###### Access CLI interface

***Objective:***

This test case verifies that the node with SAOS 10.x is reachable from the network for IP management, and to open the CLI for manual CLI-based configuration of SAOS 10.x box.

***Procedure:***

 Login to system through console port. Provision a static IP or check if any DHCP IP has been assigned to local management interface mgmtbr0.

#disable DHCP

dhcp-client client mgmtbr0 admin-enable false

#setup static IP for mgmtbr0

oc-if:interfaces interface mgmtbr0 ipv4 address address x.x.x.x config ip x.x.x.x prefix-length 20

#Setup static route to default gateway

rib vrf default ipv4 10.0.0.0/8 next-hop x.x.x.x description "default gw"

* Display the IP interfaces.

show ip interfaces brief

* Login to UI using the management IP you checked in the previous step:

ssh [diag@x.x.x.x](mailto:diag@x.x.x.x)

* + Replace x.x.x.x with IP address of the node.
  + username: diag password: ciena123
  + ~~a “-p 830” parameter for port 830 is only needed for SAOS 10.2 or earlier.~~
  + You will be logged in to the CLI
  + You can now access the configuration interface with typing
    - config

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Applying license – Primary License Server

***Objective:***

Note that the data and time set is required for the application of the license. This step is to apply license to the installed SAOS 10.x software. This will activate the features and ports will be controlled by SAOS 10.x.

***Procedure:***

* Pick one of the lab San Jose or lab Ottawa servers
* config

# license-management-config license-server-config 10.33.80.94

or

# license-management-config license-server-config 10.182.66.137 # exit

# exit

* Confirm the registration and license management state
* show license

You should see an output similar to following

+ License Management State +

| Name | Value |

+ + +

| License-server-state: | |

| Ciena-licensing:server-port | 7071 |

| Hostname | 10.182.66.137 |

| Server-oper-state | enabled |

| License-client-state: | |

|  |  |  |  |
| --- | --- | --- | --- |
| | | License-feature: | | | | |
| | | Source | | served | | |
| | | Feature-name | | SAOS-Sync | | |
| | | Version | | 1.0 | | |
| | | Description | | lt=perpetual|pn=S75-LIC-5162SYNC-P|p=SAOS SYNCHRONIZATION SOFTWARE LICENSE | | |
| | | Properties: | | | | |
| | | Count | | 3 | | |
| | | Notice | | {product.Notice} | | |
| | | Host-id | | floating | | |
| | | State | | valid | | |
| | | Acquired-count | | 1 | | |
| | | Expiration: | | | | |
| | | Expiration-date | | 16-Nov-2018 | | |
| | | Last-renewal-date | | Fri Nov 9 06:09:38 2018 | | |
| | | Time-remaining | | 6 days, 23 hours, 49 mins, 13 secs | | |
| | | Type | | subscription | | |
| | | Issuer: | | | | |
| | | Issuer-name | | Ciena | | |
| | | License-feature: | | | | |
| | | Source | | served | | |
| | | Feature-name | | SAOS-Security | | |
| | | Version | | 1.0 | | |
| | | Description | | lt=perpetual|pn=S75-LIC-5162SEC-P|p=SAOS SECURITY SOFTWARE LICENSE, PERPETUAL | | |
| | | Properties: | | | | |
| | | Count | | 3 | | |
| | | Notice | | {product.Notice} | | |
| | | Host-id | | floating | | |
| | | State | | valid | | |
| | | Acquired-count | | 1 | | |
| | | Expiration: | | | | |
| | | Expiration-date | | 16-Nov-2018 | | |
| | | Last-renewal-date | | Fri Nov 9 06:09:38 2018 | | |
| | | Time-remaining | | 6 days, 23 hours, 49 mins, 11 secs | | |
| | | Type | | subscription | | |
| | | Issuer: | | | | |
| | | Issuer-name | | Ciena | | |
| | | License-feature: | | | | |
| | | Source | | served | | |
| | | Feature-name | | SAOS-MPLS | | |
| | | Version | | 1.0 | | |
| | | Description | | lt=perpetual|pn=S75-LIC-5162MPLS-P|p=SAOS MPLS SOFTWARE LICENSE, PERPETUAL | | |
| | | Properties: | | | | |
| | | Count | | 3 | | |
| | | Notice | | {product.Notice} | | |
| | | Host-id | | floating | | |
| | | State | | valid | | |
| | | Acquired-count | | 1 | | |
| | | Expiration: | | | | |
| | | Expiration-date | | 16-Nov-2018 | | |
| | | Last-renewal-date | | Fri Nov 9 06:09:38 2018 | | |
| | | Time-remaining | | 6 days, 23 hours, 49 mins, 9 secs | | |
| | | Type | | subscription | | |
| | | Issuer: | | | | |
| | | Issuer-name | | Ciena | | |
| | | License-feature: | | | | |
| | | Source | | served | | |
| | | Feature-name | | SAOS-BaseOS\_AdvEth\_OAM | | |
| | | Version | | 1.0 | | |
| | | Description | | lt=perpetual|pn=S75-LIC-5162EO-P|p=SAOS BASE OS, ADVANCED ETHERNET & OAM SOFTWARE LICENSE, PERPETUAL | | |
| | | Properties: | | | | |
| | | Count | | 3 | | |
| | | Notice | | {product.Notice} | | |
| | | Host-id | | floating | | |
| | | State | | valid | | |
| | | Acquired-count | | 1 | | |
| | | Expiration: | | | | |
| | | Expiration-date | | 16-Nov-2018 | | |
| | | Last-renewal-date | | Fri Nov 9 06:09:38 2018 | | |
| | | Time-remaining | | 6 days, 23 hours, 49 mins, 7 secs | | |
| | | Type | | subscription | | |
| | | Issuer: | | | | |
| | | Issuer-name | | Ciena | | |

|  |  |  |  |
| --- | --- | --- | --- |
| |  | | License-feature:  Source | |  | served | |  | |
| | | Feature-name | | SAOS-Adv\_100G | | |
| | | Version | | 1.0 | | |
| | | Description | | lt=perpetual|pn=S75-LIC-5162100G-P|p=SAOS 100G SOFTWARE LICENSE, PERPETUAL | | |
| | | Properties: | | | | |
| | | Count | | 3 | | |
| | | Notice | | {product.Notice} | | |
| | | Host-id | | floating | | |
| | | State | | valid | | |
| | | Acquired-count | | 1 | | |
| | | Expiration: | | | | |
| | | Expiration-date | | 16-Nov-2018 | | |
| | | Last-renewal-date | | Fri Nov 9 06:09:38 2018 | | |
| | | Time-remaining | | 6 days, 23 hours, 49 mins, 5 secs | | |
| | | Type | | subscription | | |
| | | Issuer: | | | | |
| | | Issuer-name | | Ciena | | |
| | | Registration-id | | f6f3fd3233c3198e2d2af8acb60f46cbf0e743ea | | |
| | | Oper-state | | enabled | | |
| + |  | + | + |

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Applying license – Primary License Server

***Objective:***

Note that the data and time set is required for the application of the license. This step is to apply license to the installed SAOS 10.x software. This will activate the features and ports will be controlled by SAOS 10.x.

