admin'
      weight: 20
```



4. Execute the below command to upload the attributes:

```
fuel env --env <environment_number>⇒  
--attributes --upload
```

5. Propagate the change to vCICs manually:

- a. Log on to one of the vCICs as root user:

```
ssh root@cic-<x>
```

- b. Source the environment file:

```
source openrc
```

- c. Update the password in the vCIC identity database by using one of the following options:

- In Keystone, use the following command:

```
keystone user-password-update ⇒  
--pass '<new_password>' admin
```

Similar warnings in printout can be ignored:



```

/usr/lib/python2.7/site-packages/keystoneclient/shell.py:64: DeprecationWarning: The keystone CLI ⇒
is deprecated in favor of python-openstackclient. For a Python library, continue using ⇒
python-keystoneclient.

'python-keystoneclient.', DeprecationWarning)

/usr/lib/python2.7/site-packages/keystoneclient/v2_0/client.py:145: DeprecationWarning: Constructing ⇒
an instance of the keystoneclient.v2_0.client.Client class without a session is deprecated as of the ⇒
1.7.0 release and may be removed in the 2.0.0 release.

'the 2.0.0 release.', DeprecationWarning)

/usr/lib/python2.7/site-packages/keystoneclient/v2_0/client.py:147: DeprecationWarning: Using the ⇒
'tenant_name' argument is deprecated in version '1.7.0' and will be removed in version '2.0.0', ⇒
please use the 'project_name' argument instead

super(Client, self).__init__(**kwargs)

/usr/lib/python2.7/site-packages/debtcollector/renames.py:45: DeprecationWarning: Using the ⇒
'tenant_id' argument is deprecated in version '1.7.0' and will be removed in version '2.0.0', ⇒
please use the 'project_id' argument instead

return f(*args, **kwargs)

/usr/lib/python2.7/site-packages/keystoneclient/httpclient.py:371: DeprecationWarning: ⇒
Constructing an HTTPClient instance without using a session is deprecated as of the 1.7.0 ⇒
release and may be removed in the 2.0.0 release.

'the 2.0.0 release.', DeprecationWarning)

/usr/lib/python2.7/site-packages/keystoneclient/session.py:145: DeprecationWarning: ⇒
keystoneclient.session.Session is deprecated as of the 2.1.0 release in favor of ⇒
keystoneauth1.session.Session. It will be removed in future releases.

DeprecationWarning)

/usr/lib/python2.7/site-packages/keystoneclient/auth/identity/base.py:56: DeprecationWarning: ⇒
keystoneclient auth plugins are deprecated as of the 2.1.0 release in favor of keystoneauth1 ⇒
plugins. They will be removed in future releases.

'in future releases.', DeprecationWarning)

```

- In the OpenStack CLI use the following command:

```

openstack user set --password ⇒
'<new_password>' admin

```

The change is done even if a similar output is printed: The request you have made requires authentication. (HTTP 401) (Request-ID: req-d4bd8529-bea3-48ec-94cc-06aaad5b00e7).

- Use the Atlas web UI, as described in the OpenStack Horizon documentation, Reference [5], or use the Atlas CLI as described in section Change password for user in the [OpenStack Identity API in CEE](#).

**Note:** Perform the below steps after every update or redeployment, because manual changes are overwritten during the deployment procedure.

- d. In all vCICs, edit /root/openrc.



**Note:** To allow special characters in the password, use single quotation marks, in the format '<password>'.

- e. In all vCICs, change the `admin_password` in the file `/etc/pmapi/pmapi.conf`.
  - f. In one of the vCICs, restart PMAPI with the below command:  
  

