

System Hardening Guideline

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

1	Introduction	1
1.1	Purpose	1
1.2	Scope	1
1.3	Target Groups	2
1.4	Prerequisites	2
1.4.1	Required Competence	2
1.4.2	Documents	3
2	General	4
2.1	System Overview	4
2.2	Hardening Areas	4
2.3	Access Control	5
3	Hardening Activities	6
3.1	Hardening Before Installation and Integration	6
3.1.1	Initial System and User Accounts	6
3.1.2	Prehardened System Components	8
3.2	Hardening During Installation and Integration	10
3.2.1	Initial Administrator Credentials	10
3.2.2	DC-FW Configuration	11
3.2.3	Authenticate NTP Server	14
3.2.4	Change Legal Text Presented at Logon	14
3.2.5	ScaleIO Management Tools	14
3.2.6	Location of Logs	14
3.3	Product Security Maintenance After Installation and Integration	15
3.3.1	Manage Administrator Credentials	15
3.3.2	Change Certificates on vFuel	17
3.3.3	vCIC Host OS Hardening	17
3.3.4	Atlas User Management	18
3.3.5	vFuel User Management	18
3.3.6	GRUB User Management	18
3.3.7	Extreme Switch User Management	19
3.3.8	ScaleIO Access Control	19
3.3.9	NeLS Access Control	19
3.3.10	Managing TLS Certificates in CEE	19
3.3.11	CEE Infrastructure Network Hardening for SDN Tight Integration	20
4	Strong Password Conditions	22



Reference List

23



1 Introduction

This user guide contains general information about the hardening processes, and helps to understand the purpose of product hardening. The document gives an overview of the hardening activities that are performed during the product development, and defines hardening activities that need to be performed during and after the installation.

The first and one of the most important step of hardening is to understand the security risks threatening the system. Therefore these threats, the probability of them happening, and the impact on the Cloud Execution Environment (CEE) must be identified. Based of the likelihood and impact, the risk of the vulnerabilities are determined. If some risks are assessed as non-acceptable, controls must be applied to mitigate those risks. This document collects the available controls to mitigate the risk.

Attention!

Hardening is not an optional feature or function. Assessment of the security risks in an operational environment must be performed according to the ISO 27011 standard, refer to Section 4.2.4.2 of the ISO27011 documentation, Reference [4]. If the result of the assessment contains some acceptable risks, the corresponding control mitigating the non-important risk may not be applied, refer to Section 4.2.4.3 of the ISO27011 documentation, Reference [4]. The owner or the responsible of the CEE must assess the risks to have clear responsibility and accountability, refer to Section 6.1.1 of the ISO27011 documentation, Reference [4]. Use the [CEE Hardening Checklist](#) to collect the result of the assessment and based on that perform the required steps.

For more information on how to manage information security in telecommunications organizations, refer to ISO 27011, Reference [4].

1.1 Purpose

The purpose of this document is to describe the hardening procedures and available controls of CEE.

1.2 Scope

This user guide provides a high level overview of CEE security, enumerates the hardening areas, provides detailed background information about the required hardening steps and the commands to perform them.



ScaleIO, Extreme switches, Software Defined Networking (SDN), and the Data Center Firewall (DC-FW) are mentioned in the below sections for completeness, but their hardening procedures are out of the scope of this document.

1.3 Target Groups

This document is primarily intended to be used by the staff responsible for CEE. This includes operational personnel performing installing, updating, or maintaining activities. Furthermore, security administrators managing security and IT and Telecom (security) operational managers responsible for Information Security Management Systems (ISMS) according to section 6.1.1 in the ISO 27011 standard, Reference [4] and section 6.1.1 b) in ISO 27002 standard, Reference [3].

1.4 Prerequisites

This section states the prerequisites that have to be fulfilled.

1.4.1 Required Competence

The following sections describe the required competencies for operational personnel and decision makers.

1.4.1.1 Operational Personnel

It is required for operational personnel, performing the installing, updating, or maintaining activities to understand the security concepts before handling security. For that reason, the intended audience of the document must be skilled in security and have at least CISSP certificates or equivalent. Furthermore, deep domain knowledge on cloud and security is required, especially on those components on which the hardening steps are to be performed. The security topics are, for example, cryptography, secure protocols (IPSec, TLS, SSH, and so on), security architecture, security operations management, firewall configuration, key management, security log analysis, user management, web server security, certificate management, OpenStack, Linux, Lightweight Directory Access Protocol (LDAP) and Simple Network Management Protocol (SNMP).

1.4.1.2 Decision Makers

It is required for the decision makers, who identify operational risks and decide required controls, such as security administrators managing security and IT, and Telecom (security) operational managers responsible for ISMSs, that they understand the security concepts before taking responsibility and making decisions. At least CISSP, CISM, and ISO27001 lead auditor certificates or equivalent are required. Furthermore, deep domain knowledge on cloud and security is required, especially on those components on which the hardening steps are to be performed. The security topics are, for example, cryptography, secure protocols (IPSec, TLS, SSH, and so on), security architecture, security operations



management, firewall configuration, key management, security log analysis, user management, web server security, certificate management, OpenStack, Linux, LDAP and SNMP protocols.