***Procedure:***

* Pick one of the lab San Jose or lab Ottawa servers
* config

# license-management-config license-server-config 10.33.80.94

or

# license-management-config license-server-config 10.182.66.137 # exit

# exit

* Confirm the registration and license management state
* show license

You should see an output similar to following

+ License Management State +

| Name | Value |

+ + +

| License-server-state: | |

| Ciena-licensing:server-port | 7071 |

| Hostname | 10.182.66.137 |

| Server-oper-state | enabled |

| License-client-state: | |

|  |  |  |  |
| --- | --- | --- | --- |
| | | License-feature: | | | | |
| | | Source | | served | | |
| | | Feature-name | | SAOS-Sync | | |
| | | Version | | 1.0 | | |
| | | Description | | lt=perpetual|pn=S75-LIC-5162SYNC-P|p=SAOS SYNCHRONIZATION SOFTWARE LICENSE | | |
| | | Properties: | | | | |
| | | Count | | 3 | | |
| | | Notice | | {product.Notice} | | |
| | | Host-id | | floating | | |
| | | State | | valid | | |
| | | Acquired-count | | 1 | | |
| | | Expiration: | | | | |
| | | Expiration-date | | 16-Nov-2018 | | |
| | | Last-renewal-date | | Fri Nov 9 06:09:38 2018 | | |
| | | Time-remaining | | 6 days, 23 hours, 49 mins, 13 secs | | |
| | | Type | | subscription | | |
| | | Issuer: | | | | |
| | | Issuer-name | | Ciena | | |
| | | License-feature: | | | | |
| | | Source | | served | | |
| | | Feature-name | | SAOS-Security | | |
| | | Version | | 1.0 | | |
| | | Description | | lt=perpetual|pn=S75-LIC-5162SEC-P|p=SAOS SECURITY SOFTWARE LICENSE, PERPETUAL | | |
| | | Properties: | | | | |
| | | Count | | 3 | | |
| | | Notice | | {product.Notice} | | |
| | | Host-id | | floating | | |
| | | State | | valid | | |
| | | Acquired-count | | 1 | | |
| | | Expiration: | | | | |
| | | Expiration-date | | 16-Nov-2018 | | |
| | | Last-renewal-date | | Fri Nov 9 06:09:38 2018 | | |
| | | Time-remaining | | 6 days, 23 hours, 49 mins, 11 secs | | |
| | | Type | | subscription | | |
| | | Issuer: | | | | |
| | | Issuer-name | | Ciena | | |
| | | License-feature: | | | | |
| | | Source | | served | | |
| | | Feature-name | | SAOS-MPLS | | |
| | | Version | | 1.0 | | |
| | | Description | | lt=perpetual|pn=S75-LIC-5162MPLS-P|p=SAOS MPLS SOFTWARE LICENSE, PERPETUAL | | |
| | | Properties: | | | | |
| | | Count | | 3 | | |
| | | Notice | | {product.Notice} | | |
| | | Host-id | | floating | | |
| | | State | | valid | | |
| | | Acquired-count | | 1 | | |
| | | Expiration: | | | | |
| | | Expiration-date | | 16-Nov-2018 | | |
| | | Last-renewal-date | | Fri Nov 9 06:09:38 2018 | | |
| | | Time-remaining | | 6 days, 23 hours, 49 mins, 9 secs | | |
| | | Type | | subscription | | |
| | | Issuer: | | | | |
| | | Issuer-name | | Ciena | | |
| | | License-feature: | | | | |
| | | Source | | served | | |
| | | Feature-name | | SAOS-BaseOS\_AdvEth\_OAM | | |
| | | Version | | 1.0 | | |
| | | Description | | lt=perpetual|pn=S75-LIC-5162EO-P|p=SAOS BASE OS, ADVANCED ETHERNET & OAM SOFTWARE LICENSE, PERPETUAL | | |
| | | Properties: | | | | |
| | | Count | | 3 | | |
| | | Notice | | {product.Notice} | | |
| | | Host-id | | floating | | |
| | | State | | valid | | |
| | | Acquired-count | | 1 | | |
| | | Expiration: | | | | |
| | | Expiration-date | | 16-Nov-2018 | | |
| | | Last-renewal-date | | Fri Nov 9 06:09:38 2018 | | |
| | | Time-remaining | | 6 days, 23 hours, 49 mins, 7 secs | | |
| | | Type | | subscription | | |
| | | Issuer: | | | | |
| | | Issuer-name | | Ciena | | |

|  |  |  |  |
| --- | --- | --- | --- |
| |  | | License-feature:  Source | |  | served | |  | |
| | | Feature-name | | SAOS-Adv\_100G | | |
| | | Version | | 1.0 | | |
| | | Description | | lt=perpetual|pn=S75-LIC-5162100G-P|p=SAOS 100G SOFTWARE LICENSE, PERPETUAL | | |
| | | Properties: | | | | |
| | | Count | | 3 | | |
| | | Notice | | {product.Notice} | | |
| | | Host-id | | floating | | |
| | | State | | valid | | |
| | | Acquired-count | | 1 | | |
| | | Expiration: | | | | |
| | | Expiration-date | | 16-Nov-2018 | | |
| | | Last-renewal-date | | Fri Nov 9 06:09:38 2018 | | |
| | | Time-remaining | | 6 days, 23 hours, 49 mins, 5 secs | | |
| | | Type | | subscription | | |
| | | Issuer: | | | | |
| | | Issuer-name | | Ciena | | |
| | | Registration-id | | f6f3fd3233c3198e2d2af8acb60f46cbf0e743ea | | |
| | | Oper-state | | enabled | | |
| + |  | + | + |

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### User Configurable Reg-Id

A device is licensed with license server using 40 characters registration id by default.

What new we are getting in saos 10.7.1 is that we will be able to change the registration ID to any customized value on the device which is used for licensing.

The main advantage of this feature is that we will be easily able to identify the clients connected to license server.

***Objective:***

Objective is to change the Reg-Id of the node to the customized value.

***Procedure:***

Below is the command with which we can configure the customized reg-id on the node. Max characters allowed under this section is 30.

Text

Description automatically generated

It can be noted that once the customzed reg id is defined, the 8 chars device Id is automatically appended to the reg-id. This is the hash value of chassis serial no and is basically added to keep the reg-Id unique.

In case we unconfigure the customized reg id on the device,the device rolls back to its previuos 40 chars reg id.

One thing worth noting here is that this functionality is only applicable when licensing using server and will not be applicable when licensing using file.