```
crm resource restart clone_p_pmapi
```
  - g. Update the password in `/etc/atlasrc`.
6. On Atlas, update `/home/atlasadm/openrc`.

If the file is owned by `root`, change the owner to `atlasadm` and `0600`.

### 3.3.4 Change Password for CSC Administrator

To change the `cscadm` password, perform the following steps:

1. Change the `cscadm` by following the procedure described in section Changing CSC Interfaces Users Passwords of the Cloud SDN Hardening Guideline, Reference [2].
2. Continue with Section 3.3.4.1 on page 18 to propagate the CSC password in the CEE region.

#### 3.3.4.1 Propagate CSC Password in CEE

To propagate the changed `cscadm` password in CEE, perform the following steps:

1. Update the `cscadm` user password in the `ericsson_sdnc` Fuel plugin setting in `/mnt/cee_config/config.yaml`:

```
-
  name: ericsson_sdnc
  config_attributes:
    as_num: '100'
    odl_username: 'cscadm'
    odl_password: <NEW_PASSWORD>
```

2. Update the `cscadm` user password under `sdnc_admin_password` in `/mnt/cee_config/config.yaml`:

```
sdn:
  sdnc_admin_username: cscadm
  sdnc_admin_password: <NEW_PASSWORD>
```

3. Update the `cscadm` user password in Atlas on each vCIC:
  - a. Log on to the vCIC.



- b. Update the cscadm user password in Atlas /etc/atlasrc:

```
readonly SDNC_USERNAME=cscadm
readonly SDNC_PASSWORD=<new_password>
```

4. Update the cscadm user password in /opt/sdnc/opendaylight/karaf\_featureInstall.sh on each vCIC:

- a. Log on to the vCIC.

- b. Update the cscadm user password in the /opt/sdnc/opendaylight/karaf\_featureInstall.sh file:

```
result=$(sshpass -p '<new_password>' ssh -o ⇒
UserKnownHostsFile=/dev/null -o ⇒
StrictHostKeyChecking=no -p 8101 ⇒
$USER_ODL@localhost $1)
```

5. Validate the new configuration in vFuel:

- a. Log on to vFuel.

- b. Retrieve the environment ID from the printout of the following command:

```
fuel env
```

- c. Apply the new configuration:

```
apply_settings /var/lib/ericsson/pre_deploy/ ⇒  
/mnt/cee_config/config.yaml <env_id> ⇒  
update /etc/cee/eri_deployment_tasks.yaml ⇒  
/etc/cee/repos.yaml
```

- d. Update the deployment files with the new Fuel plugin information:

```
pre_deploy /var/lib/ericsson/pre_deploy/ ⇒  
/mnt/cee_config/config.yaml <env_id> ⇒  
/etc/cee/openstack_config/
```

- e. Run the fuel node task for every node in the CEE region:

```
fuel node --node <node_ids> ⇒  
--tasks upload_configuration
```

The node IDs are acquired from the printout of the fuel node command.

6. Change the password in the Neutron configuration on each vCIC:

- a. Log on to the vCIC.



- b. Change the password in the `/etc/neutron/plugins/ml2/ml2_conf.ini` file:

```
[ml2_odl]  
password = <new_password>
```

7. Restart the Neutron server:

```
crm resource restart clone_neutron-server
```

8. If the SDN counters (`sdn_counters`) are **disabled** in the `ericsson_openstack_config` section in `config.yaml`, skip to Step 11.

If the SDN counters are **enabled**, continue with the next step to update Ceilometer.

9. Update the CSC password in Ceilometer on all vCICs:

- a. Log on to a vCIC.

- b. Update the `/etc/ceilometer/pipeline.yaml` file:

```
ericsson.opendaylight://192.168.2.28:8383/controller/statistics?auth=basic&user=cscadm&password=<new_password>&scheme=http
```

- c. Restart the `ceilometer-agent-central` service:

```
crm resource restart p_ceilometer-agent-central
```

- d. Restart the Ceilometer services:

```
service ceilometer-agent-notification restart  
service ceilometer-api restart  
service ceilometer-collector restart  
service ceilometer-polling restart
```

10. Update Ceilometer on all compute hosts:

- a. Log on to a compute host.

- b. Update the `/etc/ceilometer/pipeline.yaml` file:

```
ericsson.opendaylight://192.168.2.28:8383/controller/statistics?auth=basic&user=cscadm&password=<new_password>&scheme=http
```

- c. Restart the `ceilometer-polling` service:

```
service ceilometer-polling restart
```





11. The procedure is complete.

### 3.3.5 Distribute SSH-keys for Personal Accounts

Individual users do not have any individual SSH-keys generated. Each user must create their own SSH-key pairs. SSH public keys are fetched from LDAP. The `cee-idam` tool can be used to store the keys in LDAP.

## 3.4 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 the [Infrastructure Administrator Management Guide](#).

## 3.5 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.

Local and LDAP user groups are listed in Table 4.

Table 4 Local and LDAP User Groups

Location	Group Name	Description
Local groups <sup>(1)</sup>	ceebackup	Members of the this group are allowed to issue <code>sudo</code> commands without being prompted for the password.
	sheriff	Members of this group are allowed to access license configuration data and TLS certificates (including trusted CA certificate, client certificate and client private key).



Location	Group Name	Description
LDAP groups	ceestatus	Members of this group are allowed to query <code>crm status</code> with <code>sudo</code> , without being prompted for a password.
	ceesudo	Members of the this group are allowed to issue <code>sudo</code> commands without being prompted for the password.
	ceeuseradmin	Members of this group are allowed to execute <code>sudo cee-idam</code> commands without being prompted for a password.
	sudo	This is the default system <code>sudo</code> group. It prompts users for a password when executing a <code>sudo</code> command.

(1) In maintenance mode (MM) only local user groups can be used.

For information about how to manage `sudo` groups, refer to [Infrastructure Administrator Management Guide](#).



## 4 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).

### 4.1 Logging Service Architecture

The logging service architecture is shown in Figure 3.

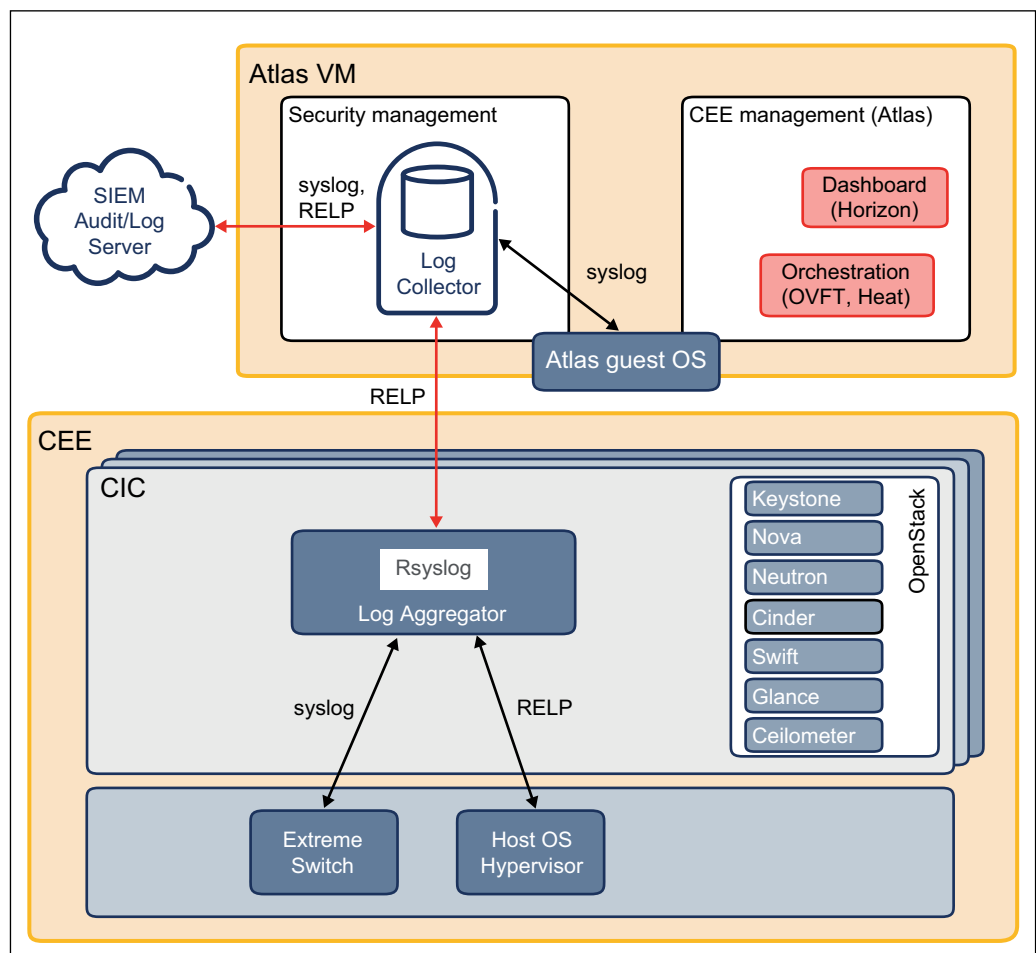


Figure 3 Logging Service Architecture

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:

- 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.

## 4.2

### 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 audit logging module of the `ericsson_logging` plugin. There is no API or CLI for changing the configuration, so when changes are needed, use the following procedure:

Update the `/var/www/nailgun/plugins/ericsson_logging-1.0/deployment_scripts/puppet/modules/ericsson_audit_logging/templates/auditd/audit.rules.erb` template file on the vFuel node. Execute the below command to apply the changes:

```
fuel node --node <node_ids> --tasks =>
eri_rsyslog_common eri=>
_rsyslog_configuration eri=>
_audit_logging_configuration --force
```

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

### 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.

## 4.3 Configure 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](#).



## 5 Network Security

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

The DC-FW is located outside CEE. For the connectivity and network description of the DC-FW refer to the [DC Firewall Hardening Guide](#) and [System Hardening Guideline](#).

For algorithms used in CEE, see Section 2 on page 2.

**Note:** These algorithms cannot be found in the `config.yaml` as they are not configurable.



## 6 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 and CSC endpoints through the northbound interface.

For settings, refer to [SW Installation in Multi-Server Deployment](#) or [SW Installation in Single Server Deployment](#), and the [Configuration File Guide](#).





## 7 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 information about the upgrade of Atlas software, refer to [Atlas SW Upgrade](#).

For more information about CEE software upgrade refer to [CEE Update and Rollback Guide](#).



## 8 Privacy

A variety of applications could be running on CEE processing the personal data of subscribers, however such data is not known, and cannot be managed by CEE directly. These applications that utilize CEE may affect subscriber privacy. Their impact on privacy is generally to be considered not under the control of CEE.

CEE provides security controls for applications in VMs that process personal data. It is the responsibility of each application to deploy those controls appropriately to protect subscribers personal data and mitigate any possible privacy impact.



## 9 Services, Ports, and Protocols

All open ports and services running on the CEE nodes, that is, vCICs, 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 DC-FW, 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 vCICs. 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:fe5: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

```

The nodes (for example compute, Cinder, vCIC nodes) are the first to be assigned IP addresses from the range, followed by the VIP addresses. As such, the VIP address allocation is site-specific, depending on the blade IP allocation.

### Reachable Services

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

The following services are reachable from the public network on a vCIC:



Table 5 Services Available on vCICs

Network or Interface	Protocol	Port	Process Name
Services listening on the vip_public address	TCP	6080	haproxy
	TCP	9696	haproxy
	TCP	8774	haproxy
	TCP	8776	haproxy
	TCP	5000	haproxy
	TCP	8777	haproxy
	TCP	8042	haproxy
	TCP	9292	haproxy
	TCP	80	haproxy
	TCP	8080	haproxy
	TCP	8052	haproxy
	TCP	9494	haproxy
	TCP	443	haproxy
	TCP	7676	haproxy
	TCP	35357	haproxy
	UDP	30165	python