1.4.2

Documents

Ensure that the following documents have been read:

- CEE Hardening Checklist
- Security User Guide
- Infrastructure Administrator Management Guide
- DC Firewall Hardening Guide



2 General

The following sections give a general overview of the system from a security point of view and define the main hardening areas.

2.1 System Overview

An overview of the security services is shown in Figure 1.

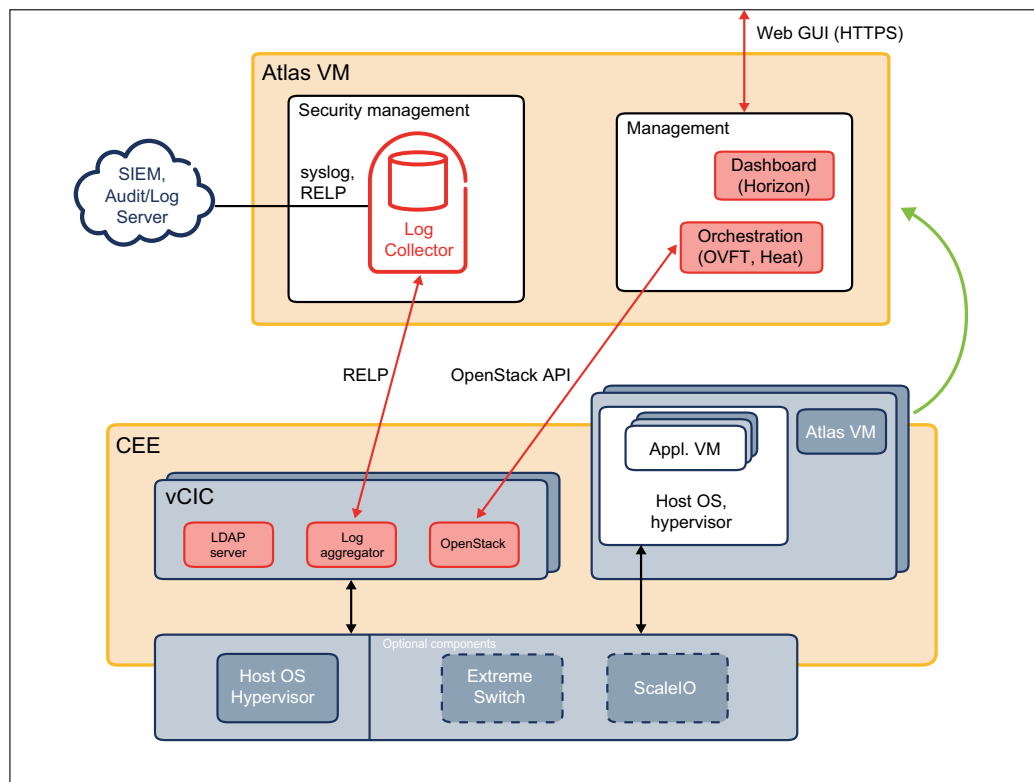


Figure 1 Current Security Solution

For an overview of the system, refer to CEE Technical Description.

For an overview of the DC-FW solution, refer to DC Firewall Hardening Guide.

2.2 Hardening Areas

The following hardening areas are defined:

**Identity and Access Management**

Credentials management includes the handling of infrastructure and OpenStack credentials, and the adherence to the password policies.

Prehardening of System Components

The prehardening of the system components ensures that only the required services are enabled on the Atlas management node, the compute hosts, the virtual Cloud Infrastructure Controller (vCIC) hosts, ScaleIO distributed storage, Extreme switches, and on the vFuel node.

Allowed Traffic Flows Through the DC Firewall between Security Domains

The configuration of the DC-FW is defined in a way to enable only the allowed traffic flows between the various Security Domains (SDs).

Certificate Management for the Northbound Interface

Managing the certificates for the northbound interface.

2.3

Access Control

AppArmor is a Linux Security Module (LSM) implementation used by default on Ubuntu hosts. It allows more granular access to resources than the traditional file-system Access Control Lists (ACLs). In CEE 6 the `libvirt-bin` AppArmor profile is updated on compute nodes to allow accessing hugepages, otherwise AppArmor configuration in CEE 6 is identical to Ubuntu 14.04 LTS.

The current AppArmor status can be checked with the command `aa-status`.



3 Hardening Activities

This section presents the various hardening activities that take place before, during, and after the installation and integration.

Note: If any of these hardening activities are not performed, the security of the system is degraded.

3.1 Hardening Before Installation and Integration

This section contains information about the hardening activities that are performed before the installation and integration of the system.

3.1.1 Initial System and User Accounts

The initial administrator and system account credentials that are created during the system installation are shown in Table 1.

Note: SDN users are not included in Table 1. For information about these users, refer to the SDN document Cloud SDN Hardening Guideline, Reference [2].