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Manage Active CLI sessions

In saos 10.x release , normally four or six concurrent sessions are allowed to login using CLI based on the system’s capability. When the system detects more than allowed concurrent logins, CLI enters the limited mode.

In the limited mode, users can view session information but cannot view & make changes to the configuration, for example, configure OSPF.

In this case it becomes important to bring system out of limited mode.In order to bring the system out of the limited mode, new enhancement has been added in saos 10.7.1 release.What happens with this is that a user with super privileges can terminate one or more active CLI sessions which allows us to bump the unwanted user who is loggined.

***Objective:***

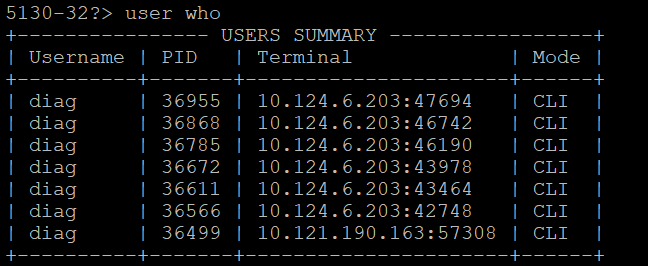
Objective is to manage multiple CLI session on 10.x device.

***Procedure:***

There are 2 steps using which we can kill the unwanted cli session on the node.

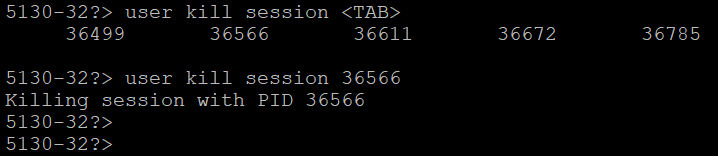
First is identifying which session do we need to kill, this can be done using user who.

**STEP1:-** Identify the session which is to be terminated



Once the session has been identified "use kill session " command in step 2 can be used to terminate that particular session.

**STEP 2 :-** Terminate the active session using process id



Few points to remember while accessing this functionality are ..

* User can terminate cli session regardless of whether the CLI is in limited mode. i.e user can kill other sessions even from limited mode as well.
* User has to have super priviledge to perform this functionality.
* User cannot terminate the current active session in which it is currently login.

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Reset to factory default

***Objective:***

The objective is to setup procedure to reset the node to factory default.

***Procedure:***

* From the cli, enter:

system reset factory-defaults

* You should see the node reboot. Once reboot is complete, all configuration on the node would have been removed. Please note, licenses would have to be re-applied.

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### ZTP

***Objective:***

Objective is to install SAOS 10.x with ZTP process. Network based ZTP process is useful when we want to ensure the same version of software is automatically installed on multiple nodes in the network. ZTP only allowed over VLAN 127, and untagged is not supported.

***Procedure:***

* Ensure you have DHCP environment setup is been done with either of
  + Option 66/67 to provide tftp server and filename of Command File
  + Option 125 to provide URL of Command Fil
* Ensure that the image you want to download is located on an HTTP/TFTP server
* Verify that the command file is located at the TFTP server and the config file is supplied
* Start the node if it is the first time it is being powered up
* Once the device boots up, Login to UI container using the management IP you checked in the previous step (default login/passwd displayed below):

ssh [diag@x.x.x.x](mailto:diag@x.x.x.x)

username: diag password: ciena123

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### SZTP

Ciena’s RFC-based Secure Zero Touch Provisioning (SZTP) enables rapid secure deployment of new platforms to the network through automatic configuration. The implementation and processes used with this feature are based on the Internet Engineering Task Force (IETF) RFC-8572, Secure Zero Touch Provisioning.

***Objective:*** Objective is to securely provision SAOS 10.x System using RFC 8572 Based Secure ZTP.

***Steps:***

* + - 1. Configure bootstrap Server with Bootstrap artifacts including on-boarding-info, NOS Image etc.
      2. Make sure System is configured with Golden config.
      3. Perform reset-to-golden-config on the system. Steps to create golden-config is given in Procedures section below.
      4. Execute ‘show ztp’ and Verify ‘ZTP State’ is ‘activating’.
      5. Executed ‘show software’ and Verify image downloading started successfully.
      6. Wait till the time when image is activated on the system. Check with ‘show software’

command.

* + - 1. Now Verify initial-configuration is replayed on the system successfully
      2. Verify ‘ZTP State’ is ‘Activated’ now in ‘show ztp’ command output.
      3. Verify System sends below Progress-Reports on bootstrap-server successfully. bootstrap-initiated

boot-image-installed-rebooting boot-image-complete bootstrap-complete

***Procedure:***

 Enter the following commands on CLI to install and configure PKIX certificates and create TLS Service Profile:

pkix-certificates install cert-name <sztp-cert-name> remote-file-uri

<client-cert-uri> cert-only false certpassphrase test login-id

<username> password <password>

pkix-ca install ca-cert-name DigiCert-CA remote-file-uri scp://[2620:11b:d0a2:f0f3::9b]/tmp/certs/ca.crt login-id <username> password <password>

pkix peer-auth-profiles peer-auth-profile <profile-name> check-ip- host false check-cert-expiry false checkfingerprint false periodic- reauthorization-max-interval <max-interval>

hello-params https-tls-profile tls-versions tls-version tls-1.2

hello-params https-tls-profile cipher-suites ciphersuite ecdhe-rsa- with-aes-256-gcm-sha384

hello-params https-tls-profile elliptic-curves ellipticcurve secp384r1

tls-service-profiles <tls-serivce-profile-name> tlsprofile- name

<tls-profile-name> tls-peer-auth-profilename <tls-peer-auth-profile- name> tls-certificate-name <cert-name>

* Use the following CLI command to configure rfc8572 based S-ZTP:

ztp ztp-type rfc8572 tls-service-profile <tls-serviceprofile-name> server-url <space separated list of serverip:port>

* Use the below command to create the golden configuration backup – the golden-config is a configuration that enables the node to initiate xZTP:

config backup golden-config

* Use the below command to start the SZTP process – by resetting to golden-config, xZTP process is automatically triggered.:

config reset golden-config

After the a few minutes, the new build should have been activated successfully. Execute a

“show software” to check the status of the new loaded software.

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

* + 1. **Verify Re-Install or Upgrade Software**

***Objective:***

Objective is to verify downloading, installation, and activation of software.