Network or Interface	Protocol	Port	Process Name
Services available on the internal network, listening on the vip__management address	TCP	9696	haproxy
	TCP	10049	haproxy
	TCP	8514	haproxy
	TCP	20514	haproxy
	TCP	8997	haproxy
	TCP	389	haproxy
	TCP	8774	haproxy
	TCP	9191	haproxy
	TCP	8775	haproxy
	TCP	8776	haproxy
	TCP	5000	haproxy
	TCP	8777	haproxy
	TCP	8042	haproxy
	TCP	3306	haproxy
	TCP	9292	haproxy
	TCP	80	haproxy
	TCP	8080	haproxy
	TCP	10000	haproxy
	TCP	8052	haproxy
	TCP	8054	haproxy
	TCP	9494	haproxy
	TCP	443	haproxy
	TCP	7676	haproxy
	TCP	35357	haproxy
	UDP	162	snmptrapd
Service available on the vip__zbx_vip_mgmt address	TCP	10051	zabbix_server
Services available on the public address	-	-	Currently there are no services listening on this address.



Network or Interface	Protocol	Port	Process Name
Services bound to the wildcard (0.0.0.0) IPv4 address <sup>(1)</sup>	TCP	22	sshd
	TCP	20514	rsyslogd
Services available on localhost (127.0.0.1)	TCP	27017	mongod
	TCP	9003	php-fpm.conf
	TCP	80	apache2
	TCP	15672	beam.smp
	TCP	25	master
	TCP	443	apache2
	TCP	389	slapd
	TCP	8774	python
	UDP	514	rsyslogd
	UDP	123	ntpd
	UDP	11211	memcached





Network or Interface	Protocol	Port	Process Name
Services available on the internal management interface (br-mgmt)	TCP	41055	beam.smp
	TCP	9191	python2.7
	TCP	5000	apache2
	TCP	8776	python2.7
	TCP	49000	xinetd
	TCP	8777	python2.7
	TCP	27017	mongod
	TCP	873	xinetd
	TCP	5673	beam.smp
	TCP	8042	python2.7
	TCP	11211	memcached
	TCP	3307	mysqld
	TCP	9292	python2.7
	TCP	80	apache2
	TCP	8052	python
	TCP	9494	python2.7
	TCP	8054	python
	TCP	4567	mysqld
	TCP	443	apache2
	TCP	7676	python
	TCP	35357	apache2
	TCP	6080	python
	TCP	8514	rsyslogd
	TCP	10050	zabbix_agentd
	TCP	389	slapd
	TCP	8997	python
	UDP	514	rsyslogd
	UDP	4952	python2.7
	UDP	5405	corosync
	UDP	54738	corosync
	UDP	38874	corosync
	UDP	55270	corosync
	UDP	8514	rsyslogd
	UDP	10514	rsyslogd
	UDP	11211	memcached
	UDP	123	ntpd



Network or Interface	Protocol	Port	Process Name
Services available on the Swift or Storage network	TCP	49001	xinetd
	TCP	873	xinetd
	TCP	8080	python
	TCP	6000	python
	TCP	6001	python
	TCP	6002	python
Services available using IPv6	TCP6	4369	epmd
	TCP6	22	sshd
	TCP6	25	master
	TCP6	20514	rsyslogd

(1) The Linux networking stack allows accepting IPv4 connections on IPv6 sockets, so the presence of an IPv6 listener implies IPv4 connectivity.

The following services are reachable from the public network on a compute host:

Table 6 Services Available on Compute Hosts

Network or Interface	Protocol	Port	Process Name
Services bound to the wildcard (0.0.0.0) IPv4 address <sup>(1)</sup>	TCP	22	sshd
	TCP	16509	libvirtd
Services available on localhost (127.0.0.1)	TCP	5900	qemu-system-x
	TCP	25	master
	UDP	123	ntpd
Services available on the internal management interface (br-mgmt)	TCP	4480	ndevalarm
	UDP	123	ntpd
Services available using IPv6	TCP6	22	sshd
	TCP6	25	master
	TCP6	16509	libvirtd

(1) The Linux networking stack allows accepting IPv4 connections on IPv6 sockets, so the presence of an IPv6 listener implies IPv4 connectivity.