For more information about initial passwords, refer to the following sections of the [Configuration File Guide](#):

- [Generated and Prefilled Passwords](#)
- [IdAM](#)
- [Zabbix CEE User](#)
- [Shelf and Blade Management](#)
- [SDN Integration on HDS](#)

Table 1 Initial Administrator and System Account Credentials

Username	Where	Type	Initial Password and Public Key Set	Password Access Allowed ⁽¹⁾	Place of Use	Allowed Human Interface
ceeadm	vCIC, compute, vFuel	Linux	Initial factory password; initial public key is generated at installation time Public key access from vCIC to vCICs, compute, and vFuel	Yes	Initial non-root administrator account for example for creating LDAP administrators or accounts. Disable after admin users are created Local user in vFuel, LDAP user for vCIC and compute	SSH, console access



Table 1 Initial Administrator and System Account Credentials

Username	Where	Type	Initial Password and Public Key Set	Password Access Allowed ⁽¹⁾	Place of Use	Allowed Human Interface
ceebackup	vCIC, vFuel	Linux	Initial factory password; initial public key is generated at installation time Public key access from vCIC to vCICs, compute, and vFuel	Yes	Backup and restore processes Local user in vCIC, vFuel	SSH, console access
ceecore	vCIC	Linux	Initial password for login locked by default, initial public key is generated at installation time Public key access from vCIC to vCICs and compute	No	Service account for crash and core management, not for login	System account, not for human operation
cmha	vCIC, compute, vFuel	Linux	Initial password for login locked by default, initial public key is generated at installation time Public key access from vCIC to vCICs, compute, and vFuel	No	System account, not for login	System account, not for human operation
Service user accounts, for example nova, bin in /etc/shadow	vCIC, compute (nova), vFuel (no OpenStack users)	Linux	No passwords, some of them have public keys if communication is required	No	Running system daemons, system account, not used for login	System accounts, not for human operation
root	vFuel	Linux	Initial factory password, password based login must be disabled after install. Root account public key access from vFuel to vCIC and compute	Yes	In operation system account to manage vCIC, compute, and vFuel	SSH, console access at bootstrap
root	vCIC, compute	Linux	Initial factory password, public key based login available only from vFuel	Yes, but console only access (no SSH)	Mainly system account for vFuel to manage vCIC and compute Console access for recovery	Console access for password, no SSH (for recovery)
root	Atlas VM	Linux	No public key based authentication	No	System account, not for login	System account, not for human operation
atlasadm	Atlas VM	Linux	Initial password to log in to Atlas, no public key based authentication by default	Yes	Initial account in Atlas VM	SSH
admin	OpenStack (vCIC, host, Atlas)	OpenStack	Initial factory passwords, no public keys	Yes	OpenStack management	Atlas dashboard, OpenStack CLI (RESTful interfaces)



Table 1 Initial Administrator and System Account Credentials

Username	Where	Type	Initial Password and Public Key Set	Password Access Allowed ⁽¹⁾	Place of Use	Allowed Human Interface
Service accounts within OpenStack	OpenStack (vCIC, compute)	OpenStack	Randomly generated passwords during installation	No	System accounts	System accounts, not for human operation
User accounts in LDAP	Compute	LDAP	No, but can be configured; password complexity can be applied	Yes	Operating system	SSH
zabbix_ce_user	Zabbix API, OpenStack	OpenStack	User and password can be set		Read-only user in Zabbix to read the GUI	GUI, RO
OpenStack cloud administrators	vCIC	OpenStack	None, no password complexity in OpenStack Mitaka release	Yes, to OpenStack	OpenStack management	OpenStack API
OpenStack cloud users	vCIC	OpenStack	None, no password complexity in OpenStack Mitaka release	Yes, to OpenStack	OpenStack limited management	OpenStack API
admin	ScaleIO MDM	ScaleIO	Password	Yes	ScaleIO management	CLI, GUI
Gateway admin user	ScaleIO GW	ScaleIO	Password	Yes	ScaleIO management	CLI
Frontend configurator user for Cinder	ScaleIO MDM	ScaleIO	Password	No		
BSP users	BSP	HW	Refer to BSP documentation, password	Yes		SSH
HDS users	HDS	HW	Refer to HDS documentation			
admin	Extreme	HW	SSH password, SOAP service	Yes		SSH, SOAP

(1) The value of this field is “Yes” in case it is a human access account. The value is “No”, if it is a system account.

Note: All these credentials are mandatory for the system to function correctly.

There are different kind of credentials in the system for machine to machine and for human intended usage. All machine to machine passwords are updated or randomly generated during the time of the deployment in order to avoid well-known passwords that would cause privilege escalation and security issues.

For more information about user and password management, refer to [Infrastructure Administrator Management Guide](#).

3.1.2 Prehardened System Components

The following components are subject to prehardening in the system:

— Compute HW



- Compute OS
- vCIC OS
- Atlas OS
- vFuel OS
- Extreme switches
- EMC ScaleIO storage

3.1.2.1 Compute HW Hardening

The compute hardware equipment is prehardened by the original vendor. For more information refer to the documentation of the manufacturer.

