HITACHI
Inspire the Next

APPLICATION NOTE

FOXMAN-UN R18 RHEL9 Hardened Installation

CIS Red Hat Enterprise Linux 9 Benchmark for Level 2 – Server

Hitachi Energy

Document ID	1KHW029185-FR18	
Document edition	FOXMAN-UN System Release:	R18
	Revision:	A
	Date:	2025-09-17

Copyright and confidentiality

Disclaimer

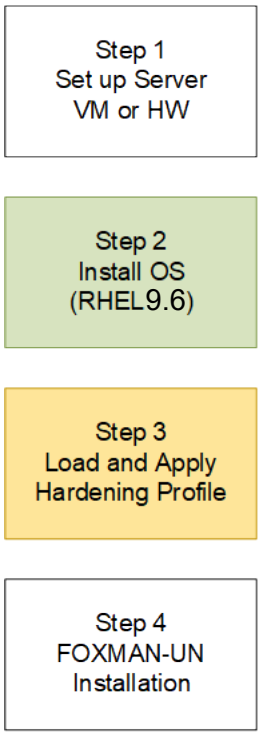
This document contains information about one or more Hitachi Energy products and may include a description of or a reference to one or more standards that may be generally relevant to the Hitachi Energy products. The presence of any such description of a standard or reference to a standard is not a representation that all the Hitachi Energy products referenced in this document support all the features of the described or referenced standard. In order to determine the specific features supported by a particular Hitachi Energy product, the reader should consult the product specifications for that Hitachi Energy product. In no event shall Hitachi Energy be liable for direct, indirect, special, incidental, or consequential damages of any nature or kind arising from the use of this document, nor shall Hitachi Energy be liable for incidental or consequential damages arising from the use of any software or hardware described in this document.
Hitachi Energy may have one or more patents or pending patent applications protecting the intellectual property in the Hitachi Energy products described in this document. The information in this document is subject to change without notice and should not be construed as a commitment by Hitachi Energy. Hitachi Energy assumes no responsibility for any errors that may appear in this document.
All people responsible for applying the equipment addressed in this manual must satisfy themselves that each intended application is suitable and acceptable, including compliance with any applicable safety or other operational requirements. Any risks in applications where a system failure and/or product failure would create a risk for harm to property or persons (including but not limited to personal injuries or death) shall be the sole responsibility of the person or entity applying the equipment, and those so responsible are hereby requested to ensure that all measures are taken to exclude or mitigate such risks.
Products described or referenced in this document are designed to be connected and to communicate information and data through network interfaces, which should be connected to a secure network. It is the sole responsibility of the system/product owner to provide and continuously ensure a secure connection between the product and the system network and/or any other networks that may be connected.
The system/product owners must establish and maintain appropriate measures, including, but not limited to, the installation of firewalls, application of authentication measures, encryption of data, installation of antivirus programs, and so on, to protect these products, the network, its system, and interfaces against security breaches, unauthorized access, interference, intrusion, leakage, and/or theft of data or information.
Hitachi Energy performs functionality testing on released products and updates. However, system/product owners are ultimately responsible for ensuring that any product updates or other major system updates (to include but not limited to code changes, configuration file changes, third-party software updates or patches, hardware change out, and so on) are compatible with the security measures implemented. The system/product owners must verify that the system and associated products function as expected in the environment in which they are deployed. Hitachi Energy and its affiliates are not liable for damages and/or losses related to security breaches, any unauthorized access, interference, intrusion, leakage, and/or theft of data or information.
This document and parts thereof must not be reproduced or copied without written permission from Hitachi Energy, and the contents thereof must not be imparted to a third party nor used for any unauthorized purpose.

Contents

1 Purpose

This document describes how to create the prerequisites for the installation of the FOXMAN-UN R18 on a CIS profile based hardened RedHat 9.6 system plus latest updates. This profile defines a baseline that aligns to the “Level 2 - Server” configuration from the Center for Internet Security® Red Hat Enterprise Linux 9 CIS Benchmarks™, v2.0.0, released 2024-06-24.

The general FOXMAN-UN installation procedure on a CIS hardened system includes the following four steps:



Please note:

Steps 1, 2, and 4 are described in FOXMAN-UN Installation Guideline - User Manual [2]. Chapter 3: Installation Process Overview.

→ A deviation in step 2, and step 3, are described in the document.

