ERICSSON

ENM Node Hardening Guidelines and Instructions

Technical Document

1/17473-AOM 901 151 Uen AL

Contents

1 Node Hardening Guidelines

> The purpose of node hardening is to eliminate as many security risks as possible.

The security of a system is fundamental if the system is to ensure confidentiality, integrity, and availability of information.

Maintaining security over time is equally important as the initial node hardening, an audit of installed software and running services must be taken periodically. A comparison with the originally installed list of applications and services must be done. This is to ensure that no different RPMs or services are installed which can jeopardize security.

2 System Overview

> ENM is modular and layered software system-based on service-oriented architecture (SOA) with strong focus on separation of business logic and mediation through layering.

ENM uses Solution Sets (units of related functionality). These are used to deploy software support for those functions purchased or licensed by the operator. ENM is fully model-driven whereby contribution of models can be used to influence ENM functionality. ENM is easily extendable by the means of Standard Development Kits.

ENM design ensures it is fully horizontally scalable and highly available.

ENM graphical interface employs de-facto standard web technologies for a modern user experience.

3 Scope of Hardening

> ENM hardening involves the complete system, that is hardware, software, and deployment scenarios.

Specific hardening areas of concern in this document are:

- System hardware and deployment
- Operating System
- Application software and services
- Network and IP traffic
- Logging

4 Overview of Hardening Lifecycle

Hardening has its own lifecycle at initial product commissioning and upgrades.

In that respect, the following concerns are covered:

— Hardening before installation

— Hardening during installation

— Hardening after installation

— Hardening before upgrade

— Hardening after upgrade

5 Node Hardening Instructions

The following sections specify hardening activities and steps needed to be operated on the ENM system to ensure that the exposure to malicious attacks is as little as possible.

ENM system must be fully installed before applying the hardening instructions.

6 Hardening before Installation

Special attention must be given to passwords selection in *Site Engineering Data (SED)*.

Ensure that all passwords requested in SED are as strong as possible according to the policy declared in that document, Reference [3].

Specifically observe passwords used for ILOs, Virtual Connects, and Onboard Administrators.

6.1 Disable Usage of Port 22

To block SSH/SFTP communication on port 22 towards ENM South Bound Interface (SBI), the following changes are required:

1. *SED File Changes*

   ENM system can be installed or upgraded after configuring the following two parameters in its SED file:

   ```
   smrs_sftp_securePort = (port within the range 1025-65535)

   smrs_sftp_port_partition_enable = true
   ```

   With these changes, the ENM system is configured to allow only SFTP communication on configured port (value of smrs_sftp_securePort) for CM_VIP, AMOS, General Scripting, and Element Manager public IPs exposed to outside of ENM.

   Note: See the document ENM Site Engineering Document, Reference [3] for details of SED parameters for port 22.

2. *Firewall Configuration to Block Port 22*

   All the Public IP addresses and Public VIP IP addresses (except CM_VIP) exposed on SBI to communicate over port 22 with all nodes must be blocked using firewall rules.

   UL Spectrum user cases use port 22 for communication from node to ENM SBI. If customer is not willing to use UL Spectrum use cases, then modify the firewall rules to block SSH/SFTP requests from node towards CM_VIP public IP interfaces on port 22.

Note: ENM system supports configurable SFTP port feature for Radio and RadioTNodes only.

If the ENM system contains nodes other than Radio and RadioTNodes, then `Prohibit Usage of Port 22` feature cannot be enabled.

SSH/SFTP communication from ENM SBI to node on port 22 cannot be blocked.

- The SED file must be changed as follows:

  ```
  smrs_sftp_securePort = (port within the range 1025-65535)

  smrs_sftp_port_partition_enable = true
  ```

  After updating the SED file and given it to the ENM system, perform the initial Installation/Upgrade on the ENM.

- Procedure to get ENM SBI Public IP interface details for configuring the firewall to block port 22.

  a. Log on the Linux Management Server (LMS) for physical deployment or log on VNF-LAF for cloud deployment.

  b. Collect all the public IP interfaces and Public VIP IP addresses (except CM_VIP public IPs) from `global.properties` to configure the firewalls.

     If the ENM is not yet installed, the public IP addresses and Public VIPs can be fetched from SED document used for ENM installation.

     If UL Spectrum use cases are not required, then configure the firewall to block port 22 over CM_VIP public IPs.

7 Hardening during Installation

No specific hardening steps must be taken during installation of ENM system.

8 Hardening after Installation

This section outlines several hardening activities that need to be taken after installation of the ENM system.

8.1 System Hardware and Deployment Hardening

No specific steps must be taken to harden the System Hardware and deployment.

8.1.1 Virtual Machine Hardening on the Peer Servers

Virtual machines can be deployed on the peer servers as part of a deployment.

These hardening steps apply to physical deployment only.

To apply hardening activities on a VM, use the VM customization feature. For more information, see the document ENM VM Customization, Reference [5].

8.1.2 HPE Enclosure Hardening

We recommend logging to Enclosure and disabling the telnet service if found there. This ensures that only SSH is used.

These hardening steps apply to physical deployment only.

8.1.2.1 Disable Telnet Procedure

Note: This procedure is only applicable for Internal Brocade SAN switches.