3.1.2.2 Compute OS Hardening

The compute host uses Ubuntu 14.04 Linux, and is, for most parts, prehardened.

All services that are running on the compute host after installation are required, and must not be disabled.

All available but unnecessary services and ports have already been disabled.

For a list of the compute host ports and services, refer to the [Security User Guide](#).

For the compute host, only Secure Shell (SSH) version two (SSH-2) is allowed as a network access protocol.

3.1.2.3 vCIC OS Hardening

The vCIC hosts use Ubuntu 14.04 Linux, and are, for most parts, prehardened.

All services that are running on the vCIC host OS after installation are required, and must not be disabled.

All available but unnecessary services and ports have already been disabled.

For a list of the vCIC ports and services, refer to the [Security User Guide](#).

For the vCIC, only SSH-2 is allowed as a network access protocol.

3.1.2.4 Atlas OS Hardening

The Atlas host uses Ubuntu 14.04 Linux, and is, for most parts, prehardened.

All services that are running on Atlas after installation are required, and must not be disabled.



All available but unnecessary services and ports have already been disabled.

For a list of the Atlas ports and services, refer to the [Security User Guide](#).

For Atlas, only SSH-2 is allowed as a network access protocol.

3.1.2.5 vFuel OS Hardening

The vFuel node uses CentOS, and is, for most parts, prehardened.

All services that are running on the vFuel node after installation are required, and must not be disabled.

For a list of the vFuel ports and services, refer to the [Security User Guide](#).

For vFuel, only Secure Shell (SSH) version two (SSH-2) is allowed as a network access protocol.

3.1.2.6 Extreme Switch Hardening

The Extreme switches are prehardened by Extreme Networks.

3.1.2.7 EMC ScaleIO Storage Hardening

Note: This section is only applicable if EMC ScaleIO storage is used.

If CEE is installed with a managed ScaleIO storage solution, the ScaleIO solution is prehardened by EMC. For more information, refer to [ScaleIO Security Configuration Guide](#), Reference [7].

3.2 Hardening During Installation and Integration

This section contains information about the hardening activities that are performed during the installation and integration.

For more information about user configuration, refer to the following documents:

- Sections [IdAM](#) and [LDAP Users](#) in the [Configuration File Guide](#)
- SDN document [Cloud SDN Hardening Guideline](#), Reference [2]

3.2.1 Initial Administrator Credentials

The initial credentials for all of the predefined local administrators are configured in `config.yaml` during the system installation. The default passwords for the following human access accounts must be changed before installing the system, or immediately after the system deployment:

- `ceedm`, for more information, see [Section 3.3.5](#) on page 18.



- `ceebackup`, for more information, see Section 3.3.5 on page 18.
- `root` user for vFuel, for more information, see Section 3.3.5 on page 18.
- `root` user for vCIC host and compute host, for more information, see Section 3.3.3 on page 17.
- `atlasadm`, for more information, see Section 3.3.4 on page 18.
- `admin`, for more information, see Section 3.3.7 on page 19.

For detailed instructions on how to manage administrator passwords, refer to the [Infrastructure Administrator Management Guide](#) and the [Security User Guide](#).

3.2.2 DC-FW Configuration

In the current system, the DC-FW is located outside the Cloud Execution Environment (CEE).

The DC-FW provides protection for the system, and also acts as an O&M firewall.

The DC-FW is used to enforce access control between SDs.

In the DC-FW two logical firewall instance types can be defined, one is responsible for controlling the CEE management traffic, another is responsible for the protection of the tenant.

The SDs, and their relations are shown in Figure 2. The O&M-FW is a logical instance in the DC-FW. Tenant firewall is another logical instance in the DC-FW, that protects the data center from external attacks, by performing basic screening of tenant traffic.

Settings of the tenant firewall is out of the scope of this document, as the exact settings depend on the security expectations of the tenant. The tenant traffic must not be mixed with the O&M traffic.

At the perimeter of CEE, a Data Center Gateway (DC-GW) and DC-FW protects the internals of the CEE. For more information refer to the [DC Firewall Hardening Guide](#).