The information in this document is specific for the RHEL release 9.6 and the FOXMAN-UN R18.

For other versions / releases please check for a document update.

The procedure described herein is for hardening the FOXMAN-UN core components on the RedHat 9.6. It covers:

- the deviation in step 2, identified as step 2*. See section 2.1 below
- the loading any application of the hardening profile, identified as step 3.

For the step 1 (preparation of a HW or a Virtual Machine (VM)) resource requirements, check the FOXMAN-UN R18 release note [1].

For step 4 (installation of the FOXMAN-UN R18) see the FOXMAN-UN R18 Installation Guideline [2].

The procedure described herein does **not include** the hardening of installations where FOXMAN-UN clients are installed decentralized on Windows or other Linux Systems.

2 Hardening Procedure

2.1 Step 2* - Deviation from the standard OS installation

For the step 2*: installation of the RHEL 9.6, a deviation from the standard procedure (see reference [2]) is required.

The CIS hardening requests a dedicated file system setup as defined in the FOXMAN-UN Release Note R18 [1], tables “Recommended Partitioning Setup” and “Recommended LVM Physical Volume” in chapter “Partition Setup”.

Recommended values are dependent on the actual deployment.

Changes that need to be done:

- **/home** must be on a separate partition or logical volume and has to be created in the partitioning layout before installation can occur with a security profile.
- **/tmp** must be on a separate partition or logical volume and has to be created in the partitioning layout before installation can occur with a security profile.
- **/var** must be on a separate partition or logical volume and has to be created in the partitioning layout before installation can occur with a security profile.
- **/var/tmp** must be on a separate partition or logical volume and has to be created in the partitioning layout before installation can occur with a security profile.
- **/var/log** must be on a separate partition or logical volume and has to be created in the partitioning layout before installation can occur with a security profile.
- **/var/log/audit** must be on a separate partition or logical volume and has to be created in the partitioning layout before installation can occur with a security profile.

2.1.1 Deviation from the standard CIS Red Hat Enterprise Linux 9 Benchmark for Level 2 - Server profile

List of excluded rules to run the NMS.

- xccdf_org.ssgproject.content_rule_sudo_require_authentication
- xccdf_org.ssgproject.content_rule_no_shelllogin_for_systemaccounts
- xccdf_org.ssgproject.content_group_ensure_rsyslog_log_file_configuration
- xccdf_org.ssgproject.content_rule_rsyslog_files_permissions
- xccdf_org.ssgproject.content_rule_rsyslog_files_ownership
- xccdf_org.ssgproject.content_rule_rsyslog_files_groupownership
- xccdf_org.ssgproject.content_rule_dir_perms_world_writable_sticky_bits
- xccdf_org.ssgproject.content_rule_package_xorg-x11-server-common_removed
- xccdf_org.ssgproject.content_rule_xwindows_runlevel_target
- xccdf_org.ssgproject.content_rule_accounts_umask_etc_profile
- xccdf_org.ssgproject.content_rule_accounts_umask_etc_bashrc
- xccdf_org.ssgproject.content_rule_kernel_module_usb-storage_disabled
- xccdf_org.ssgproject.content_rule_package_gdm_removed

2.2 Step 3: Load and apply hardening profile

Risk of operating trouble!

The following rules, when applied, carry some risks with system operation under specific operating conditions and might be rolled back to default by the operator after thorough assessment:

- CCE-83700-5: Configure auditd admin_space_left Action on Low Disk Space
- CCE-83701-3: Configure auditd max_log_file_action Upon Reaching Maximum Log Size
- CCE-83703-9: Configure auditd space_left Action on Low Disk Space

→ They will affect the following settings when applied (comparison of applied and default):

CIS hardened	default
max_log_file = 6	max_log_file = 8
max_log_file_action = keep_logs	max_log_file_action = ROTATE
space_left_action = email	space_left_action = SYSLOG
admin_space_left_action = halt	admin_space_left_action = SUSPEND

- CCE-83450-7: Configure System Cryptography Policy (disable-SHA1)

→ can affect secure communication to FOX61x nodes which are provisioned with existing public keys.

→ In case communication is lost, enable ssh_rsa public keys by running /opt/nem/bin/private/reconfigure_nem and select option 2 when prompted: 2) Change ESW support: to **LEGACY**.

Risk of operating trouble!