The following services are reachable from the public network on vFuel:



Table 7 Services Available on vFuel

Network or Interface	Protocol	Port	Process Name
Services available on localhost (127.0.0.1)	TCP	15672	beam.smp
	TCP	25	master
	TCP	25151	python2
	UDP	123	ntpd
Services bound to the eth0 interface	TCP	5672	beam.smp
	TCP	873	xinetd
	TCP	53	dnsmasq
	UDP	123	ntpd
	UDP	53	dnsmasq



Network or Interface	Protocol	Port	Process Name
Services bound to other addresses	TCP	5000	python2
	TCP	8777	python
	TCP	8080	nginx: master
	TCP	80	httpd
	TCP	4369	epmd
	TCP	22	sshd
	TCP	5432	postgres
	TCP	8443	nginx: master
	TCP	443	httpd
	TCP	35357	python2
	TCP	41055	beam.smp
	TCP	8000	nginx: master
	TCP	8001	uwsgi
	TCP	514	rsyslogd
	TCP6	61613	beam.smp
	TCP6	25	master
	TCP6	514	rsyslogd
	UDP	67	dnsmasq
	UDP	69	xinetd
	UDP	123	ntpd
	UDP	123	ntpd
	UDP	123	ntpd
	UDP	514	rsyslogd
	UDP6	123	ntpd
	UDP6	514	rsyslogd

The following services are reachable from the public network on Atlas:



Table 8 Services Available on Atlas

Network or Interface	Protocol	Port	Process Name
Services available from the Atlas NBI	TCP	8000	haproxy
	TCP	8004	haproxy
	TCP	8888	haproxy
	UDP	123	ntpd
Services available from the Atlas SBI	TCP	8000	haproxy
	TCP	8004	haproxy
	TCP	8888	haproxy
	UDP	123	ntpd
Services bound to the wildcard (0.0.0.0) IPv4 address <sup>(1)</sup>	TCP	8989	apache2
	TCP	20514	rsyslogd
	TCP	8003	python
	TCP	80	apache2
	TCP	4369	epmd
	TCP	22	sshd
	TCP	443	apache2
	UDP	68	dhclient
	UDP	123	ntpd
Services available on localhost (127.0.0.1)	TCP	8000	python
	TCP	8004	python
	TCP	5672	beam.smp
	TCP	25672	beam.smp
	TCP	3306	mysqld
	TCP	11211	memcached
	TCP	15671	beam.smp
	TCP	8888	python
	UDP	11211	memcached
	UDP	123	ntpd



Network or Interface	Protocol	Port	Process Name
Services available using IPv6	TCP6	22	sshd
	TCP6	20514	rsyslogd
	TCP6	4369	epmd
	UDP6	123	ntpd

(1) The Linux networking stack allows accepting IPv4 connections on IPv6 sockets, so the presence of an IPv6 listener implies IPv4 connectivity.

The following services are reachable from the public network on ScaleIO nodes:

Table 9 Services Available on ScaleIO

Network or Interface	Protocol	Port	Process Name
ScaleIO GW management interfaces	TCP	6611	mdm
	TCP	7072	sds
	TCP	9011	mdm
	TCP	9099	lia
	TCP	25620	mdm
	TCP	25640	sds

For the mapping between port number and service name, refer to the [System Hardening Guideline](#).

### TCP Ports Used

The list of TCP ports used are shown in Table 10.