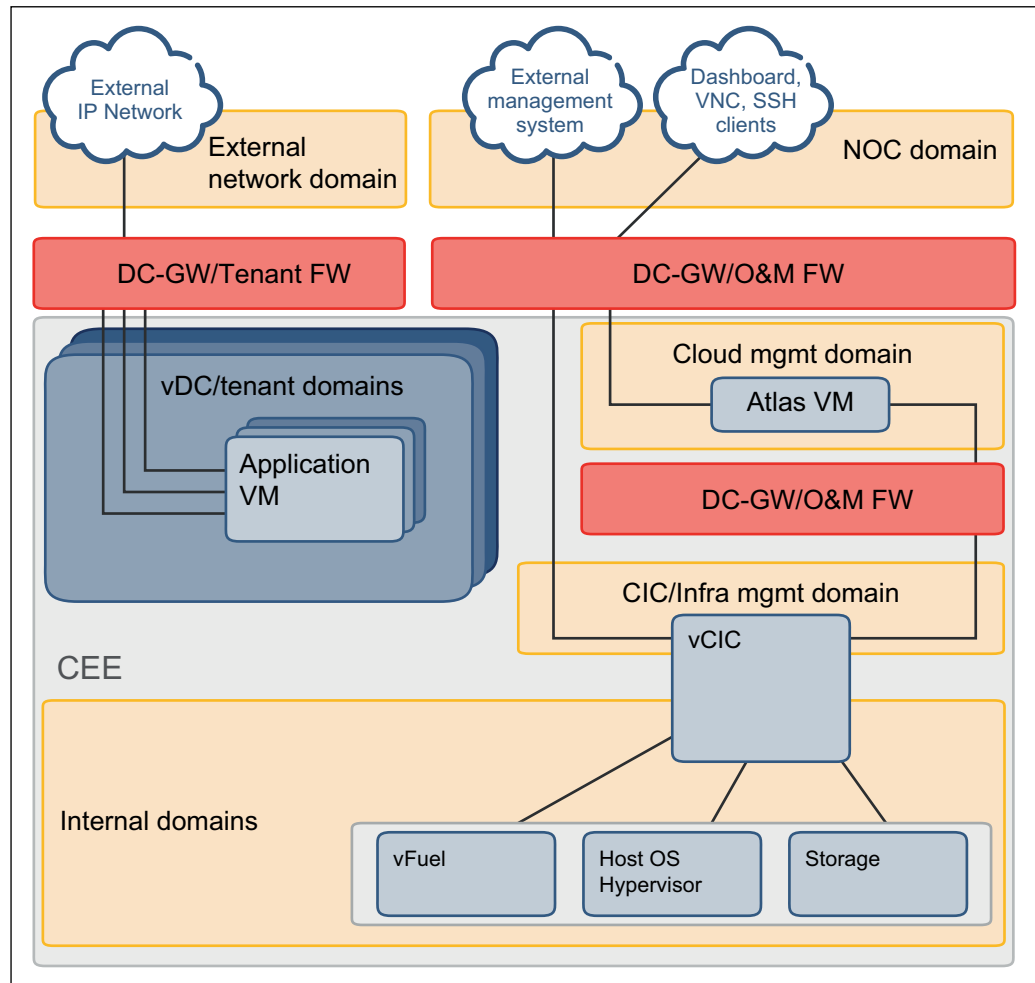


Figure 2 Security Domains

For the logical configuration of the O&M-FW during the installation (grouped by outbound direction), use Table 2, Table 3, and Table 4 as references.

Table 2 Traffic Flows from NOC Domain

Source			Destination			Service		
Security Domain	Address	Port	Security Domain	Address	Port	Proto	Application	Information
NOC	Admin clients	Any	Cloud management domain	CIC northbound public IP	443	HTTPS	TLS	Zabbix vHost
NOC	Admin clients	Any	Cloud management domain	Atlas northbound	443	TCP	HTTPS	Atlas Horizon service
NOC	Admin clients	Any	CIC/infra management domain	CIC northbound public IP	5900:15899	TCP	HTTPS	VNC Console Address



Table 2 Traffic Flows from NOC Domain

Source			Destination			Service		
Security Domain	Address	Port	Security Domain	Address	Port	Proto	Application	Information
NOC	Admin/browser	Any	CIC/infra management domain	CIC northbound public IP	8774	TCP		Nova
					8775			Nova
					8776			Cinder
					6080			Nova
NOC	Admin clients	Any	Cloud management domain	CIC northbound public IP	6611	TCP	TLS	ScaleIO GUI

Table 3 Traffic Flows from Cloud Management Domain

Source			Destination			Service		
Security Domain	Address	Port	Security Domain	Address	Port	Proto	Application	Information
Cloud management domain	Atlas Southbound	Any	CIC/infra management domain	CIC northbound public IP	22	TCP	SSH SCP, SFTP	Non-REST API access to the CIC
Cloud management domain	Admin/browser	Any	CIC/infra management domain	CIC northbound public IP	6080	TCP	HTTPS	OpenStack VNC support
Cloud management domain	Cloud Management System	Any	CIC/infra management domain	CIC HAProxy	5000	TCP	HTTPS	Keystone-1
					6080			Nova-novncproxy
					8052			Watchmen
					8054			Watchmen
					8080			Swift
					8774			Nova
					8776		HTTPS	Cinder
					8777			Ceilometer
					9292			Glance
					9494			Glance
					9696			Neutron
					35357			Keystone-2
					30165	UDP	SNMP	Watchmen
Cloud management domain	Browser/Client	Any	Cloud management domain	Atlas southbound	8888	TCP	HTTPS	ovtf API
					8004			heat API
					8003			heat API cloudwatch
					8000			heat API cnf



Table 4 Traffic Flows from CIC/Infra Management Domain

Source			Destination			Service		
Security Domain	Address	Port	Security Domain	Address	Port	Proto	Application	Information
CIC/infra management domain	CIC public API address	Log aggregator	Cloud management domain	Atlas south bound	20514	TCP	RELP	Log collector in Atlas
CIC/infra management domain	CIC public API address	NMS Server	NOC	NOC	162	UDP	SNMP v2	FM:SNMP traps
CIC/infra management domain	Extreme Switch	123	NOC	NOC	123	UDP	ntp	ntp-server in NOC time server

For more information about how to set the rules in DC-FW, refer to [DC Firewall Hardening Guide](#).