The following rule(s), when applied, will lock user accounts when the CIS scan is run after FOXMAN-UN installation:

- CCE-86113-8: xccdf_org.ssgproject.content_rule_no_password_auth_for_systemaccounts

As nemadm and dirac have user IDs less than 1000 (i.e., 199 and 200, respectively), these users will be locked if the scan is run after FOXMAN-UN installation.

→ If this rule is applied, only run the scan **before installing FOXMAN-UN**.

- CCE-83627-0 Set Account Expiration Following Inactivity

→ Before applying hardening, change the root password.

This Step 3 is supported by loading an RPM (*ssg-rhel9-ds-hitachienergy-nms-customizations-17.1.1-1.noarch.rpm*), which includes a FOXMAN-UN adapted CIS profile.

This profile defines a baseline that aligns to the “Level 2 - Server” configuration from the Center for Internet Security® Red Hat Enterprise Linux 9 CIS Benchmarks™, v2.0.0, released 2024-06-24, for the following rules which are not applied:

- For FOXMAN-UN, DIRAC, and Quantis crypto key generator:
  - CCE-83543-9 Ensure Users Re-Authenticate for Privilege Escalation - sudo
  - CCE-83623-9 Ensure that System Accounts Do Not Run a Shell Upon Login
  - CCE-83689-0 Ensure System Log Files Have Correct Permissions
  - CCE-83946-4 Ensure Log Files Are Owned By Appropriate User
  - CCE-83834-2 Ensure Log Files Are Owned By Appropriate Group
  - CCE-83895-3 Verify that All World-Writable Directories Have Sticky Bits Set
  - CCE-84104-9 Remove the X Windows Package Group
  - CCE-84105-6 Disable X Windows Startup By Setting Default TargeT
  - CCE-90828-5 Ensure the Default Umask is Set Correctly in /etc/profile

- CCE-83644-5 Ensure the Default Bash Umask is Set Correctly
- CCE-83851-6 Disable Modprobe Loading of USB Storage Driver
- CCE-83549-6 Remove the GDM Package Group

Preconditions for loading and applying the hardening profile:

- Server / VM set up and loaded & updated with the RHEL 9.6.
- Disk partition and mountpoints according to the previous chapter.
- Admin & root accounts and privileges given.
- Customized profile RPM available on the system.

The hardening procedure is done according to the official RedHat hardening guide:

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html/security_hardening/index

2.2.1 Update OS to the RHEL 9.6 release

Make sure the correct version of the Pod Manager tool (podman container engine) is installed. The required version is: podman-4 (for RHEL 9.6) or as defined in the latest FOXMAN-UN R18 release note.

Also make sure the latest CIS Red Hat Enterprise Linux 9 Benchmark 1.0.0 profiles and fix tools are loaded.

To install this version on dnf/yum based systems, enter the following command as root:

```
# yum --releasever=9.6 update
```

To install this version on subscription-based systems, enter the following commands as root:

```
# subscription-manager release --set=9.6
# dnf update
```

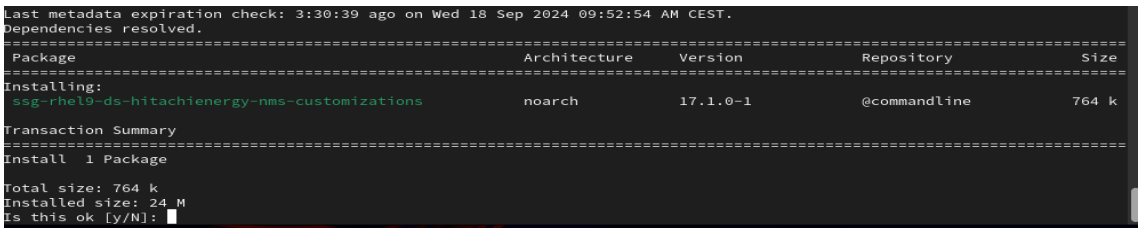
2.2.2 Predefined customization CIS profile and OpenScap installation

OpenScap Workbench Installation:

Run the following command to install openscap workbench tool, which guides you through the hardening process:

```
# dnf install -y scap-workbench
```