**Note:** For the list of TCP ports in SDN, refer to the following SDN documents:

- Section Interfaces, Ports, and Protocols in the Security User Guide,
- Section Port Filtering with IPv4 Tables in the Cloud SDN Hardening Guideline, Reference [2]

Table 10 TCP Ports in CEE

22	Used for SSH connection
25	SMTP
53	DNS
80	<ul style="list-style-type: none"><li>• HTTP</li><li>• apache2 (vCIC, Atlas) to reach Zabbix and Atlas web UI<sup>(1)</sup></li></ul>



389	LDAP port (vCIC)
443	<ul style="list-style-type: none"> <li>• HTTPS</li> <li>• apache2 (vCIC, Atlas) to reach Zabbix and Atlas web UI.</li> </ul>
514	syslog (vFuel)
873	rsync port (vCIC, vFuel)
3306	MySQL (vCIC, Atlas)
3307	MySQL (vCIC)
4369	Erlang port mapper daemon (vCIC, Atlas, vFuel)
4480	ndevalarm (compute)
4567	MySQL WSREP (vCIC)
5000	OpenStack Identity / Keystone API (vCIC, vFuel)
5432	PostgreSQL (vFuel)
5672	amqp / RabbitMQ (Atlas, vFuel)
5673	RabbitMQ (vCIC)
5900-15899	VNC console (compute)
6000	OpenStack Object / Swift server (vCIC)
6001	OpenStack Object / Swift Container (vCIC)
6002	OpenStack Object / Swift Account (vCIC)
6080	OpenStack NoVNC proxy (vCIC)
6611	MDM (ScaleIO)
7072	SDS (ScaleIO)
7676	CEE PMAPI (vCIC)
8000	OpenStack Heat (Atlas) Nailgun / nginx (vFuel)
8001	Nailgun / uwsgi (vFuel)
8003	OpenStack Heat (Atlas)
8004	OpenStack Heat (Atlas)
8042	OpenStack AODH
8052	CEE Watchmen API (vCIC)
8054	Zabbix endpoint
8080	<ul style="list-style-type: none"> <li>• OpenStack Object / Swift Proxy Server</li> <li>• Nailgun / nginx (vFuel)</li> </ul>
8443	Cobbler / nginx (vFuel)



8514	CEE log receiver port (vCIC, ScaleIO nodes)
8774	OpenStack Compute (Nova) API
8775	OpenStack Compute (Nova) Metadata API
8776	OpenStack Block (Cinder) API
8777	<ul style="list-style-type: none"> <li>• OpenStack Metering (Ceilometer) API</li> <li>• OSTF server (vFuel)</li> </ul>
8888	<ul style="list-style-type: none"> <li>• OpenStack OVFT on Atlas</li> <li>• Reverse HTTP proxy on vCICs</li> </ul>
8989	OpenStack Mistral (Atlas)
8997	CEE CMHA API (vCIC)
9003	PHP-FPM
9011	MDM (ScaleIO)
9099	LIA (ScaleIO)
9191	OpenStack Image (Glance) Registry
9292	OpenStack Image (Glance) API
9494	OpenStack Image v3 (Glare) API
9696	OpenStack Neutron API (vCIC)
10000	haproxy statistic port (vCIC)
10049	Zabbix agent
10050	Zabbix agent
10051	Zabbix server
11211	memcached (vCIC, Atlas)
15671	RabbitMQ management port (Atlas)
15672	RabbitMQ (vCIC, vFuel)
16509	Libvirt (compute)
20000 + AMQP port (25672)	RabbitMQ
20514	CEE syslog port used for the audit trail (vCIC, Atlas)
25151	Cobbler (vFuel)
25620	MDM (ScaleIO)
25640	SDS (ScaleIO)
27017	MongoDB (vCIC)
35357	OpenStack Identity (vCIC, vFuel)





41055	RabbitMQ
49000	Mirantis OpenStack galeracheck
49001	Mirantis OpenStack swiftcheck
61613	RabbitMQ (vFuel)

(1) In apache and haproxy, clients are automatically redirected to HTTPS port 443.

## UDP Ports Used

The list of UDP ports used are shown in Table 11.