Steps

1. Connect to the switch and log on as administrator user.
2. Identify the active policies for IPv4 and IPv6.

   ```
   switch:admin> ipfilter --show | grep active
   ```

   Example

   ```
   ieatc7000-181sanfc3:admin> ipfilter --show | grep active
   ```

   ```
   Name: default_ipv4, Type: ipv4, State: active
   ```

   ```
   Name: default_ipv6, Type: ipv6, State: active
   ```

3. Clone the active policies.

   Use the `ipfilter --clone` command for IPv4 and IPv6.

```
switch:admin> ipfilter --clone BlockTelnetv4 -from <IPv4 default policy>
switch:admin> ipfilter --clone BlockTelnetv6 -from <IPv6 default policy>
```

4. Save the new policies.

   Use the `ipfilter --save` command for IPv4 and IPv6.

```
switch:admin> ipfilter --save BlockTelnetv4
switch:admin> ipfilter --save BlockTelnetv6
```

5. Verify that the new policies exist.

   User the `ipfilter --show` command.

```
switch:admin> ipfilter --show
```

   Example

```
atc7000-65fc1:admin>  ipfilter --show
```

```
Name: default_ipv4, Type: ipv4, State: active
Rule    Source IP                                Protocol   Dest Port   Actio →
n
1     any                                             tcp       22     permit
2     any                                             tcp       23     permit
3     any                                             tcp       80     permit
4     any                                             tcp      443     permit
5     any                                             udp      161     permit
6     any                                             udp      123     permit
7     any                                             tcp      600 - 1023     →
 permit
8     any                                             udp      600 - 1023     →
 permit


Name: default_ipv6, Type: ipv6, State: active
Rule    Source IP                                Protocol   Dest Port   Actio →
n
1     any                                             tcp       22     permit
2     any                                             tcp       23     permit
3     any                                             tcp       80     permit
4     any                                             tcp      443     permit
5     any                                             udp      161     permit
```

```
6     any                                          udp      123     permit

7     any                                          tcp      600 - 1023     →
 permit

8     any                                          udp      600 - 1023     →
 permit


Name: BlockTelnetv4, Type: ipv4, State: defined

Rule    Source IP                                Protocol   Dest Port   Actio →
n

1     any                                          tcp       22     permit

2     any                                          tcp       23     permit

3     any                                          tcp       80     permit

4     any                                          tcp      443     permit

5     any                                          udp      161     permit

6     any                                          udp      123     permit

7     any                                          tcp      600 - 1023     →
 permit

8     any                                          udp      600 - 1023     →
 permit

Name: BlockTelnetv6, Type: ipv6, State: defined

Rule    Source IP                                Protocol   Dest Port   Actio →
n

1     any                                          tcp       22     permit

2     any                                          tcp       23     permit

3     any                                          tcp       80     permit

4     any                                          tcp      443     permit

5     any                                          udp      161     permit

6     any                                          udp      123     permit

7     any                                          tcp      600 - 1023     →
 permit

8     any                                          udp      600 - 1023     →
 permit
```

6. Add a rule to the policies.

   Use the `ipfilter --addrule` command.

```
switch:admin> ipfilter --addrule BlockTelnetv4 -rule 1 -sip any -dp 23 -prot →
o tcp -act deny

switch:admin> ipfilter --addrule BlockTelnetv6 -rule 1 -sip any -dp 23 -prot →
o tcp -act deny
```

Note: The rule number assigned must precede the default rule number for this protocol. For example, in the defined policy, the Telnet rule number is 2. To block effectively Telnet, the rule number 1 must be assigned to the new rule.

If the user chooses not to use 1, the user must delete the Telnet rule number 2 after adding this rule.

7. Identify and delete the telnet rule in the policies that permits input TCP traffic over port 23.

```
switch:admin> ipfilter --show -a BlockTelnetv4
```

```
Name: BlockTelnetv4, Type: ipv4, State: defined (modified)
Rule Source_IP Proto Dest_Port Action Flow Destination_IP
1 any tcp 23 D I/P any
2 any tcp 22 P I/P any
3 any tcp 23 P I/P any
4 any tcp 80 P I/P any
5 any tcp 443 P I/P any
6 any udp 161 P I/P any
7 any udp 123 P I/P any
8 any tcp 600-1023 P I/P any
9 any udp 600-1023 P I/P any
```

```
switch:admin> ipfilter --show -a BlockTelnetv6
```

```
Name: BlockTelnetv6, Type: ipv6, State: defined (modified)
Rule Source_IP Proto Dest_Port Action Flow Destination_IP
1 any tcp 23 D I/P any
2 any tcp 22 P I/P any
3 any tcp 23 P I/P any
4 any tcp 80 P I/P any
5 any tcp 443 P I/P any
6 any udp 161 P I/P any
7 any udp 123 P I/P any
8 any tcp 600-1023 P I/P any
9 any udp 600-1023 P I/P any
```

Example

In the example, the rule three is deleted from both policies.

```
switch:admin> ipfilter --delrule BlockTelnetv4 -rule 3
```

```
switch:admin> ipfilter --delrule BlockTelnetv6 -rule 3
```

8. Save the new IP filter policies.

   Use the `ipfilter --save` command.

```
switch:admin> ipfilter --save
```

9. Verify if the new policy is correct.

   Use the `ipfilter --show` command.

```
switch:admin> ipfilter --show
```

   Example

```
atc7000-65fc1:admin> ipfilter --show
```

```
Name: default_ipv4, Type: ipv4, State: active
Rule    Source IP                                Protocol   Dest Port   Actio →
n
1     any                                           tcp       22     permit
2     any                                           tcp       23     permit
3     any                                           tcp       80     permit
4     any                                           tcp      443     permit
5     any                                           udp      161     permit
6     any                                           udp      123     permit
7     any                                           tcp      600 - 1023      →
 permit
8     any                                           udp      600 - 1023      →
 permit
```

```
Name: default_ipv6, Type: ipv6, State: active
Rule    Source IP                                Protocol   Dest Port   Actio →
n
1     any                                           tcp       22     permit
2     any                                           tcp       23     permit
3     any                                           tcp       80     permit
4     any                                           tcp      443     permit
5     any                                           udp      161     permit
6     any                                           udp      123     permit
7     any                                           tcp      600 - 1023      →
 permit
8     any                                           udp      600 - 1023      →
 permit
```

```
Name: BlockTelnetv4, Type: ipv4, State: defined
Rule    Source IP                                Protocol   Dest Port   Actio →
n
1     any                                           tcp       23       deny
2     any                                           tcp       22     permit
3     any                                           tcp       80     permit
4     any                                           tcp      443     permit
5     any                                           udp      161     permit
6     any                                           udp      123     permit
7     any                                           tcp      600 - 1023     →
 permit
8     any                                           udp      600 - 1023     →
 permit
```

```
Name: BlockTelnetv6, Type: ipv6, State: defined
Rule    Source IP                                Protocol   Dest Port   Actio →
n
1     any                                           tcp       23       deny
2     any                                           tcp       22     permit
3     any                                           tcp       80     permit
4     any                                           tcp      443     permit
5     any                                           udp      161     permit
6     any                                           udp      123     permit
7     any                                           tcp      600 - 1023     →
 permit
8     any                                           udp      600 - 1023     →
 permit
```