***Procedure:***

* Load installation is through ONIE – Open Network Install Environment
* After initial installation of a SAOS load on a box, you should be able to upgrade to another load without need to go back to ONIE.
* \*Following the example below and enter the following command to download the build

from user’s own URL – please note the URL below is for reference only:

software download url [http://x.x.x.x/valimar-snapshot/manifest/saos-10-05-01-](http://x.x.x.x/valimar-snapshot/manifest/saos-10-05-01-0096.yml) [0096.yml](http://x.x.x.x/valimar-snapshot/manifest/saos-10-05-01-0096.yml)

* After the a few minutes, the build should have downloaded successfully. Execute a “show software” to check the download status.
* Once the build has downloaded successfully, execute the command install to install the software.

software install package saos-10-05-01-0096 defer-activation

* \*Once installation is complete, activate the load to complete the upgrade.

software activate package saos-10-05-01-0096

* After the a few minutes, the build should have been activated successfully. Execute a

“show software” to check the status. You should see something like this:

5144-009> show software

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| +  | | Name | | | SOFTWARE STATE  Value | +  | | | |
| +  | | Current operation | +  | | idle | +  | | | |
| |  |  |  |  +  |  |  |  |  | | RPC Status  Running package version Package build info Active bootchain  Components: BIOS image  BOOT FPGA image ONIE image  cn\_alarm\_1 | |  |  |  |  +  |  |  |  |  | | idle  saos-10-05-01-0096  Wed Dec 02 03:16:15 2020  01-05-01-0096  0017  00.00.2a Ciena\_2019.02.01-0040  01-05-01-0096 | autouser | onxvpnjk23 | |  |  |  |  +  |  |  |  |  | |
| | | cn\_central-logger\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_cfm\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_cnfp\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_collectd\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_dataplane\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_dhcp-ctrl\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_dhcpl3relay\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_dns\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_dot1x\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_eoam\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_erps\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_feds\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_hal\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_ipservices\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_lacp\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_lldp\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_ntp\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_pkix\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_pon-ctrl\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_ppm\_1 | | | 01-05-01-0096 |  |  | | |

| cn\_rstp\_1 | 01-05-01-0096 |

| cn\_sat\_1 | 01-05-01-0096 |

| cn\_snmp-agent\_1 | 01-05-01-0096 |

| cn\_storage\_1 | 01-05-01-0096 |

| cn\_svcdirectory\_1 | 01-05-01-0096 |

| cn\_sync-hal\_1 | 01-05-01-0096 |

| cn\_sync\_1 | 01-05-01-0096 |

| cn\_system\_1 | 01-05-01-0096 |

| cn\_tdm\_1 | 01-05-01-0096 |

| cn\_telemetry\_1 | 01-05-01-0096 |

| cn\_twamp\_1 | 01-05-01-0096 |

| cn\_ui\_1 | 01-05-01-0096 |

| cn\_val-gui\_1 | 01-05-01-0096 |

| cn\_ztp\_1 | 01-05-01-0096 |

| xg\_xgrade-agent\_1 | 01-05-01-0096 |

+ + +

| Available packages: | |

**| saos-10-05-01-0096 | activated** |

+ + +

\*can combine the steps and use “software install” without the defer-activation parameter. “software install” will download, install and activate the load on the system in one step.

**Test Case Results:**

Passed: Yes No Verified by Date/Time Comments

###### Verify Manual network-based installation

***Objective:***

Objective is to install SAOS 10.x on a system, using the manual network-based installation.

***Procedure:***

* Login to system console port.
* When ONIE comes up it will try to find the resource for ZTP. If you want to specify the location of the installer file manually, which is different from what it might fetch from network installer, you should stop it:

ONIE:/ # onie-discovery-stop

* Then proceed with the manual installation from the installer file from http, tftp or ftp server.

ONIE:/ # onie-nos-install <http://x.x.x.x/installer.bin> ONIE:/ # onie-nos-install tftp://x.x.x.x/installer.bin ONIE:/ # onie-nos-install ftp://x.x.x.x/installer.bin

Replace x.x.x.x with IP address or the URL of where the image is residing. Here is an example:

ONIE:/ # onie-nos-install <http://x.x.x.x/valimar-> snapshot/17-12-00-0141/meta-onie-installer-dnx/meta\_01-00- 00-0181-core.bin

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Verify USB-based installation of SAOS 10.x

***Objective:***

Objective is to install SAOS 10.x on a system using USB-based method.

***Procedure:***

* Ensure that the format of your USB stick is FAT32 formatted.
* Ensure that the image you want is on the USB stick
* Ensure that the image is named “**onie-installer**”. This is important. Currently, the load name cannot be named anything else.
* Start the node if it is the first time it is being powered up, or follow the following steps otherwise
* Login to UI container using the management IP you checked in the previous step:

ssh [diag@x.x.x.x](mailto:diag@x.x.x.x)

username: diag password: ciena123

When ONIE comes up it will try to find the resource for ZTP. Wait for the installation to complete from here.

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Verify NTP or verify the date and time

***Objective:***

Setting date and time are required before application of licenses. Set NTP or date for Ciena SAOS 10.x using Linux commands. Proper data and time setup are required for license application.

***CLI NTP Procedure:***

* Establish a ssh connection to ValCLI

ssh [diag@X.X.X.X](mailto:diag@X.X.X.X)

password: ciena123

* Send the following config command
  + config

system ntp associations remote-ntp-server server-entry 10.33.80.21 admin-state enabled

* Check the NTP State with the following command
  + show ntp client
* The output would be something like:

+---------- NTP CLIENT STATE +

| Name | Value |

+ + +

| Admin State | enabled |

| Mode | polling |

| Polling Min Interval | 16 |

| Polling Max Interval | 16 |

| Auth Admin State | disabled |

| Synchronized | True |

| Delay | 62.161 |

| Offset | 0.006 |

| Jitter | 0.017 |

| Drift (PPM) | -4.485 |

+ + +

+--------- NTP CONFIGURED SERVERS +

| Address | Auth Key ID | Admin State |

+ + + +

| 10.33.80.21 | | enabled |

+ + + +

+ NTP OPER SERVERS

+

| Address | Auth Key ID | Server State | Server Condition | Auth State | Offset |

+ + + + +

+ +

| 10.33.80.21 | | reach | syspeer | none

| 0.006 |

+ + + + +

+ +

***Date & Time Set Procedure:***

* Login to UI using the management IP you checked in the previous step:

ssh [diag@x.x.x.x](mailto:diag@x.x.x.x)

username: diag password: ciena123

* Enter the following command to change the date and time on the system. This will only work if NTP is disabled:

config

system set clock 2018-11-03T18:39:00Z

* Show the system time:

5162-002> show clock

+ System Clock +

| Name | Value |

+ + +

| Current Time | 2018-11-03 18:39:03 UTC |

* To enable NTP, the manually set clock will be overwritten.

config

system ntp admin-state enabled

5162-002> show clock

+ System Clock +

| Name | Value |

+ + +

| Current Time | 2018-11-08 13:22:28 UTC |

+ + +

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

* + 1. **Configuration – Show running**

***Objective:***

Objective is to display the show running command

***Procedure:***

* On Valimar cli, display the configuration by issuing following command.
  + show running
* A list of configuration information is displayed in JSON-like format.
* The user can also list the provisioning information per feature basis. To do that, we use the following command to display the sections of the provisioning we can display:
  + show running section ?

