

CEE Hardening Checklist

Cloud Execution Environment

CHECK LIST

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	Target Audience	1
1.2	Required Competence	1
2	Hardening Checklists	3
2.1	Assess Hardening Activities	3
2.2	Perform Hardening Activities	7
	Reference List	13





1 Introduction

This document enumerates the various hardening steps that must be performed in order to make the Cloud Execution Environment (CEE) secure during its whole lifecycle.

Attention!

Hardening is not an optional feature or function. The assessment of security risks in an operational environment must be performed (refer to Section 4.2.4.2 in ISO 27011, Reference [1]). 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 in ISO 27011, Reference [1]). The owner or the responsible (refer to Section 6.1.1 in ISO 27011, Reference [1]) of the CEE node must assess the risks to have clear responsibility and accountability.

For more information on how to manage information security in the telecommunications organization, refer to the ISO 27011 standard, Reference [1].

This document provides two checklists, one to assess, and one to perform the hardening activities described in [System Hardening Guideline](#). For more information, see Section 2 on page 3.

1.1 Target Audience

This document is primarily intended to be used by staff responsible for CEE. This includes operational personnel performing installing, upgrading/updating, or maintaining activities. Furthermore, security administrators managing security and IT, and Telecom (security) operational managers responsible for Information Security Management System (ISMS) according to ISO 27011, Reference [1] and ISO 27002, Reference [2]. More specifically, in Section 6.1.1 in ISO 27011, Reference [1] and in Section 6.1.1 b) in ISO 27002, Reference [2].

1.2 Required Competence

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

1.2.1 Operational Personnel

It is required for operational personnel, performing the installing, upgrading/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 or equivalent certificates. 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).

1.2.2 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 or equivalent certificates 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.



2 Hardening Checklists

This section includes the checklists and provides information on their use.

2.1 Assess Hardening Activities

Table 1 is an assessment template for each hardening item described in section **Hardening Activities** in the **System Hardening Guideline**. During the assessment of each hardening activity, the following must be explained in the comment section of Table 1:

- The reason why the activity is needed, or detailed explanation why it is not needed.
- Who made the decision, especially when the activity is deemed unneeded.
- How to manage the risks of not applying the hardening activity, for example, to whom the risk is transferred to, who accepted the risk, or how to mitigate the risk, if needed.

Table 1 Assessment of Hardening Activities

Assessed as Compulsory [Y/N]	Hardening Activity	Comments Detailed explanation: if not applied, why, decision made by, how to manage the risk
	Configure initial system and administrator credentials.	
	Check the prehardening setup for system components (Compute OS, vCIC OS, Atlas OS, vFuel OS, Extreme switches,, and EMC ScaleIO).	



Table 1 Assessment of Hardening Activities

Assessed as Compulsory [Y/N]	Hardening Activity	Comments Detailed explanation: if not applied, why, decision made by, how to manage the risk
	Change the default passwords of the initial administrator credentials.	
	Configure the Data Center Firewall rules.	
	Authenticate the upstream NTP servers.	
	Change the predefined legal message shown before logon attempts.	
	Configure logs.	



Table 1 Assessment of Hardening Activities

Assessed as Compulsory [Y/N]	Hardening Activity	Comments Detailed explanation: if not applied, why, decision made by, how to manage the risk
	Configure ScaleIO management tools.	
	Create additional credentials. Each system administrator must use an individual personal account when logging in.	
	Change the root password for vCIC, compute, and Atlas.	
	Disable root access with password for vCIC, compute, and Atlas.	
	Lock root user access on vFuel, after the additional account is created.	



Table 1 Assessment of Hardening Activities

Assessed as Compulsory [Y/N]	Hardening Activity	Comments Detailed explanation: if not applied, why, decision made by, how to manage the risk
	Lock ceeadm user access on vFuel after the additional account is created.	
	Change passwords for all vFuel administrators on a regular basis.	
	Change the password for the Grand Unified Bootloader (GRUB) user.	
	Change the password for the local admin user in the Extreme switch.	
	Control ScaleIO access.	