10. Activate the new IP filter policy.

    Use the `ipfilter --activate` command for IPv4 and IPv6.

```
switch:admin> ipfilter --activate BlockTelnetv4
switch:admin> ipfilter --activate BlockTelnetv6
```

11. Verify if the new policies are active.

    Use the `ipfilter --show` command.

```
atc7000-65fc1:admin> ipfilter --show
```

```
Name: default_ipv4, Type: ipv4, State: defined
Rule    Source IP                                Protocol   Dest Port   Actio →
n
1     any                                           tcp       22     permit
```

```
2     any                                          tcp        23     permit
3     any                                          tcp        80     permit
4     any                                          tcp       443     permit
5     any                                          udp       161     permit
6     any                                          udp       123     permit
7     any                                          tcp       600 - 1023     →
 permit
8     any                                          udp       600 - 1023     →
 permit
```

```
Name: default_ipv6, Type: ipv6, State: defined
Rule    Source IP                                Protocol   Dest Port   Actio →
n
1     any                                          tcp        22     permit
2     any                                          tcp        23     permit
3     any                                          tcp        80     permit
4     any                                          tcp       443     permit
5     any                                          udp       161     permit
6     any                                          udp       123     permit
7     any                                          tcp       600 - 1023     →
 permit
8     any                                          udp       600 - 1023     →
 permit
```

```
Name: BlockTelnetv4, Type: ipv4, State: active
Rule    Source IP                                Protocol   Dest Port   Actio →
n
1     any                                          tcp        23       deny
2     any                                          tcp        22     permit
3     any                                          tcp        80     permit
4     any                                          tcp       443     permit
5     any                                          udp       161     permit
6     any                                          udp       123     permit
7     any                                          tcp       600 - 1023     →
 permit
8     any                                          udp       600 - 1023     →
 permit
```

```
Name: BlockTelnetv6, Type: ipv6, State: active
Rule    Source IP                                Protocol   Dest Port   Actio →
n
1     any                                          tcp        23       deny
2     any                                          tcp        22     permit
3     any                                          tcp        80     permit
4     any                                          tcp       443     permit
```

```
5     any                                          udp      161     permit
6     any                                          udp      123     permit
7     any                                          tcp      600 - 1023      →
 permit
8     any                                          udp      600 - 1023      →
 permit
```

Note: These steps must be performed on all the enclosures.

Results

Disabled Telnet Successfully.

Note: Although the telnet access is disabled, access to the CLI through the SSH, the serial console (from the OA), and the Java Web interface are still available.

8.1.3 Disable IPv6 Stack Support

IPv6 protocol stack is internally used by different components of the system and it is not possible to disable IPv6 protocol stack completely in ENM deployment.

These hardening steps apply to physical deployment only.

Nevertheless protection from rogue IPv6 Router Advertisement it is possible to be done using the following steps (by setting certain `sysctl` parameters).

Prerequisites

No prerequisites.

Steps

1. Log on the Peer server with `litp-admin` user and change to root.
2. Make a copy of the existing `sysctl` configuration file.
3. Run the command:

```
cp /etc/sysctl.conf /etc/sysctl.conf.bak
```

4. Edit `/etc/sysctl.conf` and add the following lines to the bottom:

```
net.ipv6.conf.default.autoconf=0
net.ipv6.conf.default.accept_ra=0
net.ipv6.conf.default.accept_ra_defrtr=0
net.ipv6.conf.default.accept_ra_rtr_pref=0
net.ipv6.conf.default.accept_ra_pinfo=0
net.ipv6.conf.default.accept_source_route=0
net.ipv6.conf.default.accept_redirects=0
net.ipv6.conf.all.autoconf=0
net.ipv6.conf.all.accept_ra=0
```

```
net.ipv6.conf.all.accept_ra_defrtr=0
net.ipv6.conf.all.accept_ra_rtr_pref=0
net.ipv6.conf.all.accept_ra_pinfo=0
net.ipv6.conf.all.accept_source_route=0
net.ipv6.conf.all.accept_redirects=0
```

Results

Changes are applied after next reboot.

8.1.4 Disable and Enable Email Relay Service

The disabling of the email relay service impacts the use cases which require mail sending to external destinations (for example, alarm routing through email)

Prerequisites

No prerequisites.

Steps

1. Log on the `lvsrouter` VMs.
2. Update the file `/ericsson/enm/lvsrouter/etc/template_main.cf` as follows.

   From:

   ```
   inet_interfaces = all
   #inet_interfaces = $myhostname
   #inet_interfaces = $myhostname, localhost
   #inet_interfaces = localhost
   ```

   to:

   ```
   #inet_interfaces = all
   #inet_interfaces = $myhostname
   #inet_interfaces = $myhostname, localhost
   inet_interfaces = localhost
   Then restart postfix service with:
   # /bin/systemctl restart postfix.service
   Repeat actions on all lvsrouter VM.
   ```

8.1.5 Hardening of Virtual Connect (VC)

These hardening steps apply to physical deployment only.

8.1.5.1 Disable SNMP on Virtual Connect

Prerequisites

No prerequisites.

Steps

1. Log on the Web Interface on the VC.
2. Go to `SNMP Configuration` option.
3. Disable SNMP by unselecting the `Enable V1, V2` field. Unselect `Enable V3` too if it is set.

8.1.5.2 Check for Secure SSL Ciphers

Prerequisites

No prerequisites.