5162-003> show running section <TAB>

ciena-bw-calculation-mode:bw-calculation-mode ciena-mef-fd:fds ciena-sync:sync

ciena-cfm:cfm-global-config ciena-mef-fp:fps ciena-tdm-global:tdm-global ciena-dhcp:dhcp-client ciena-mef-frame-to-cos-map:frame-to-cos-maps ciena-tls-service-

profile:tls-service-profiles

ciena-dhcpv6-client:dhcpv6-client ciena-mef-logical-port:logical-ports ciena-tls:hello-params ciena-eoam:eoam-global-config-status ciena-mef-mac-management:mac-management ciena-vrf:vrf

ciena-ieee-lag:agg-global ciena-mef-pfg-profile:pfg-profiles ciena-ztp:ztp ciena-ieee-lldp:lldp-global-config ciena-mpls:mpls ietf-alarms:alarms

ciena-ieee-rstp:rstp ciena-packet-ptp:ptps ietf-netconf-acm:nacm

ciena-isis:isis ciena-packet-xcvr:xcvrs mef-cfm:default-md-levels ciena-itut-g8032-draft:g8032-rings ciena-pkix:pkix openconfig-interfaces:interfaces

ciena-licensing:license-management-config ciena-ppm:ppm openconfig-platform:components

ciena-management-plane:management-plane ciena-rib:rib openconfig-system:system

ciena-mef-classifier:classifiers ciena-sat:sat openconfig-telemetry:telemetry- system

ciena-mef-cos-to-frame-map:cos-to-frame-maps ciena-sr:segment-routing

ciena-mef-egress-qos:egress-qos ciena-subsystem-resource:subsystems

* As an example, display the isis section of the provisioning file.
* show running section ciena-isis:isis

5162-003> show running section ciena-isis:isis ciena-isis:isis

instance

tag Section3

dynamic-hostname True net

49.FAFA.0101.8110.2162.00

level-type level-1 proto-ipv4

redistribute protocol

name static level level-1

fast-reroute level

level-type level-1 lfa

per-prefix-enable True ti-lfa

per-prefix-enable True

level

level-type level-2 lfa

per-prefix-enable True

ti-lfa

per-prefix-enable True

interfaces

interface

name if5

interface-type point-to-point

interface

name if10

interface-type point-to-point

interface

name if23

interface-type point-to-point

interface

name lb1

interface-type point-to-point

mpls-te

router-id 10.181.102.162 level-type level-1

cspf-flag True

segment-routing

enabled True

srgb

lower-bound 16000

upper-bound 23999

**Test Case Results:**

Passed: Yes No Verified by Date/Time Comments

###### Verify System Power Cycle will maintain the configuration

***Objective:***

To verify that SAOS 10.x on sytem maintains configuration and operation following a disruption to power.

***Procedure:***

* Login to UI container using the management IP you checked in the previous step:

ssh [diag@x.x.x.x](mailto:diag@x.x.x.x)

username: diag password: ciena123

* Then issue the reboot command below or power cycle the node.
  + system restart
* Once powered up verify that device can be reachable by management network, and login is re-enabled.
* Login to the box and confirm configuration is still in place.

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Create New User Account

***Objective:***

Setup a new user account to access the system.

***Procedure:***

* SAOS 10.1 supports two local user groups:
  + SYSTEM\_ROLE\_DIAG : The user has access to CLI, NETCONF, and also to Linux shell.
  + SYSTEM\_ROLE\_USER : The user has access to CLI and NETCONF.
* Enter the following command on CLI to create a new local user User1:

config

system aaa authentication users user **User1** config username User1 role SYSTEM\_ROLE\_USER password Password1

* Verify that the user has been created:

5162\_001> show aaa users

+ USER ACCOUNT TABLE +

| Username | Role | Sessions | Lockout |

+ + + + +

| diag | SYSTEM\_ROLE\_DIAG | | |

| user | SYSTEM\_ROLE\_USER | | |

| **User1** | SYSTEM\_ROLE\_USER | | |

+ + + + +

* Ensure that the user has been added to NACM group -otherwise provisioning by local user will not be allowed.
  + config
  + nacm groups group super user-name User1

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Create New User Account

***Objective:***

Setup a new user account to access the system.

***Procedure:***

* SAOS 10.1 supports two local user groups:
  + SYSTEM\_ROLE\_DIAG : The user has access to CLI, NETCONF, and also to Linux shell.
  + SYSTEM\_ROLE\_USER : The user has access to CLI and NETCONF.
* Enter the following command on CLI to create a new local user User1:

config

system aaa authentication users user **User1** config username User1 role SYSTEM\_ROLE\_USER password Password1

* Verify that the user has been created:

5162\_001> show aaa users

+ USER ACCOUNT TABLE +

| Username | Role | Sessions | Lockout |

+ + + + +

| diag | SYSTEM\_ROLE\_DIAG | | |

| user | SYSTEM\_ROLE\_USER | | |

| **User1** | SYSTEM\_ROLE\_USER | | |

+ + + + +

* Ensure that the user has been added to NACM group -otherwise provisioning by local user will not be allowed.
  + config
  + nacm groups group super user-name User1

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Management - Source IP

***Objective:***

Objective is to verify Source IP management IP. Source IP management address must be set on the system for proper communication with remote applications such as telemetry, radius, syslog etc..

***Procedure:***

* Create a loopback interface with **role of management**.
  + oc-if:interfaces interface lb1 config name lb1 cn-if:type loopback **role management**
  + oc-if:interfaces interface lb1 ipv4 addresses address 10.181.102.164 config ip 10.181.102.164 prefix-length 32
* Show the ip interface

5144-008> show ip int b

+ IP INTERFACES BRIEF

+

| | | | | Status | | Underlay |

| Interface | IP Address | VRF | Origin | Admin | Oper | Role | Binding |

+ + +

+

+ + + + +

| **mgmtbr0** | 10.181.37.142 | default | STATIC | **DOWN | DOWN** | management | -

|

| remote | unassigned | default | - | UP | UP | management | remote-fd |

| if21 | 172.18.1.1 | default | STATIC | UP | DOWN | data | VLAN4001 |

| if22 | 172.18.4.2 | default | STATIC | UP | UP | data | VLAN4004 |

| if23 | 172.18.5.1 | default | STATIC | UP | UP | data | VLAN4005 |

| **lb1** | 10.181.102.164 | default | STATIC **| UP | UP** | management | -

|

+ + +

+

+ + + + +

5144-008> show management-plane

+ DEFAULT SOURCE IP INTERFACE +

| Interface |

+ +

| |

+ +

* Now set the default source ip to loopback address just created.
  + management-plane default-source-ip interface lb1
* Show the management plane default source IP.