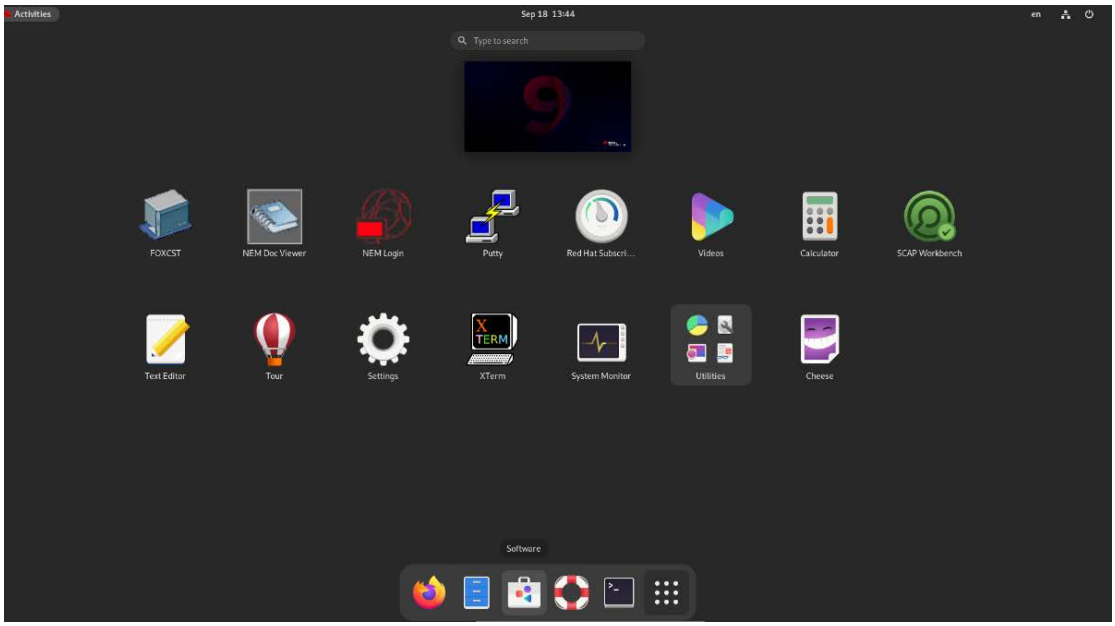
```
# dnf localinstall -y ssg-rhel9-ds-hitachienergy-nms-customizations-17.1.1-1.noarch.rpm
```



The rules which block a successful operation of the FOXMAN-UN (and DIRAC) application are deselected (see Step 3: Load and apply hardening profile).