Steps

1. Log on the Web Interface on the VC.
2. Check that only secure ciphers for SSL are allowed (this is the default).

8.1.5.3 Change the SNMP Community Name (If Needed)

Prerequisites

No prerequisites.

Steps

1. Log on the `ILO` as either `OA` administrator or `OA` operator.
2. Set the SNMP community name with the new string.

   ```
   SET SNMP COMMUNITY {READ | WRITE } "string"
   ```

   Max 20 characters are allowed on each.

8.1.5.4 SSL Hardening

Prerequisites

No prerequisites.

Steps

1. Open ILO web UI.
2. Click **Administration** > **Security** > **Encryption** > **Enforce AES/3DES Encryption** > **Enabled**.
3. Click **Administration** > **Security** > **Encryption** > **ssl Certificate** > **Customize** > **Import Certificate**.

   Generate a certificate with 2048 bits if necessary.

8.2 Operating System Hardening

Hardening of the ENM Operating System is detailed in LITP Node Hardening Instructions, Reference [6], and must be performed right after ENM installation is completed.

No additional operating system configuration must be done after hardening steps have been applied.

Security patches for the operating system are included with ENM delivery. Operating System patching is not done by default after the product is released and must be requested from Ericsson.

8.3 Application and Services Hardening

This section describes hardening and configuration activities that must be performed in ENM system to reduce further the surface of vulnerabilities.

8.3.1 ILO and Onboard Administrator (OA) Hardening

These hardening steps apply to physical deployment only.

8.3.1.1 Turn off Telnet

Prerequisites

No prerequisites.

Steps

1. Log on the **OA** GUI.
2. Navigate to **Enclosure Information** > **Enclosure Settings** > **Network Access**.
3. Unselect **Enable Telnet** on **Protocols** tab.

8.3.1.2 Disable SNMP

Prerequisites

No prerequisites.

Steps

1. Log on the **OA** GUI.
2. Navigate to **Enclosure Information** > **Enclosure Settings** > **SNMP Settings**.
3. Unselect **Enable SNMP** on **Settings** tab.

8.3.2 How to Change Root Passwords for OpenDJ

These hardening steps apply to physical deployment only and must be executed from the Management Server (MS-1).

For the installation and upgrade, the OpenDJ root password is taken from the SED variable LDAP_ADMIN_PASSWORD.

Root Password for OpenDJ is changed by running the following script:

```
[root@ms-1]# /opt/ericsson/opendj/change_opendj_password.sh
```

Note: Because of existing Access Control implementation, when `OpenDJ` root password is changed, all VMs must be restarted using the new password.

This procedure involves downtime that depends on the deployment size. The procedure involves a rolling over LITP plan for services and scripting clusters and the duration of the plan varies depending on the deployment size.

When the password is changed, enter the new password into the `LDAP_ADMIN_PASSWORD` parameter in the SED - preferably directly after the password change procedure, as the change affects subsequent ENM upgrades.

Prerequisites

— Root access to Management Server (MS-1).

— SED is available for updates.

Steps

1. Take a snapshot of the system.

   See Create ENM Snapshot on page 23.

2. Log on the ENM MS as the litp-admin user and switch to the root user.

3. Change directory.

   ```
   [root@ms-1]# cd /opt/ericsson/opendj/
   ```

4. Run the script.

   ```
   [root@ms-1]# sh change_opendj_password.sh
   ```

5. Enter the following information to update the password in OpenDJ.

   — Current password

   — New password which fulfills the following credentials:

   The following are the password policies described in ENM Identity and Access Management System Administrator Guide, Reference [1]:

   — Password must have at least eight characters.

   — Password must contain at least one lower case alpha character.

   — Password must contain at least one upper case alpha character.

   — Password must contain at least one numeric character.

   — Password must not contain: username, first name, or last name.

   — Password can contain special characters (non-alphanumeric characters).

   — Only hyphen (-), underscore (_), and period (.) are allowed in password.

   — The system asks if the password has to be changed. If so, click y or n if you resign.

   Repeat the new password and then confirm the password change.

Result: The following message is displayed on successful completion of the command. `Password was changed successfully`

If the new password does not comply with the password policies, the change is rejected.

The root passwords in `OpenDJ` are updated. Log files are on MS-1 in the following location: `/var/log/opendj`.

Note: After the password change, it is also important to enter the new password into the `LDAP_ADMIN_PASSWORD` parameter in the SED - preferably directly after the password change procedure, as the change affects subsequent ENM upgrades.

6. Execute the following commands.

   These commands modify the yum repositories so that when the LITP plan is generated it contains rolling over node tasks for services and scripting clusters.

   ```
   [root@ms-1]# cd /var/www/html/ENM_services/
   [root@ms-1]# touch *.rpm
   [root@ms-1]# yum clean all && createrepo .
   [root@ms-1]# cd /var/www/html/ENM_scripting/
   [root@ms-1]# touch *.rpm
   [root@ms-1]# yum clean all && createrepo .
   ```

7. Create and run the LITP plan.

   ```
   [root@ms-1]# litp create_plan
   [root@ms-1]# litp show_plan
   [root@ms-1]# litp run_plan
   ```

8. Monitor the progress of the plan and wait for it to complete.

   ```
   [root@ms-1]# /opt/ericsson/enminst/bin/monitor_plan.sh
   ```

9. Remove the snapshot taken in Step 1 once the procedure has completed successfully. See Remove ENM Snapshot on page 24.

   Note: If the procedure does not complete successfully, restore the snapshot taken at the beginning of this procedure:

   For detailed instructions about restoring snapshots, see the *Restore the System Using Snapshots* section in the document ENM Upgrade Instructions, Reference [9].

8.3.2.1 Create ENM Snapshot

Create a snapshot of the ENM deployment.