3.2.3 Authenticate NTP Server

Authenticate the upstream NTP servers as described in section [NTP Authentication](#) in the [Configuration File Guide](#).

3.2.4 Change Legal Text Presented at Logon

To change the predefined message shown before logon attempts, update the `config.yaml` as described in section [Legal Text Presented at Logon](#) in the [Configuration File Guide](#).

3.2.5 ScaleIO Management Tools

Note: This section is only applicable if EMC ScaleIO storage solution is used and deployed in CEE managed mode.

ScaleIO is accessible with GUI, which must be deployed outside CEE (for example in a NOC domain) on the `public_vip` network, on port 6611. The EMC ScaleIO GUI requires the MDM IP address, set to the `public_vip` address.

Managing ScaleIO via CLI is also possible from CEE nodes that are running the ScaleIO Meta Data Manager (MDM) component.

3.2.6 Location of Logs

Logs are written to the following locations:

- **vFuel logs**, including `rsyslogd` logs and local logs, are stored under `/var/log/remote/<host_name_or_ip_address>`.



An example is:

```
[root@fuel ~]# ll /var/log/remote/
total 36
drwxr-x--- 3 root root 4096 May  9 13:39 127.0.0.1
lrwxrwxrwx 1 root root 22 May  9 12:18 192.168.0.20 -> compute-0-2.domain.tld
lrwxrwxrwx 1 root root 21 May  9 12:18 192.168.0.21 -> cinder-0-5.domain.tld
lrwxrwxrwx 1 root root 22 May  9 12:18 192.168.0.22 -> compute-0-4.domain.tld
lrwxrwxrwx 1 root root 22 May  9 12:18 192.168.0.23 -> compute-0-3.domain.tld
lrwxrwxrwx 1 root root 22 May  9 12:18 192.168.0.24 -> compute-0-6.domain.tld
lrwxrwxrwx 1 root root 16 May  9 12:48 192.168.0.25 -> cic-3.domain.tld
lrwxrwxrwx 1 root root 16 May  9 12:48 192.168.0.26 -> cic-2.domain.tld
lrwxrwxrwx 1 root root 16 May  9 12:48 192.168.0.27 -> cic-1.domain.tld
drwxr-x--- 4 root root 4096 May  9 12:57 cic-1.domain.tld
drwxr-x--- 4 root root 4096 May  9 12:57 cic-2.domain.tld
drwxr-x--- 4 root root 4096 May  9 12:57 cic-3.domain.tld
drwxr-x--- 4 root root 4096 May  9 13:02 cinder-0-5.domain.tld
drwxr-x--- 5 root root 4096 May  9 12:45 compute-0-2.domain.tld
drwxr-x--- 5 root root 4096 May  9 12:45 compute-0-3.domain.tld
drwxr-x--- 5 root root 4096 May  9 12:45 compute-0-4.domain.tld
drwxr-x--- 5 root root 4096 May  9 13:01 compute-0-6.domain.tld
```

If CEE is configured to write logs to vFuel (`ericsson.logging.forward_to_fuel` is set to `true`), logs are written to vFuel even after deployment. If `ericsson.logging.forward_to_fuel` is set to `false`, only vFuel logs are written under `/var/log/remote/<host_name_or_ip_address>`.

- For the location of **infrastructure related logs**, refer to Audit and Security Logging.
- For the location of **Atlas logs**, refer to the Locating Files section in the Atlas Troubleshooting Guideline, Reference [1].
- In CEE deployments with tightly integrated SDN, the logging framework of SDN processes is independent from CEE. For more information on **SDN logs**, refer to the SDN document Logging, Reference [5].
- For the location of **ScaleIO logs**, refer to Audit and Security Logging.
- For the location of **licensing related (NeLS) logs**, refer to Audit and Security Logging.

3.3 Product Security Maintenance After Installation and Integration

This section contains information about the hardening activities that are performed after the installation and integration.

3.3.1 Manage Administrator Credentials

This section describes the management of administrator credentials.



3.3.1.1 Changing Password for Predefined Administrator Credentials

The passwords for the predefined administrator credentials must be changed on a regular basis.