**Note:** Dynamic ports can change.

Table 11 UDP Ports in CEE

53	DNS (vFuel, vCIC)
67	dnsmasq (vFuel)
68	DHCP (Atlas), used for setting up IP addresses on tenant VMs
69	TFTP (vFuel)
123	NTP, used by ntpd for clock synchronization
162	SNMP trapd (vCIC)
514	CEE syslog receiver (all)
3780	conntrackd (vCIC)
4480	CEE ndevalarm (compute)
4952	OpenStack Metering (Ceilometer)
5405	Corosync (vCIC)
8514	CEE rsyslog relay (vCIC, ScaleIO)
10514	CEE syslog relay (vCIC)
11211	memcached (Atlas)
30165	CEE Watchmen
8361 (dynamic)	DHCP DDNS
34161 (dynamic)	Swift object replicator (vCIC)
42717 (dynamic)	Corosync (vCIC)
48189 (dynamic)	Corosync (vCIC)
47408 (dynamic)	CMHA (vCIC)



52400 (dynamic)	Corosync (vCIC)
54481 (dynamic)	Swift container replicator (vCIC)
56251 (dynamic)	Swift account replicator (vCIC)

10

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](#).

[illegible]



# Appendix

## 11 Command Descriptions

### 11.1 passwd

#### Syntax

**passwd** <username>

#### Description

The command **passwd** has to be used to change the password of **ceedm** and additional accounts created with the **cee-idam** tool

The password has to be changed both on vFuel and on one of the vCICs, as the password change does not propagate automatically.

#### Examples

The following is an example of the execution of the command on vFuel for changing the password of the **ceedm** user:

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

The following is an example of the execution of the command on vCIC for changing the password of the **ceedm** user:

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



## 11.2 idamsetup

### Syntax

```
idamsetup -u <username> [ -r <remote_user> ] [ -p <password> ]⇒
[ -c <credentials_file> ] [ -e <environment_id> ] [-v] [-f]
```

### Description

This command can be issued on vFuel.

This command requires root privileges, so it must be executed as a user with passwordless sudo privileges of vFuel and the remote nodes , or as root user if no other users exist.

---

---

### Attention!

Passing sensitive information such as passwords as command arguments can lead to information disclosure and is therefore not recommended, especially on multi-user systems. Any sensitive information included in the commands is visible in the history and the argument list.

---

---

### Optional Arguments

Parameter	Description
-U <username>	Username of the modified account
-r <remote_user>	Username of the user used for logging on to remote nodes. This user must have passwordless sudo privileges on the remote nodes.  Default value if unspecified: ceeadm
-p <password>	Password for the modified user. Can only be used for users that have passwords. <sup>(1)</sup>
-c <credentials_file>	If specified, idamsetup reads the password from a file.
-e <environment_id>	The execution of the command is limited to one environment. The argument identifies the region in which the command is executed, in multi-region deployments. <sup>(2)</sup>



Parameter	Description
-V -VV	Verbose mode, can be specified multiple times. <ul style="list-style-type: none"><li>• -V enables informational messages</li><li>• -VV enables debugging messages</li></ul>
-f	Force execution, even when not all nodes are online. This argument must only be used in recovery actions.

(1) Passing passwords as command arguments can lead to information disclosure and is therefore not recommended. The use of credentials files is recommended instead.

(2) Multi-region deployment is not possible in this CEE release.



## Reference List

### Ericsson Documentation

- [1] BSP User Management, 6/1553-APR 901 0549/1
- [2] Cloud SDN Hardening Guideline, 2/1553-AXD 101 08/6-V1
- [3] Security User Guide, 2/1553-HSD 101 048/3-V1

### 3PP Documentation

- [4] EMC Documentation web page, <https://mydocuments.emc.com/>
- [5] OpenStack Horizon documentation, <https://docs.openstack.org/horizon/pike/user/log-in.html#openstack-dashboard-settings-tab>

### Standards

- [6] Open Virtualization Format Specification, 2.1.0 2013-12-12, [http://dmf.org/sites/default/files/standards/documents/DSP0243\\_2.1.0.pdf](http://dmf.org/sites/default/files/standards/documents/DSP0243_2.1.0.pdf)