Steps

1. Log on the `ENM MS` as the `litp-admin` user and switch to the root user.
2. List the snapshots.

   ```
   [root@ms-1]# cd /opt/ericsson/enminst/bin
   [root@ms-1]# bash enm_snapshots.bsh --action list_snapshot
   ```

   The output contains information if any LVM, SFS, or SAN snapshots exist. Search the output for text similar to the following messages:

   Example

   ```
   [root@ms-1]# cd /opt/ericsson/enminst/bin
   [root@ms-1]# bash enm_snapshots.bsh --action list_snapshot
   2015-08-15 09:39:55 INFO list_snapshots : SFS SNAP: No NAS snapshots found o →
   n the system.
   2015-08-15 09:39:55 INFO list_snapshots : LVM SNAP: No LVM snapshots found o →
   n the system.
   2015-08-15 09:39:57 INFO list_snapshots : SAN SNAP : No LUN snapshots found  →
   on the system.
   2015-08-15 09:39:57 INFO main : ENM list_snapshot finished successfully
   ```

   If any snapshots exist, go to step 3. If no snapshots exist, go to step 4.
3. Remove the snapshot.

   ```
   [root@ms-1]# bash enm_snapshots.bsh --action remove_snapshot
   ```

   Result: ENM remove_snapshot is finished successfully.
4. Create the snapshot.

   ```
   [root@ms-1]# bash enm_snapshots.bsh --action create_snapshot
   ```

   Result: ENM create_snapshot is finished successfully.
5. Validate the snapshot.

   ```
   [root@ms-1]# bash enm_snapshots.bsh --action validate_snapshot
   ```

   Result: ENM validate_snapshot is finished successfully.

8.3.2.2 Remove ENM Snapshot

Remove a snapshot of the ENM deployment.

Steps

1. Log on the ENM MS as the litp-admin user and switch to the root user.
2. Remove the snapshot.

```
[root@ms-1]# cd /opt/ericsson/enminst/bin
[root@ms-1]# bash enm_snapshots.bsh --action remove_snapshot
```

Result: ENM remove_snapshot is finished successfully.

8.3.3 How to Change SSO Password for OpenDJ

A root user can update the SSO OpenDJ password.

These hardening steps apply to physical deployment only and must be executed from the Management Server (MS-1).

For the installation and upgrade, the SSO OpenDJ password is taken from the SED variable COM_INF_LDAP_ADMIN_ACCESS.

SSO Password for OpenDJ is changed by running the following script:

```
[root@ms-1]# /opt/ericsson/opendj/change_config_sso_password.sh
```

Note: Because of existing Access Control implementation, when OpenDJ SSO password is changed, all VMs must be restarted, to start using the new password.

This procedure involves downtime that depends on the deployment size. The procedure involves a rolling over LITP plan for services and scripting clusters and the duration of the plan varies depending on the deployment size.

When the password is changed, enter the new password into the COM_INF_LDAP_ADMIN_ACCESS parameter in the SED - preferably directly after the password change procedure, as the change affects subsequent ENM upgrades.

Prerequisites

— Root access to Management Server (MS-1).

— SED is available for updates.

Steps

1. Take a snapshot of the system.

   See Create ENM Snapshot on page 23.

2. Log on the `ENM MS` as the `litp-admin` user and switch to the root user.

3. Change directory.

   ```
   [root@ms-1]# cd /opt/ericsson/opendj/
   ```

4. Run the script.

   ```
   [root@ms-1]# sh change_config_sso_password.sh
   ```

5. Enter the following information to update the password in `OpenDJ`.

   — Current SSO `OpenDJ` password

   — New password which fulfills the following credentials:

   The following are the password policies described in the document ENM Identity and Access Management System Administrator Guide, Reference [1]:

   — Password must have at least eight characters.

   — Password must contain at least one lower case alpha character.

   — Password must contain at least one upper case alpha character.

   — Password must contain at least one numeric character.

   — Password must not contain: username, first name, or last name.

   — Password can contain special characters (non-alphanumeric characters).

   — Only hyphen (-), underscore (_), and period (.) are allowed in password.

   — The system asks if the password has to be changed. If so, click y or n if you resign.

   Repeat the new password and then confirm the password change.

   Result: The following message is displayed on successful completion of the command: `Password was changed successfully`.

If the new password does not comply with the password policies, the change is rejected.

The SSO `OpenDj` password is updated. Log files are on MS-1 in the following location: `/var/log/opendj`.

Note: After the password change, it is also important to enter the new password into the `COM_INF_LDAP_ADMIN_ACCESS` parameter in the SED - preferably directly after the password change procedure, as the change affects subsequent ENM upgrades.

6. Execute the following commands.

   These commands modify the yum repositories so that when the LITP plan is generated it contains rolling over node tasks for services.

```
[root@ms-1]# cd /var/www/html/ENM_services/
[root@ms-1]# touch *.rpm
[root@ms-1]# yum clean all && createrepo .
```

7. Create and run the LITP plan.

```
[root@ms-1]# litp create_plan
[root@ms-1]# litp show_plan
[root@ms-1]# litp run_plan
```

8. Monitor the progress of the plan and wait for it to complete.

```
[root@ms-1]# /opt/ericsson/enminst/bin/monitor_plan.sh
```

9. Remove the snapshot taken in step 1 once the procedure has completed successfully. See Remove ENM Snapshot on page 24.

   Note: If the procedure does not complete successfully, restore the snapshot taken in step 1.

   For detailed instructions about restoring snapshots, see the *Restore the System Using Snapshots* section in the document ENM Upgrade Instructions, Reference [9].

8.3.4 Handling of User Password

A user password must follow defined password policies:

— Password complexity

— Force password change

— Password lockout

Potential Security Risk

A user must not store password in browser, cache, and files by using `Autocomplete` features to protect ENM system from unauthorized access.

8.3.5 How to Change Root Passwords for OpenIDM

A root user can update admin passwords in OpenIDM, by changing openidm_admin_password in `global.properties` file.

These hardening steps apply to physical deployment only.

Prerequisites

User must have root access to Management Server (`MS-1`) and Service Cluster (`svc`).