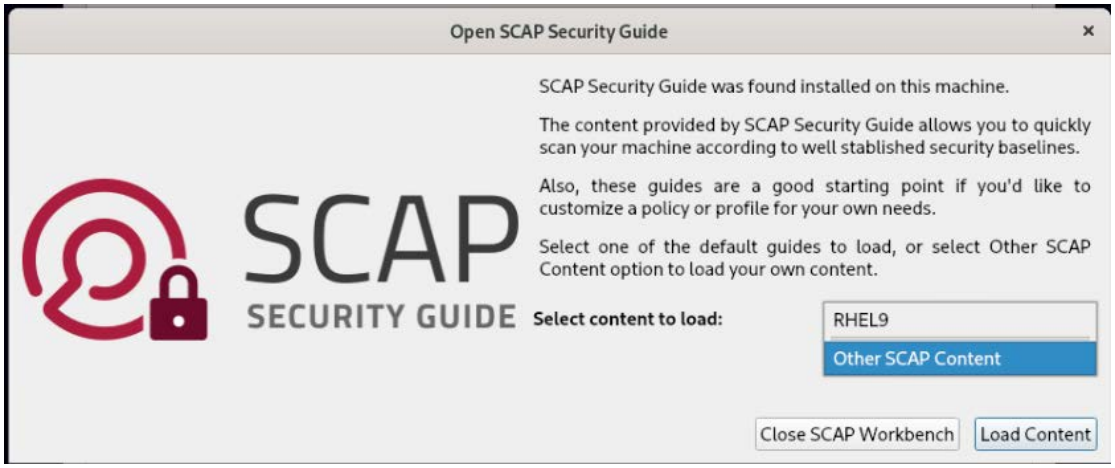
2.2.3 OpenScap hardening

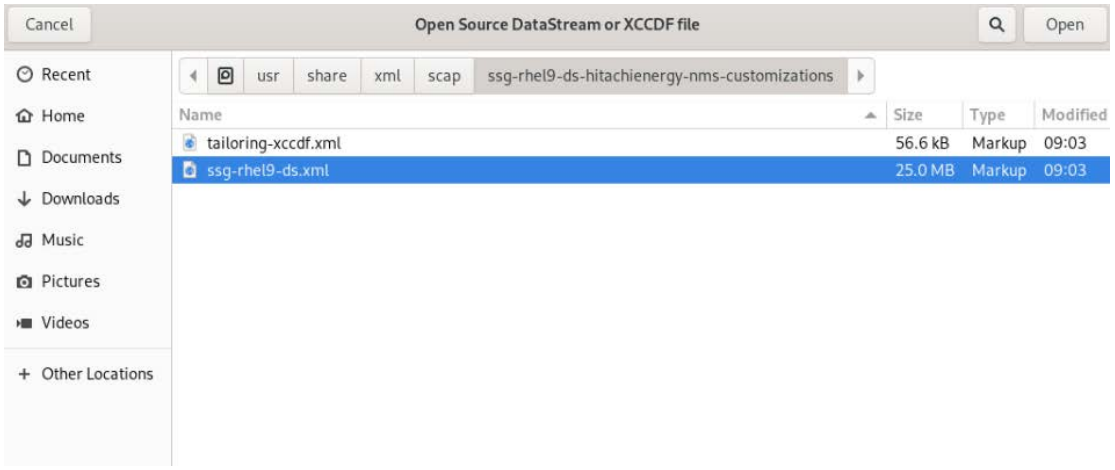
As root user, start SCAP Workbench:



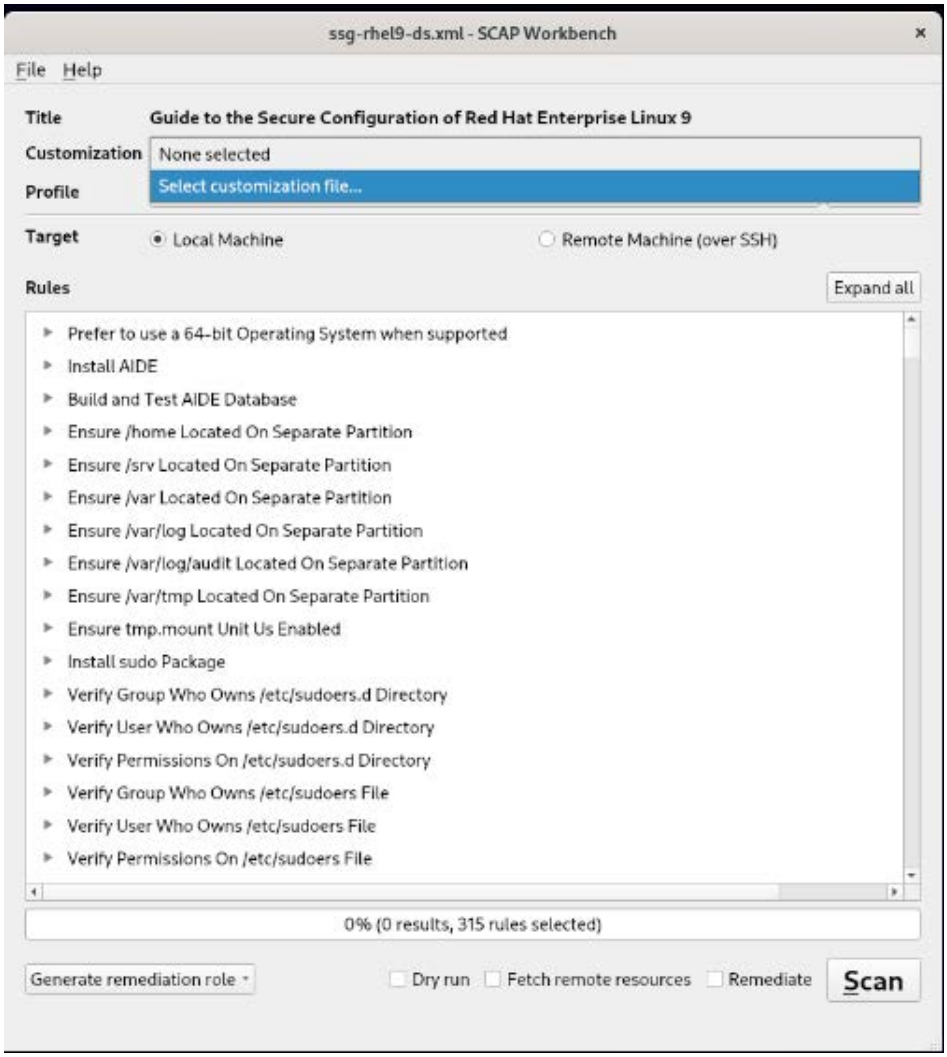
Select Other Content and then navigate to:

/usr/share/xml/scap/ssg-rhel9-ds-hitachienergy-nms-customizations/ssg-rhel9-ds.xml and open it:

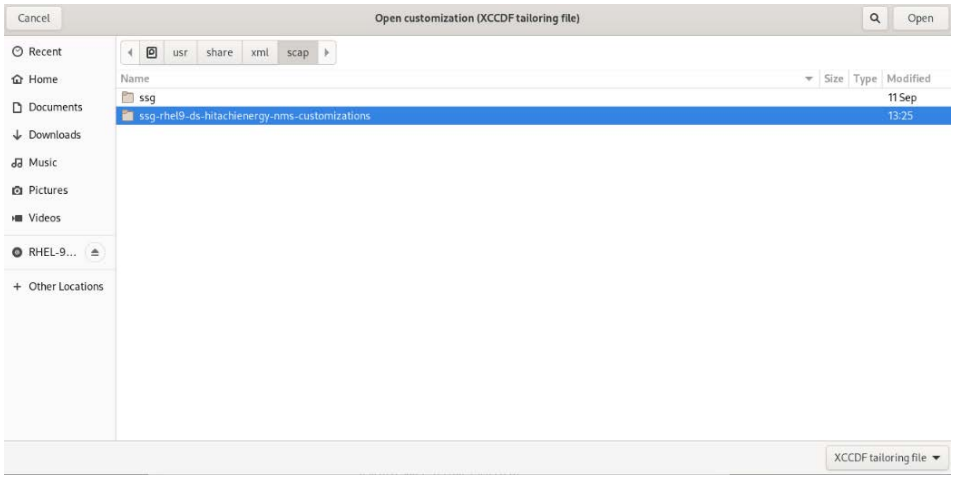




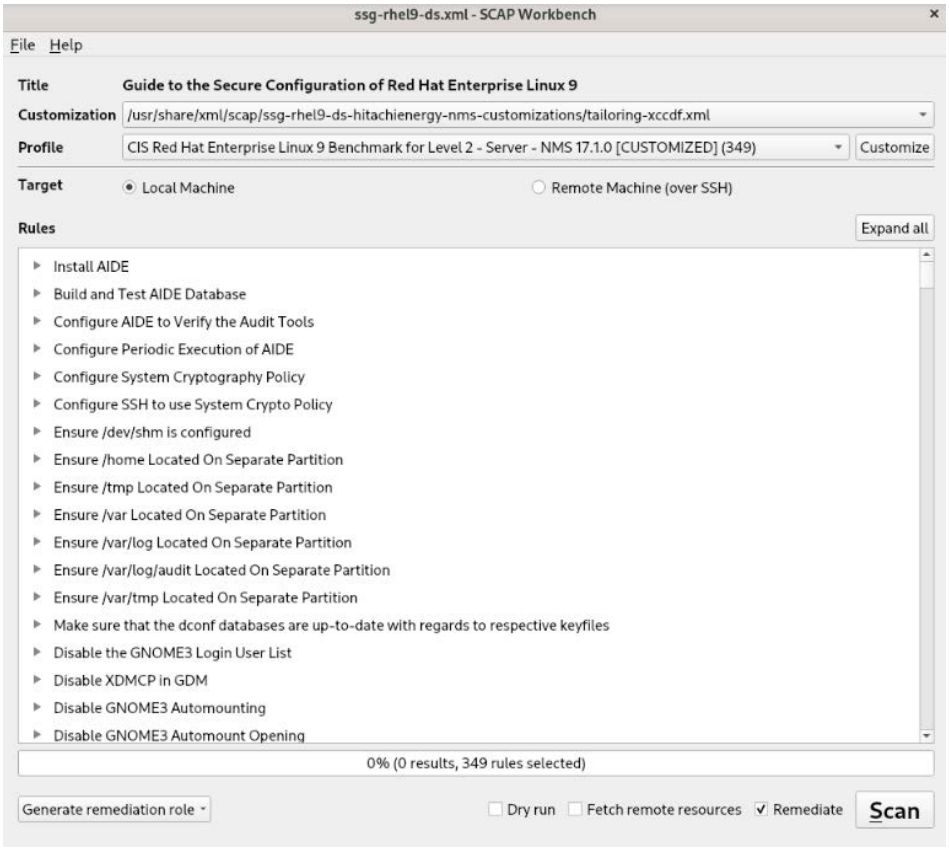
Open customization:



From file dialog navigate to \usr\share\xml\scap\ssg-rhel9-ds-hitachienergy-nms-customizations\tailoring-xccdf.xml file:

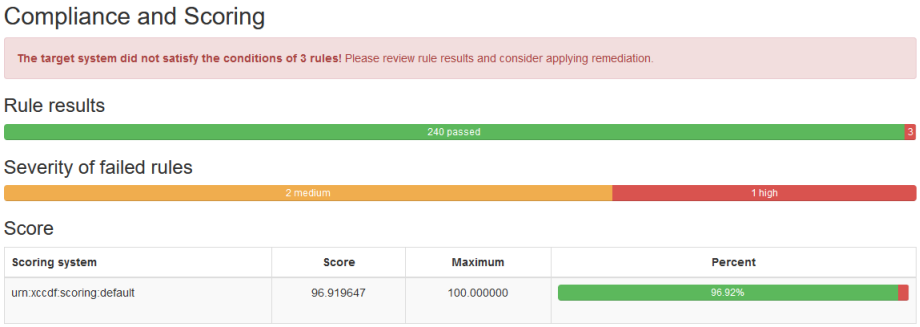


Click Ok to check the **Remediate** option:



Apply **Scan**

After that check the scoring (the result may be different from the one shown here):



Manual remediation:

Some rules require a **manual action** because an automatic fix is not supported.

CCE-83849-0

The grub2 boot loader should have a superuser account and password protection enabled to protect boot-time settings.

Since plaintext passwords are a security risk, generate a hash for the password by running the following command:

```
# grub2-setpassword
```

When prompted, enter the password that was selected.

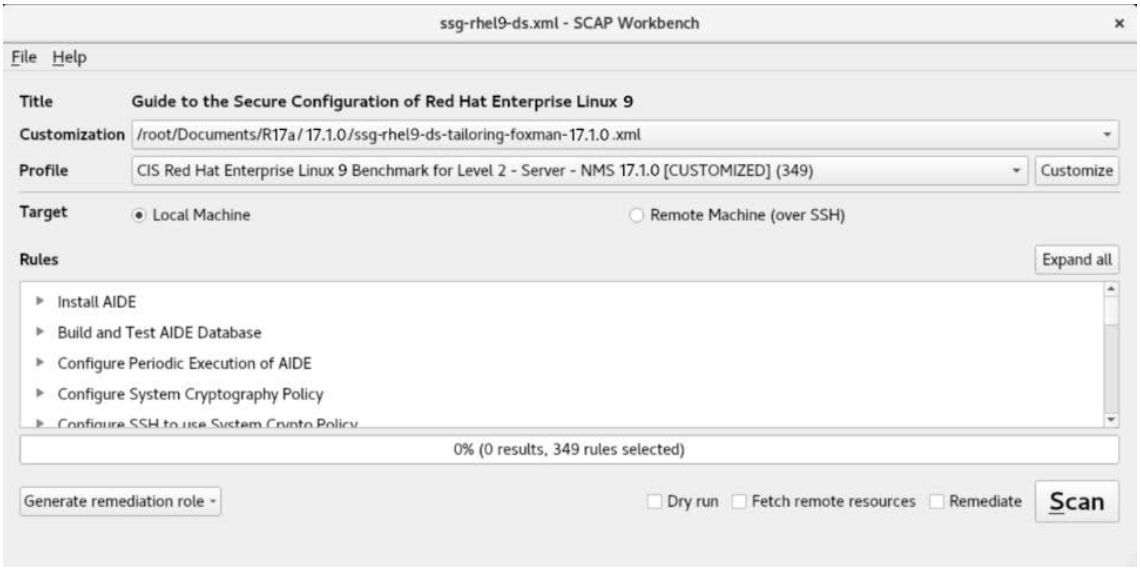
Once the superuser password has been added, update the grub.cfg file by running:

```
# grub2-mkconfig -o /boot/grub2/grub.cfg
```

Reboot the server.