For the detailed procedure of managing the following predefined administrator credentials, and for the procedure of changing the passwords, refer to the [Infrastructure Administrator Management Guide](#) and the [Security User Guide](#):

- root user for vCIC host and compute host, for more information see Section 3.3.3 on page 17.
- atlasadm, for more information see Section 3.3.4 on page 18.
- ceeadm, for more information see Section 3.3.5 on page 18.
- ceebackup, for more information see Section 3.3.5 on page 18.
- root user for vFuel, for more information see Section 3.3.5 on page 18.
- grub user, for more information see Section 3.3.6 on page 18.
- admin, for more information see Section 3.3.7 on page 19.

The passwords must fulfill the strong password conditions. For the strong password conditions, see Section 4 on page 22, or refer to your local company policy for defining strong passwords.

3.3.1.2 Changing Password for Operator Defined Administrator Credentials

It is strongly advised to regularly change the administrator passwords of the credentials that are defined by the operator in the system.

For detailed instructions on how to manage administrator passwords, refer to the [Infrastructure Administrator Management Guide](#) and the [Security User Guide](#).

3.3.1.3 Creating Additional Credentials

During the first startup of the system, only the default administrator credentials are available. In addition to those credentials, each system administrator must use individual personal user accounts when logging in. The use of shared accounts is not recommended. For the vCIC hosts, the compute host, the storage solution, and for the Extreme switches, individual user accounts are provisioned in the LDAP server. For Atlas, user accounts are local.

For more information about credentials management, refer to [Infrastructure Administrator Management Guide](#).



3.3.2 Change Certificates on vFuel

3.3.2.1 Change Cobbler Certificate

To change the Cobbler certificate on vFuel, perform the following steps:

1. Acquire the new certificate and key in pem x509 format with the necessary characteristics (for example, using OpenSSL).
2. Create a backup of the current certificate and key. The location of the certificate and the key are listed in `/etc/httpd/conf.d/ssl.conf`.
3. Copy the new certificate (`cobbler.crt`) and key (`cobbler.key`) to the `/var/lib/fuel/keys/master/cobbler/` directory on vFuel.
4. Restart the Apache and Cobbler services:

```
systemctl restart httpd.service
systemctl restart cobblerd.service
```

5. Check the availability of the Cobbler Web UI at `https://<VFUEL_IP_ADDRESS>/cobbler_web`.

3.3.2.2 Change Fuel Web GUI Certificate

1. Acquire the new certificate and key in pem x509 format with the necessary characteristics (for example, using OpenSSL).
2. Create a backup of the current certificate and key on vFuel. The location of the certificate and the key are listed in `/etc/nginx/conf.d/services.conf`. The location is by default `/var/lib/fuel/keys/master/nginx/`.
3. Copy the new certificate (`nginx.crt`) and key (`nginx.key`) to the `/var/lib/fuel/keys/master/nginx/` directory on vFuel.
4. Restart the Apache and Nginx services:

```
systemctl restart httpd.service
systemctl restart nginx.service
```

5. Check the availability of the Fuel Web UI at `https://<VFUEL_IP_ADDRESS>:8443`.

3.3.3 vCIC Host OS Hardening

After the installation, the root password must be changed. For the procedure of changing the root password, refer to the documents [SW Installation in Multi-Server Deployment](#) and [SW Installation in Single Server Deployment](#).

The root access with a password to vCIC host is disabled by default, and only administrator accounts defined in the LDAP can be used for login.



The `ceedm` account is not to be used for direct login after the administrator accounts in LDAP have been created.

3.3.4 Atlas User Management

For Atlas, user accounts are local. The initial system user, `atlasadm`, with `sudo` rights is created during the prehardening. The password of the `atlasadm` is set during the installation procedure.

For more information refer to [Atlas SW Installation](#).

3.3.5 vFuel User Management

After the initial installation, only the `root` user exists in the vFuel server. The CEE deployment adds the `ceedm`, `cmha`, and `ceebackup` users to the vFuel server.

It is possible to use the `ceedm` user to access the vFuel server for creating the initial personal accounts. After that, the `ceedm` user must only be used by infrastructure components, and during update and rollback.

It is recommended to create additional local Linux user accounts to the vFuel server for personnel administering the system.

It is possible to disable predefined users after the access is available with additional users, with the following command:

```
usermod -e 1 <username>
```

It is possible that `root` access is required during system update and expansion. In such cases, the `root` account must be enabled with the following command:

```
usermod -e "" root
```

Once the activities that require the `root` access have been completed, it is recommended to lock the account again.

The passwords for all vFuel administrators must be changed by using the `passwd` command on a regular basis.

It is possible to configure users with password expiry. Enter `passwd -?` for the available options.

3.3.6 GRUB User Management

After the successful deployment of the system, it is recommended to change the password for the Grand Unified Bootloader (GRUB) user, as described in section [Change GRUB Password in the Runtime Configuration Guide](#).



For more information about the initial configuration of the GRUB password, used for CEE installation, refer to section [GRUB Configuration](#) in the [Configuration File Guide](#).

3.3.7 Extreme Switch User Management

The Extreme switch default user account is defined as `admin` without a password defined. After the successful deployment of the system, it is recommended to change the password for the local `admin` user in the Extreme switch.