5144-008> show management-plane

+ DEFAULT SOURCE IP INTERFACE +

| Interface |

+ +

| lb1 |

+ +

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Syslog Setup

***Objective:***

Objective is to validate syslog server setup. This test is a continuation of the Source IP testcase.

***Procedure:***

* Enter the management IP on 10x node. The node in this testcase is in-band managed via a routable loopback interface “lb1”.
  + show ip interfaces brief

3928-003> show ip int b

+ IP INTERFACES BRIEF +

| | | | | Status | | Underlay |

| Interface | IP Address | VRF | Origin | Admin | Oper | Role | Binding |

+ + + + + + + + +

| mgmtbr0 | 10.181.35.227 | default | STATIC | DOWN | DOWN | management | - |

| remote | unassigned | default | - | UP | UP | management | remote-fd |

**| lb1 | 10.181.102.165 | default | STATIC | UP | UP | management | -** |

| if10 | 172.18.1.2 | default | STATIC | UP | UP | data | VLAN4001 |

| if9 | 172.18.2.1 | default | STATIC | UP | UP | data | VLAN4002 |

+ + + + + + + + +

* Setup the syslog server
  + syslog log-actions remote dest 10.181.65.17 admin-state enabled
* Validate the syslog setup on the node.

3928-003> show syslog

+--- REMOTE --+

| Admin-State |

+ +

| enabled |

+ +

+ DESTINATION +

| Server IP | Admin-State | Port | Facility | Severity | Custom prefix |

+ + + + + + +

| 10.181.65.17 | enabled | 514 | ietf-syslog-types:local6 | info | |

+ + + + + + +

* Show management plane default, currently the node does not have the default source IP set to the loopback “lb1”.

3928-003> show management-plane

+ DEFAULT SOURCE IP INTERFACE +

| Interface |

+ +

| |

+ +

* Disable a logical port and check on syslog server for any messages received on the syslog server.

diag@3928-003# logical-ports logical-port 10 admin-state disable Applying 1 edit

diag@3928-003# logical-ports logical-port 10 admin-state enable Applying 1 edit

* There are no messages received on syslog server.

Graphical user interface, application

Description automatically generated

* Set the management source ip on the node as the “lb1”.

management-plane default-source-ip interface lb1

* Show the management-plane source IP on node

3928-003> show management-plane

+ DEFAULT SOURCE IP INTERFACE +

| Interface |

+ +

| lb1 |

+ +

* Disable a logical port and check on syslog server for any messages received on the syslog server.

diag@3928-003# logical-ports logical-port 10 admin-state disable

Applying 1 edit diag@3928-003#

diag@3928-003# logical-ports logical-port 10 admin-state enable Applying 1 edit

* Validate on the syslog server that the messages have been received. Messages have been received on the syslog server.

Graphical user interface, text, application

Description automatically generated

* To delete the syslog server:

no syslog

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### TLS profiles

***Objective:***

Objective is to setup TLS profiles for use in Telemetry and SZTP.

***Procedure:***

* Enter the following command on CLI to create a TLS Service Profile:

config

*pkix peer-auth-profiles peer-auth-profile peer-auth- profile check-cert-expiry true*

*hello-params tls-profile cipher-suites cipher-suite ecdhe-rsa-with-aes-128-cbc-sha*

*hello-params tls-profile elliptic-curves elliptic- curve ciena-tls-types:secp256r1*

*hello-params tls-profile session-resumption-timeout 600*

*tls-service-profiles test tls-profile-name tls- profile*

*tls-service-profiles test tls-peer-auth-profile-name peer-auth-profile*

*tls-service-profiles test tls-certificate-name testCert*

* Then attach Telemetry and SZTP to the test TLS profile:

telemetry-system server config tls-service-profile test ztp tls-service-profile test

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Pkix and TLS- IP host list

***Objective:***

Secure TLS require PKIX ( public key infrastructure / X.509) to manage the devices private keys and CA and device certificates. New enhancement introduced in SAOS 10.4 and onwards – check IP host list (while peer authentication). Check IP host allows the user to specify which devices are allowed to connect to it. The user configures a list of acceptable IP addresses and DNSs then enables check IP host. The list is cross-referenced with either the Subject Alternate Name or the Common Name of the certificate. If it matches, then a TLS connection will be allowed.

***Procedure:***

* Add entries to ip-host-list:

pkix peer-auth-profiles peer-auth-profile <peer-auth- profile-name> ip-host-list <ip-address|hostname> <ip- address|hostname> <ip-address|hostname>

* Enable check IP/host:

pkix peer-auth-profiles peer-auth-profile <peer-auth- profile-name> check-ip-host true

* Validate with below commands

5170-208> show tls

+ TLS SERVICE PROFILES +

| Name | Value |

+ + +

| Service Profile Name | test |

| TLS Profile Name | tls-profile |

**|** Peer Auth Profile Name | https-peer-auth-profile |

| Certificate Name | testCert |

+ + +

+----------- **PEER AUTH PROFILES** +

| Name | Value |

+ + +

| Profile Name | https-peer-auth-profile |

| Check Expiry | True |

| Check IP/Host | True |

| IP/Host List | 10.121.190.169 |

+ + +

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Telemetry

***Objective:***

Objective is to verify Telemetry with PKIX certificates. This testcase is related to the PKIX testcase.

***Procedure:***

* Setup a gnmi-client on a linux server. For this test, the gnmi-client is setup on the server/VM 10.181.65.91.
* Download the certificates from CA server to the node.

pkix-certificates install login-id ftpuser password ciena123 cert-name cert-openssl-1.1.1 cert-passphrase ciena remote-file-uri <ftp://10.181.65.91/~/gnmi/ValimarDevServer-openssl-1.1.1.p12> cert-only false

pkix-ca install login-id ftpuser password ciena123 ca-cert-name ValimarCa remote-file-uri [ftp://10.181.65.91/~/gnmi/ValimarDevCa-](ftp://10.181.65.91/~/gnmi/ValimarDevCa-openssl-1.1.1.cert.pem) [openssl-1.1.1.cert.pem](ftp://10.181.65.91/~/gnmi/ValimarDevCa-openssl-1.1.1.cert.pem)

* Validate that the certificates have been downloaded:

3928-003> show pkix

+ CA CERTIFICATES +

| Name | Value |

+ + +

| CA Name | ValimarCa |

| Subject Common Name | |

| Issuer Common Name | |

| Valid Until | Aug 8 23:19:19 2040 UTC (19 years) |

+ + +

+---- CERTIFICATE REVOCATION LISTS ---+

| Name | Value |

+ + +

| No Entries |

+ + +

+ DEVICE CERTIFICATES +

| Name | Value |

+ + +

| Certificate Name | cert-openssl-1.1.1 |

| Algorithm ID | - |

| Private Key | present |

| Subject Common Name | ValimarDevServer-openssl-1.1.1-rsa4096 |

| Issuer Common Name | - |

| Valid Until | Aug 24 21:40:12 2021 UTC (10 months) |

+ + +

* Setup TLS, PKIX, and Telemetry server.