Table 1 Assessment of Hardening Activities

Assessed as Compulsory [Y/N]	Hardening Activity	Comments Detailed explanation: if not applied, why, decision made by, how to manage the risk
	Control NeLS access.	
	Ensure that TLS certificates are available for ScaleIO services.	

Provide the date when the assessment of the hardening activities were completed:

Provide the name of the personnel who performed the assessment:

2.2 Perform Hardening Activities

Table 2 lists the hardening activities as described in section [Hardening Activities](#) in the [System Hardening Guideline](#), that must be performed during installation, based on the result of the assessment. If no assessment was performed, it is expected that all items are mandatory to be performed. If some items are assessed as not required in the assessment, and the **why it is not needed, how to manage the risk**, and **who made the decision** fields are filled, the activity may not need to be performed.

Fill the table for each activity that is already performed.

If there are comments, for example, “it was only possible to perform partially”, or “there is an error in the process and a Trouble Report (TR) is raised to cover the issue”, provide this information there.



Table 2 List of Hardening Activities

[Y/N]	Phase for the Hard ening Activity	Hardening Activity	Reference ⁽¹⁾	Comments
	Before installat ion	Configure initial system and administrator credentials.	Initial System and User Accounts	
	Before installat ion	Check the prehardening setup for system components (Compute OS, vCIC OS, Atlas OS, vFuel OS, Extreme switches, and EMC ScaleIO).	Prehardened System Components	
	During installat ion	Change the default passwords of the initial administrator credentials.	Initial Admi nistrator Credentials	
	During installat ion	Configure the Data Center Firewall rules.	DC-FW Configuration	



Table 2 List of Hardening Activities

[Y/N]	Phase for the Hard ening Activity	Hardening Activity	Reference ⁽¹⁾	Comments
	During installat ion	Authenticate the upstream NTP servers.	Authenticate NTP Server	
	During installat ion	Change the predefined legal message shown before logon attempts.	Change Legal Text Presented at Logon	
	During installat ion	Configure logs.	Location of Logs	
	During installat ion	Configure ScaleIO management tools.	ScaleIO Management Tools	
	After installat ion	Create additional credentials. Each system administrator must use an individual personal account when logging in.	Creating Additional Credentials	



Table 2 List of Hardening Activities

[Y/N]	Phase for the Hard ening Activity	Hardening Activity	Reference ⁽¹⁾	Comments
	After installat ion	Change the root password for vCIC, compute, and Atlas.	vCIC Host OS Hardening Atlas User Management vFuel User Management	
	After installat ion	Disable root access with password for vCIC, compute, and Atlas.	vCIC Host OS Hardening Atlas User Management vFuel User Management	
	After installat ion	Lock root user access on vFuel, after the additional account is created.	vFuel User Management	
	After installat ion	Lock ceeadm user access on vFuel after the additional account is created.	vFuel User Management	



Table 2 List of Hardening Activities

[Y/N]	Phase for the Hard ening Activity	Hardening Activity	Reference ⁽¹⁾	Comments
	After installat ion	Change passwords for all vFuel administrators on a regular basis.	vFuel User Management	
	After installat ion	Change the password for the GRUB user.	GRUB User Management	
	After installat ion	Change the password for the local admin user in the Extreme switch.	Extreme Switch User Management	
	After installat ion	Control ScaleIO access.	ScaleIO Access Control	



Table 2 List of Hardening Activities

[Y/N]	Phase for the Hard ening Activity	Hardening Activity	Reference ⁽¹⁾	Comments
	After installat ion	Control NeLS access.	NeLS Access Control	
	After installat ion	Ensure that TLS certificates are available for ScaleIO services.	Certificates for ScaleIO	

(1) The corresponding section from the System Hardening Guideline

Provide the date when the listed hardening activities were completed:

Hardening performed by:



Reference List

Standards and Web Pages

- [1] 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>
- [2] ISO27002: Information technology — Security techniques — Code of practice for information security controls ISO/IEC 27002 Second edition 2013-10-01, <http://www.iso.org>