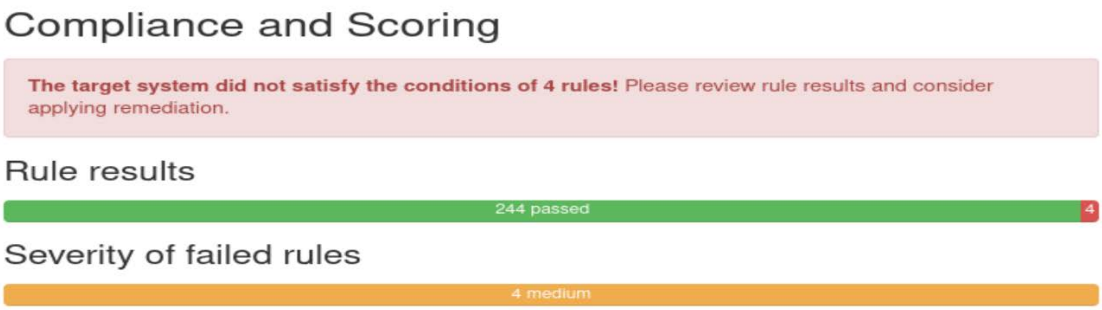
Check by openscap final result after manual fix.

Run the scap Scan only:



Final score:

Final score can be different from your installation, so a failed analysis is required to define what is expected and what is not.



Failed analysis:

Group	Severity	Result
result = **fail**		
Ensure that System Accounts Do Not Run a Shell Upon Login	medium	fail
Verify that All World-Writable Directories Have Sticky Bits Set	medium	fail
Ensure No World-Writable Files Exist	medium	fail
Ensure All Files Are Owned by a Group	medium	fail
Ensure No Daemons are Unconfined by SELinux	medium	fail

After that, check the scoring.

CCE-83623-9 Ensure that System Accounts Do Not Run a Shell Upon Login

Some accounts are not associated with a human user of the system, and exist to perform some administrative function. Should an attacker be able to log into these accounts, they should not be granted access to a shell.

CCE-83895-3 Verify that All World-Writable Directories Have Sticky Bits Set

When the so-called 'sticky bit' is set on a directory, only the owner of a given file may remove that file from the directory. Without the sticky bit, any user with write access to a directory may remove any file in the directory. Setting the sticky bit prevents users from removing each other's files. In cases where there is no reason for a directory to be world-writable, a better solution is to remove that permission rather than to set the sticky bit. However, if a directory is used by a particular application, consult that application's documentation instead of blindly changing modes.

To set the sticky bit on a world-writable directory DIR, run the following command:

```
$ sudo chmod +t DIR
```

CCE-83902-7 Ensure No World-Writable Files Exist

It is generally a good idea to remove global (other) write access to a file when it is discovered. However, check with documentation for specific applications before making changes. Also, monitor for recurring world-writable files, as these may be symptoms of a misconfigured application or user account. Finally, this applies to real files and not virtual files that are a part of pseudo file systems such as sysfs or procfs.

CCE-83906-8 Ensure All Files Are Owned by a Group

If any files are not owned by a group, then the cause of their lack of group-ownership should be investigated. Following this, the files should be deleted or assigned to an appropriate group. The following command will discover and print any files on local partitions which do not belong to a valid group:

```
$ df --local -P | awk '{if (NR!=1) print $6}' | sudo xargs -I '{}' find
'{}' -xdev -nogroup
```

To search all filesystems on a system including network mounted filesystems the following command can be run manually for each partition:

```
$ sudo find PARTITION -xdev -nogroup
```

3 Additional information

3.1 Referenced documents

Ref #	Document kind, title	Document no.
[1]	FOXMAN-UN Release Note R18	1KHW002499
[2]	FOXMAN-UN Installation Guideline - User Manual	1KHW002426
[3]	red_hat_enterprise_linux-9-security_hardening-en-us	(Web page)
[4]	red_hat_enterprise_linux-9-performing_a_standard_rhel_installation-en-us	(Web page)

Hitachi Energy Ltd
Bruggerstrasse 72
5400 Baden - Switzerland

Phone: please refer to https://www.hitachienergy.com/contact-us/Customer-Connect-Center (Customer Connect Center)
Email: communication.networks@hitachienergy.com

www.hitachienergy.com/communication-networks

Document ID: 1KHW029185 FR18 Rev. A