hello-params tls-profile cipher-suites cipher-suite ecdhe-rsa- with-aes-128-cbc-sha

hello-params tls-profile elliptic-curves elliptic-curve ciena- tls-types:secp256r1

hello-params tls-profile session-resumption-timeout 3600 pkix peer-auth-profiles peer-auth-profile peer-auth-profile check-cert-expiry true

tls-service-profiles test tls-profile-name tls-profile

tls-service-profiles test tls-peer-auth-profile-name peer-auth- profile

tls-service-profiles test tls-certificate-name cert-openssl- 1.1.1

telemetry-system server config enable true

telemetry-system server config tls-service-profile test exit

* Validate TLS setup:

3928-003> show tls

+------------ TLS SERVICE PROFILES +

| Name | Value |

+ + +

| Service Profile Name | test |

| TLS Profile Name | tls-profile |

| Peer Auth Profile Name | peer-auth-profile |

| Certificate Name | cert-openssl-1.1.1 |

+ + +

+---------- PEER AUTH PROFILES +

| Name | Value |

+ + +

| Profile Name | peer-auth-profile |

| Check Expiry | True |

| Check IP/Host | - |

| Check Fingerprint | - |

| Fingerprint List | - |

+ + +

+ HELLO PARAMS +

| Name | Value |

+ + +

| Profile Name | tls-profile |

| Protocol Versions | tls-1.2 |

| Cipher Suites | ecdhe-rsa-with-aes-128-cbc-sha |

| Elliptic Curves | secp256r1 |

| Sess. Resumption Timeout (s) | 3600 |

| OCSP State | disabled |

| NONCE State | enabled |

| Default OCSP Responder URL | - |

+ + +

* Subscribe to a sensor from the gnmi-client and validate that messages are being received. Output from GNMI-client on remote server polling for 10x node system memory:

ftpuser@ftpuser:~/gnmi$

gnmi\_cli -a 10.181.102.165:6702 -updates\_only -qt s -dt s - sample\_interval 50000 -client\_types gnmi -insecure -client\_crt Vali marDevClient-openssl-1.1.1.cert.pem -client\_key ValimarDevClient- openssl-1.1.1.key.pem -with\_user\_pass -q **/ciena-sys-tmet:system- state/memory**

username: diag password:

Ciena/ciena-sys-tmet:system-state/memory/active, 2189152256

Ciena/ciena-sys-tmet:system-state/memory/available, 1533530112

Ciena/ciena-sys-tmet:system-state/memory/buffers, 684834816

Ciena/ciena-sys-tmet:system-state/memory/cached, 895356928

Ciena/ciena-sys-tmet:system-state/memory/free, 213032960

Ciena/ciena-sys-tmet:system-state/memory/inactive, 697450496

Ciena/ciena-sys-tmet:system-state/memory/total, 4113903616

Ciena/ciena-sys-tmet:system-state/memory/used, 2320678912

Ciena/ciena-sys-tmet:system-state/memory/used-percent, 62.7

Ciena/ciena-sys-tmet:system-state/memory/active, 2189561856

Ciena/ciena-sys-tmet:system-state/memory/available, 1534181376

Ciena/ciena-sys-tmet:system-state/memory/buffers, 684843008

Ciena/ciena-sys-tmet:system-state/memory/cached, 895713280

Ciena/ciena-sys-tmet:system-state/memory/free, 213442560

* Verify telemetry sensor subscription:

3928-003> show telemetry subscriptions

+--------------------------- TELEMETRY SUBSCRIPTIONS +

| Index | Name | Value |

+ + + +

| 1 | Subscription: | |

| | Subscription-ID | 4ca324bf-db60-48ea-9e3b-6325346268e0 |

| | Subscription State | |

| | User Name | diag |

| | Subscription Mode | stream |

| | Update Only | True |

| | Sample Interval | 5000000000 |

| | Subscription Message | |

| | Telemetry Sensor Paths | |

| | Telemetry Sensor Path | /ciena-sys-tmet:system-state/memory |

| | Telemetry Sensor ID | 17435055178426406752 |

| | Telemetry Sensor Sub-Mode | target-defined |

+ + + +

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### RADIUS over TLS configuration

***Objective:***

Objective is to successfully authenticate to a Ciena device using RADSEC.

***Procedure:***

* Download the CA and Device Certificates:

pkix-ca install ca-cert-name RADSECCA remote-file-uri sftp://1.1.1.1/home/tls/certs/RadSecClntCA.pem login-id tls password tls pkix-certificates install cert-name RADSECCLIENT cert-only **false** remote- file-uri sftp://1.1.1.1/home/tls/certs/RadSecClntCert.p12 cert- passphrase ciena123 login-id tls password tls

* Then create TLS Profile configuration (can also follow TLS profile step in the document):

hello-params TLS\_PROFILE1 cipher-suites cipher-suite rsa-with-aes-256- cbc-sha

hello-params TLS\_PROFILE1 elliptic-curves elliptic-curve ciena-tls- types:secp256r1

hello-params TLS\_PROFILE1 session-resumption-timeout 3600 hello-params TLS\_PROFILE1 tls-versions tls-version tls-1.2

pkix peer-auth-profiles peer-auth-profile PAPROFILE1 check-cert- expiry **true**

tls-service-profiles TLS\_SRVR\_PROFILE1 tls-profile-name TLS\_PROFILE1 tls-service-profiles TLS\_SRVR\_PROFILE1 tls-peer-auth-profile-name PAPROFILE1

tls-service-profiles TLS\_SRVR\_PROFILE1 tls-certificate-name RADSECCLIENT

* Then Create AAA configuration:

system aaa accounting config accounting-method RADSERVER

system aaa accounting events event AAA\_ACCOUNTING\_EVENT\_LOGIN config event-type AAA\_ACCOUNTING\_EVENT\_LOGIN

system aaa accounting events event AAA\_ACCOUNTING\_EVENT\_LOGIN config record START\_STOP

system aaa server-groups server-group RADSERVER config name RADSERVER system aaa server-groups server-group RADSERVER config type RADSEC system aaa server-groups server-group RADSERVER servers

server 1.1.1.1 config address 1.1.1.1

system aaa server-groups server-group RADSERVER servers server 1.1.1.1 config admin-state enabled

system aaa server-groups server-group RADSERVER servers

server 1.1.1.1 radsec config tls-service-profile TLS\_SRVR\_PROFILE1 system aaa server-groups server-group RADSERVER servers

server 1.1.1.1 config name radsecserver

* Last step is to configure Authentication parameters:

system aaa authentication config authentication-method RADSERVER no system aaa authentication config authentication-method AUTH\_LOC system aaa authentication config authentication-method AUTH\_LOC

NOTE: for server configuration you can refer to the following confluence page. <https://confluence.ciena.com/pages/viewpage.action?pageId=603288778>

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Syslog over TLS configuration

***Objective:***

Objective is to successfully generate Syslog messages over a secure TLS session.