By default, CEE installation creates a user defined in the `config.yaml` system configuration, which is used by system components, such as OpenStack Neutron, for accessing and configuring the switch. This user must not be modified at runtime.

For managing the local switch accounts, refer to the Extreme EXOS documentation.

3.3.8 ScaleIO Access Control

Note: This section is only applicable if EMC ScaleIO storage solution is used.

Change the initial passwords as described in the “Access Control Settings” section of the ScaleIO Security Configuration Guide, Reference [7]. After changing the passwords, update the `config.yaml` with the new passwords. This is needed because ScaleIO administrator users are not managed by the Identity and Access Management (IdAM).

3.3.9 NeLS Access Control

Note: In CEE 6 NeLS connection is not mandatory.

Change the initial passwords as described in the NeLS document NeLS Security User Guide, Reference [6]. For more information and possible restrictions, refer to the [Configuration File Guide](#).

3.3.10 Managing TLS Certificates in CEE

For more information on the necessary certificates and the tasks to perform before installation, refer to the [CA and NBI Certificates for Secure HTTPS Access](#) section of the documents [SW Installation in Multi-Server Deployment](#) and [SW Installation in Single Server Deployment](#). To configure a secure NBI connection, refer to section [Secure NBI API Endpoints](#) in the [Configuration File Guide](#).

3.3.10.1 Certificates for ScaleIO

Note: This section is only applicable if EMC ScaleIO storage solution is used.



Ensure that TLS certificates are available. For more information, refer to the “Communication Security Settings” section of the ScaleIO Security Configuration Guide, Reference [7].

3.3.11 CEE Infrastructure Network Hardening for SDN Tight Integration

The procedure described in this section serves to prevent Neutron from selecting VNIs used by HDS for infrastructure connectivity through the L3 fabric, by creating separate Neutron networks for the infrastructure networks. Perform the following steps:

1. Log on to a vCIC as admin.
2. Create an infrastructure project:

```
openstack project create <project_name>
```

Example output:

```
root@cic-1:~# openstack project create cee_infra
+-----+-----+
| Field      | Value                                     |
+-----+-----+
| description | None                                     |
| enabled     | True                                    |
| id          | 71e18a4e3d98463d9079ca2ea29cfe69      |
| name        | cee_infra                             |
+-----+-----+
```

Note: Make a note of the UUID shown in the `id` field, as it will be required later.

3. Identify the VNIs used by the CEE infrastructure networks using the HDS CCM.
4. For each VNI, create a Neutron network assigned to the UUID of the infrastructure project, with `vxlan` network type, using the VNI as `segmentation_id`.

```
neutron net-create --tenant-id <project_UUID> --provider:network_type vxlan =>
--provider:segmentation_id <network_VNI> <network_name>
```

Note: The UUID can be retrieved using `openstack project list`.

For example:



```
root@cic-1:~# neutron net-create --tenant-id 71e18a4e3d98463d9079ca2ea29cfe69 =>
--provider:network_type vxlan --provider:segmentation_id 4098 cee_om_sp_1_forvlan201_cee1
Created a new network:
```

Field	Value
admin_state_up	True
availability_zone_hints	
availability_zones	
created_at	2018-03-22T09:01:39
description	
id	c342a213-5cbe-4c65-8fac-b51a22e0fe92
ipv4_address_scope	
ipv6_address_scope	
mtu	1450
name	cee_om_sp_1_forvlan201_cee1
port_security_enabled	True
provider:network_type	vxlan
provider:physical_network	
provider:segmentation_id	4098
router:external	False
shared	False
status	ACTIVE
subnets	
tags	
tenant_id	71e18a4e3d98463d9079ca2ea29cfe69
updated_at	2018-03-22T09:01:39

Example 1 Neutron Network Creation for Infrastructure VNI



4 Strong Password Conditions

In order to set a strong password, the following conditions must be met:

- The length of the password must be at least 12 characters.
- The password must contain the following:
 - At least one lower-case alphabetic character
 - At least one upper-case alphabetic character
 - At least one numeric character
 - At least one special character
- The password must not contain more than three consecutive instances of the same character class.
- Real names or words must not be used.
- The password must not be the same as the user name.



Reference List

- [1] Atlas Troubleshooting Guideline, 6/1553-CRA 119 1873/5 Uen B
- [2] Cloud SDN Hardening Guideline, 2/1553-AXD 101 08/6-V1
- [3] ISO27002: Information technology — Security techniques — Code of practice for information security controls ISO/IEC 27002 Second edition 2013-10-01, <http://www.iso.org>
- [4] ISO27011: Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002 ISO/IEC 27011 First edition 2008-12-15, <http://www.iso.org>
- [5] Logging, 3/198 22-AXD 101 08/6-V1
- [6] NeLS Security User Guide, 5/1553-AVA 901 45/2
- [7] ScaleIO® Security Configuration Guide, 2/1553-CNA 403 3308/5