Steps

1. Log on the ENM MS (MS-1) as the `litp-admin` user and switch to the root user.
2. Go to the specified directory.

   ```
   cd /opt/ericsson/openidm/
   ```

3. Run the following script:

   ```
   sh change_openidm_password.sh
   ```

4. Enter current `OpenIDM` password when prompted.

   `Please provide current password:`

5. Insert a new password which fulfills with the following criteria:

   * Password must have at least eight characters.

   * Password must contain at least one lower case alpha character.

   * Password must contain at least one upper case alpha character.

   * Password must contain at least one numeric character.

   * Password must not contain: username, first name, or last name.

   * Password can contain special characters (non-alphanumeric characters).

However, only hyphen (-), underscore (_), and period (.) are allowed in password.

6. Confirm new password when a confirmation message is displayed.

   The following message is displayed on successful completion of the command:

   ```
   Password was changed successfully
   ```

   It is important to change `Openidm Admin Password` in the SED to reflect the new password.

7. Log on the `SVC`.

8. Restart `OpenIDM`.

   Result: After `OpenIDM` is restarted, the new password is active.

Results

```
[root@atrcxb3347-1 ~]# hagrp -offline Grp_CS_svc_cluster_openidm -any         -
 after  -offline  wait for 10 sec
[root@atrcxb3347-1 ~]# virsh undefine openidm
[root@atrcxb3347-1 ~]# hagrp -online Grp_CS_svc_cluster_openidm -any
```

Note: `/var/log/openidm`

The root passwords in `OpenIDM` are updated.

Changes are rejected if the new password does not comply with the password policies as outlined in the log files are on `MS-1` in the document ENM Identity and Access Management System Administrator Guide, Reference [1].

8.3.6 Keep up to Date Adobe Flash Player

An instance of Adobe Flash Player comes with the ENM system.

After ENM installation, it is recommended to look for the most up-to-date version or security patches available from Adobe and download or apply to your local deployment. This ensures that your Player is up-to date with the most recent security patches.

8.3.7 User Session Security

> The user session is managed by ENM SSO application generating session cookies returned back to user client/browser.

The current setting of the session cookies consists of the following attributes:

Attribute	Description	Value
Secure	Allows the Access Manager cookie to be set in a secure mode in which the browser only returns the cookie when a secure protocol such as HTTP(S) is used.	true
HttpOnly	HttpOnly cookies are meant to be transmitted only over HTTP and HTTPS, and not through non-HTTP methods, such as JavaScript functions.	true
Path	Specifies that a cookie is sent to the URL designated in the path. Specify any string representing a path on the server. A slash (/) indicates root directory.	/

No further settings are required.

Note: The application can also store non-session cookies into the user browser (for example, "ssocookie"), used for internal status information. Since they do not transport any sensitive information, this hardening setting can be not applied.

8.3.8 How to Set Single User Session Quota Constraint

This feature consists to enable and disable the Single User Session Quota Constraint at system wide.

The constraint has been introduced to allow just one active session per user at the same time, for all ENM users.

By default, the constraint is disabled.

Once the constraint is enabled, when a new authentication by a specific user is performed (via UI, NBI, Scripting), all user session tokens previously created by the same user are invalidated.

As a consequence, any request performed providing the invalidated tokens to access a protected resource is rejected.

Note:

— Warning: When Single User Session Constraint is enabled, if logging to ENM with an account already used by a running script or FMX rule, the execution of the script or rule is interrupted. SSH/SFTP connections previously opened are not affected and remain active (they are not closed or reset), but any script or rule running through them is interrupted due to invalid token.

— Warning: When Single User Session Constraint is enabled, if logging to ENM with an account already logged in by an active UI session in a WEB browser, the previous UI session execution is interrupted and UI automatically redirects user to login page, due to invalid token.

This is applicable also when ENM UI session is launched first for a given user and SSH session opened for the same user, then ENM UI session logs out.

When enabled, the restriction is applied to all authentication methods: UI, NBI, Scripting.

This configuration can be done through PIB parameters using the `config.py` command script.

8.3.8.1 Configure the Single User Session Quota Constraint

To enable the single user session quota constraint, the `enabledSessionConstraint` parameter must be configured. It is a Boolean flag to enable or disable the Single Session Quota Constraint.

The root user can change the value using the Platform Integration Bridge (PIB) script to configure the single user session quota constraint.

Prerequisites

SSO and SECSERV services must be up and running.

Steps

1. Connect to the server (MS for physical environment or EMP for cloud environment), following the instructions in the section *Connect to a Virtual Machine* in ENM System Administrator Guide, Reference [4].
2. Find the SSO VM names.

   For physical environment, run the command:

   ```
   # grep sso /etc/hosts
   ```

   For cloud environment, run the command:

   ```
   # consul members | grep sso
   ```

3. Get the current system setting.

   Connect to one of the SSO VMs as root user and run the following command using one of the SSO VM names found in step 2, adding `:8080` as the value of the `app_server_address parameter`:

   ```
   # /opt/ericsson/PlatformIntegrationBridge/etc/config.py read --name=enableSe
   ssionConstraint --app_server_address=security-sso-0:8080
   ```

   If the returned value is false, the constraint is disabled.

   If the returned value is true, the constraint is enabled.

4. Enable Single User Session Quota Constraint.

   Run the command:

   ```
    # /opt/ericsson/PlatformIntegrationBridge/etc/config.py update --name=enabl
   eSessionConstraint --value=true --app_server_address=security-sso-0:8080
   ```

5. Disable Single User Session Quota Constraint.

   Run the command:

   ```
   # /opt/ericsson/PlatformIntegrationBridge/etc/config.py update --name=enable
   SessionConstraint --value=false --app_server_address=security-sso-0:8080
   ```

8.3.9 FMX Hardening

For steps to be taken for FMX hardening, follow the instructions described in the section *FMX Redis Cluster Security* of the document ENM Monitoring System Administrator Guide, Reference [2].

8.3.10 Apache Hardening

> ENM embeds few Apache Web Servers instances depending by the different deployment flavors.

In LITP-based deployments, it can be found in:

— Management Server physical machine

— HTTPD VMs.

In OpenStack based deployments, it can be found in:

— VNF-LCM VM

— HTTPD VMs.

Installations are in the standard location and all these instances are already hardened by default.

Additional configuration can be added to disable fully HTTP TRACE and TRACK methods, but because of the volatile nature of the VMs, the configuration is repeated in case of Upgrade or HA events.

See http://access.redhat.com/solutions/198813.

8.4 Logging Hardening

The logging hardening activities are grouped as follows:

— Logging configuration

— Auditing

— Time synchronisation

8.4.1 Logging Configuration

— Security logging is on by default.

— Access to log files is restricted by default.

— All log files are configured with detailed time stamps.

8.4.2 Auditing

Security and system auditing is enabled by default.

This auditing logs connections and failed connection attempts.

8.4.3 Time Synchronization

A default NTP plug-in is supplied and can be pointed at any external secure server.

8.5 Network and IP Traffic Hardening

The network-related and IP traffic-related hardening activities are grouped as follows:

— Network configuration

— Routing configuration

- Host-based firewall configuration
- Securing services
- IPsec configuration

8.5.1 Network Configuration

ENM can be used to configure certain network capabilities that strengthen the security of the overall Ericsson network solution.

Such capabilities are treated as features and product documentation must be considered to understand to what extent they can be used in any particular ENM release.

8.5.2 Routing Configuration

ENM VLAN layout comes pre-configured in production.

No additional configuration steps are required.

8.5.3 Host-based Firewall Configuration

ENM firewalls come pre-configured in production.

No additional configurations are done.

8.5.4 Securing Services

ENM services come pre-configured in production.

No additional security measures are taken.

8.5.5 IPSec Configuration

ENM system does not support IPSec configuration within its own infrastructure.

8.6 Configure AMOS Using Global Moshellrc File

> This section describes the changes to `Global Moshellrc` file for the described scenarios.

Prerequisites

No prerequisites.

Steps

If Port 22 is blocked in ENM Environment, do the following.

1. Log on Linux Management Server (LMS) for physical deployments or log on VNF-LAF for cloud deployments.
2. Log on the AMOS VM.
3. Read the values of `smrs_sftp_securePort` and of `smrs_sftp_port_partition_enable`.

   For physical environment:

   ```
   cat /ericsson/tor/data/global.properties | grep -e smrs_sftp_securePort -e s →
   mrs_sftp_port_partition_enable
   ```

   For cloud environment:

   ```
   /usr/bin/consul kv get -recurse | grep -i -e smrs_sftp_securePort -e smrs_sf →
   tp_port_partition_enable
   ```

4. Do the following if the value of `smrs_sftp_securePort` is different from 22 and the value of `smrs_sftp_port_partition_enable` is true.

   a. Log on any AMOS VM as root user.

   b. Open the `moshellrc` file:`/home/shared/common/moshell/moshellrc`.

      If `export_port` property is present in the `moshellrc` file, change the value of `export_port` property with the value of `smrs_sftp_securePort` as in the following.

      If `export_port` property is not present, append the value of `export_port` property in the `moshellrc` file as follows:

      ```
      export_port=<value of smrs_sftp_securePort>
      ```

If Port 22 is enabled (Not Blocked) after upgrade, do the following.

5. Make sure that the `export_port` property entry is removed from the `moshellrc` file: `/home/shared/common/moshell/moshellrc`.

8.7 VNX Hardening

8.7.1 SSL/TLS Protocol Triple-DES Information Disclosure Vulnerability

Dell_EMC support is recommended to perform the procedure outlined in the document VNX: CVE-2016-2183 - SSL/TLS Protocol Triple-DES Information Disclosure Vulnerability, Reference [7].

This procedure requires a reboot of the SP management server, but it does not affect service to any host connected to the storage.

Note: This procedure must be run during a maintenance window.

8.7.2 SSL Certificate Cannot Be Trusted and SSL Self-Signed Certificate

The section outlines the steps to perform when using either CA signed SHA-2 certs or self-signed SHA-2 certs. SHA-1 certs are not used, all new CA certs used are SHA-2 by default.

SSL certificate from a recognized Certificate Authority must be installed on all Storage Processors to correct the issue.

For CA signed SHA-2 certs, to add or change an SSL certificate on a Storage Processor, one of the following procedures described in the document Security Configuration Guide for VNX, Reference [8], must be run:

— *Adding or changing a Storage Processor SSL certificate using a web browser.*

— *Adding or changing a Storage Processor SSL certificate using openssl.*

Note: These procedures are applicable for VNX2 and all new CA certs are SHA-2.

For self-signed SHA-2 certs, to add or change an SSL certificate on a Storage Processor, follow the procedures described in the section Set Signature Algorithm on Unisphere to SHA-2 on page 35.

8.7.3 Set Signature Algorithm on Unisphere to SHA-2

The procedure must be run from the ENM MS and for both SPA and SPB IPs.

Prerequisites

No Prerequisites.

Steps

1. Create working directory and switch to it.

   a. `mkdir /var/tmp/vnx_hardening`

b. `cd /var/tmp/vnx_hardening`

2. Create key.

```
openssl genrsa -des3 -passout pass:<PASSWORD> -out <VNX_ID_and_SP>.key 2048
```

Table 1

<PASSWORD>	The password for the generated key.
<VNX_ID_and_SP>	The VNX name with either SPA or SPB appended. For example, VNX-120spa.

3. Create certificate request.

```
openssl req -new -sha256 -key <VNX_ID_and_SP>.key -passin pass:<PASSWORD> -o
ut <VNX_ID_and_SP>.csr -days 1825 -subj '/CN=<SP_IP>/'
```

Table 2

<VNX_ID_and_SP>	Key file created in step 2.
<PASSWORD>	The password for the generated key.
<SP_IP>	IP address of storage processor A or B.

4. Create certificate.

a.
```
openssl x509 -in <VNX_ID_and_SP>.csr -sha256 -out <VNX_ID_and_SP>.crt -
req -signkey <VNX_ID_and_SP>.key -days 1825
```

b. Enter password for the key, created in step 2.

Table 3

<VNX_ID_and_SP>.key	Key file created in step 2.
<VNX_IS_and_SP>.csr	Certificate request file created in step 3.

5. Verify that certificate is SHA-2.

a.
```
openssl x509 -in <VNX_ID_and_SP>.crt -noout -text
```

b. Verify that the Signature Algorithm is `sha256WithRSAEncryption`.

6. Create package for certificate and private key.

```
openssl pkcs12 -export -in <VNX_ID_and_SP>.crt -inkey <VNX_ID_and_SP>.key -o
ut <VNX_ID_and_SP>.pfx -passin pass:<PASSWORD> -passout pass:<PASSWORD>
```

7. Import certificate to VNX.

   a.
   ```
   /opt/Navisphere/bin/naviseccli -h <SP_IP> -user <SAN_USER> -scope 0 -pa
   ssword <SAN_PASSWORD> security -pkcs12upload -file <VNX_ID_and_SP>.pfx
   -passphrase <PASSWORD>
   ```

   b. If prompted to accept the certificate, select `[2] Accept and Store`.

   Table 4

<SP_ID>	IP address of storage processor A or B.
<SAN_USER>	Username for the VNX admin.
<SAN_PASSWORD>	Password for the specified VNX user.
<VNX_ID_and_SP>.pfx	File created in Step 6.
<PASSWORD>	The password for the generated key.

8. Verify that the Signature Algorithm is on `Unisphere`.

   a.
   ```
   echo | openssl s_client -showcerts -connect <SP_IP>:443 2>/dev/null | o
   penssl x509 -inform pem -noout -text
   ```

   b. Verify that the Signature Algorithm is `sha256WithRSAEncryption`.

   Table 5

<SP_IP>	IP address of storage processor A or B.

9. Remove the working directory.

   ```
   rm -rf /var/tmp/vnx_hardening
   ```

10. Repeat steps from 1 to 9 for all Storage Processors.

9 Hardening before Upgrade

This section outlines hardening activities that need to be taken before upgrade of the ENM system.

9.1 Enable Usage of Port 22

> This task describes the rollback procedure to unblock the port 22.

Port 22 can be enabled for SSH/SFTP communication from node to ENM.

— ENM system must be upgraded with the following parameters in the SED file:

```
smrs_sftp_port_partition_enable = false

smrs_sftp_securePort = 22
```

— Firewall configurations between the node and ENM SBI must be updated using the steps as follows.

Prerequisites

System must be up and running with port 22 being prohibited.

Steps

1. Get ENM SBI public IP interface details to configure Firewall.
    a. Log on the Linux Management Server (LMS) for physical deployments or log on VNF-LAF for cloud deployments
    b. Collect all the public IP interfaces and Public VIP IP addresses (include CM_VIP public IPs if they are blocked on port 22 using firewalls) from `global.properties` to configure the firewalls.
2. Get configured SFTP port.
    a. Log on the LSM for physical deployments or log on VNF-LAF for cloud deployments.
    b. Get the configured SFTP port.

    Run the command:

    ```
    cat /ericsson/tor/data/global.properties | grep -e smrs_sftp_secure →
    Port
    ```

3. Unblock the port 22 for all the public IP Interfaces and Public VIP IP addresses obtained in step 1.

4. Change the SED file and upgrade the ENM system.

   The SED file must be changed with the following parameters:

   ```
   smrs_sftp_port_partition_enable = false
   smrs_sftp_securePort = 22
   ```

   The ENM system is upgraded with the modified SED file. After the successful upgrade, the further communication cannot be performed on Configurable Port.

10 Hardening after Upgrade

This section outlines hardening activities that need to be taken after upgrade of the ENM system.

10.1 Configure AMOS Using Global Moshellrc File

> This section is used to verify AMOS configuration after upgrade using global Moshellrc file.

Follow the steps described in section Configure AMOS Using Global Moshellrc File on page 33.

11 Node Hardening Checklist

V	Hardening Activity	Comments
	Only required RPMs are installed.	
	Only required services are running.	
	Only relevant processes are running.	
	Only required Cron jobs are running.	
	Unnecessary user accounts are removed.	
	No unnecessary SUID or SGID programs.	
	Remote root logons are disabled.	
	SELinux is enabled.	
	X-Windows is not in use.	
	Mount points are exposed to minimal list of clients.	
	Latest security patches are installed.	
	Logon banner is present.	
	Password aging is configured.	
	Idle time-out is configured.	
	Strong passwords are enforced.	
	Accounts are locked after repeated logon attempts.	
	Remote logon is by SSH only.	
	Firewall rules are configured.	
	Access to log files is restricted.	
	Automatic log file rotating is configured.	
	Security auditing is enabled.	
	Source routing is disabled.	
	Key pair files are secured.	
	NTP server is secure.	
	Grub password is protected.	
	All development tools are removed.	
	Testing, vulnerability analysis, debugging tools.	
	Backdoors and sniffers.	

References

[1] ENM Identity and Access Management System Administrator Guide, 2/1543-aom 901 151-1 Uen

[2] ENM Monitoring System Administrator Guide, 1/1543-aom 901 151-2 Uen

[3] ENM Site Engineering Document, 1/1057-AOM 901 151

(Available from local Ericsson Support)

[4] ENM System Administrator Guide, 1/1543-aom 901 151 Uen

[5] ENM VM Customization (Available from Local Ericsson Support), 1/1543-CRA 119 2165

[6] LITP Node Hardening Instructions, 2/1531-CSA 113 110

[7] VNX: CVE-2016-2183 - SSL/TLS Protocol Triple-DES Information Disclosure Vulnerability, https://support.emc.com/kb/493924

[8] Security Configuration Guide for VNX, https://www.emc.com/collateral/TechnicalDocument/docu48491.pdf

[9] ENM Upgrade Instructions, 1/153 72-AOM 901 151

(Available from local Ericsson Support)