***Procedure:***

* Download the CA and Device Certificates:

pkix-ca install ca-cert-name SYSLOGCA remote-file-uri sftp://1.1.1.1/home/tls/certs/SyslogCA.pem login-id tls password tls pkix-certificates install cert-name SYSLOGCLIENT cert-only **false** remote- file-uri sftp://1.1.1.1/home/tls/certs/SyslogClntCert.p12 cert- passphrase ciena123 login-id tls password tls

* Then create TLS Profile configuration (can also follow TLS profile step in the document):

hello-params 'TLS\_PROFILE2' tls-versions tls-version tlscmn:tls-1.2 hello-params 'TLS\_PROFILE2' cipher-suites cipher-suite tlscmn:rsa-with- aes-256-cbc-sha

hello-params 'TLS\_PROFILE2' elliptic-curves elliptic-curve ciena-tls- types:secp256r1

tls-service-profiles TLS\_SRVR\_PROFILE2 tls-profile-name TLS\_PROFILE1 tls-service-profiles TLS\_SRVR\_PROFILE2 tls-peer-auth-profile-name PAPROFILE1

tls-service-profiles TLS\_SRVR\_PROFILE2 tls-certificate-name SYSLOGCLIENT

* Then configure Syslog:

syslog log-actions remote-syslog-tls admin-state disabled tls-service- profile "TLS\_SRVR\_PROFILE2"

syslog log-actions remote-syslog-tls destination '1.1.1.1' severity alert critical debug emergency error info notice warning

* The last step is to verify that the transport error = Success:

CN5166-0004-R203> show syslog tls statis

+--------- SYSLOG TLS SERVER STATISTICS +

| Name | Value |

+ + +

| Server Address | 1.1.1.1 |

| Oper State | enabled |

| Connection Attempts | 1 |

| Successful Connections | 1 |

| Failed-tcp Connections | 0 |

| Failed-tls Connections | 0 |

| timed-out-connections | 0 |

| Unexpected Close Connections | 0 |

| Closed Connections | 0 |

| Last Transport Error | Success |

+ + +

NOTE: for server configuration you can refer to the following confluence page. <https://confluence.ciena.com/pages/viewpage.action?pageId=614967766>

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### SSH Public Key Authentication

***Objective:***

Authenticate to the device with a public key instead of a password.

***Procedure:***

* Generate the public private key pair on the client (note that this will depend on the client in use. Example below is a Linux client):

*ssh-keygen -t rsa -b 2048 -N "" -f key\_pair*

* Install the Public key on the device:

ssh-user-pubkey-install user diag url <http://1.1.1.1/pub.key>

* Configure SSH server (example below):

system ssh-server config encryption-algorithm aes256-cbc system ssh-server config mac-algorithm hmac-sha2-256

system ssh-server config kex-algorithm diffie-hellman-group14-sha256 system ssh-server config pka-algorithm ssh-rsa

* Enable public key authentication:

system ssh-server config public-key-authentication enabled

* Verify public key is installed and associated with correct user:

CN5166-0004-R203> show system ssh-server user-pubkey user-name diag

+ SSH USER PUBLIC KEYS +

| Name | Value |

+ + +

| User | diag |

| Fingerprint(MD5) | 56:15:0a:04:15:0c:09:b8:60:f5:1f:c4:f2:44:09:72 |

| Fingerprint(SHA-1) | cJYRbUOM0C3MmF3FhMbVRhgn2AU |

+ + +

* Verify Encryption algorithm is correct :

CN5166-0004-R203> show system ssh-server config

+ SSH SERVER CONFIG +

| Name | Value |

+ + +

| Encryption Algorithm | aes256-cbc |

| Kex Algorithm | diffie-hellman-group14-sha256 |

| MAC Algorithm | hmac-sha2-256 |

| Public Key Algorithm | ssh-rsa |

| Public Key Authentication | enabled |

| Rekey Limit | 500M |

| Rekey Time | None |

+ + +

* Authenticate to the device with client and key

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Verify SAOS 10.x software version

***Objective:***

Objective is to verify Ciena SAOS 10.x installed.

***Procedure:***

* Login to CLI using the management IP you checked in the previous step:

ssh [diag@x.x.x.x](mailto:diag@x.x.x.x)

username: diag password: ciena123

* Issue the following command to verify
  + show software
* You should see an output like the following:

+ SOFTWARE STATE +

| Name | Value |

+ + +

| Current operation | idle |

| RPC Status | idle |

| Running package version | saos-10-01-00-0149 |

| Active bootchain | 01-01-00-0149 |

| Standby bootchain | 01-01-00-0149 |

+ + +

| Components: | |

| cn\_telemetry\_1 | 01-01-00-0149 |

| cn\_dhcp-ctrl\_1 | 01-01-00-0149 |

| cn\_alarm\_1 | 01-01-00-0149 |

| cn\_lacp\_1 | 01-01-00-0149 |

| cn\_collectd\_1 | 08-00-00-0165 |

| cn\_cnfp\_1 | 01-01-00-0149 |

| cn\_eoam\_1 | 01-01-00-0149 |

| cn\_dataplane\_1 | 01-01-00-0149 |

| cn\_feds\_1 | 01-01-00-0149 |

| cn\_dhcpl3relay\_1 | 01-01-00-0149 |

| cn\_snmp-agent\_1 | 01-01-00-0149 |

| cn\_svcdirectory\_1 | 01-01-00-0149 |

| cn\_cfm\_1 | 01-01-00-0149 |

| cn\_sync\_1 | 01-01-00-0149 |

| cn\_hal-dnx\_1 | 01-01-00-0149 |

| cn\_storage\_1 | 01-01-00-0149 |

| cn\_ui\_1 | 01-01-00-0149 |

| xg\_xgrade-agent\_1 | 08-00-00-0165 |

| cn\_central-logger\_1 | 08-00-00-0165 |

| cn\_sync-hal\_1 | 01-01-00-0149 |

| cn\_lldp\_1 | 01-01-00-0149 |

| cn\_ntp\_1 | 01-01-00-0149 |

| cn\_system\_1 | 01-01-00-0149 |

| cn\_ztp\_1 | 01-01-00-0149 |

| cn\_sat\_1 | 01-01-00-0149 |

| cn\_dns\_1 | 01-01-00-0149 |

| cn\_ipservices\_1 | 01-01-00-0149 |

| cn\_pkix\_1 | 01-01-00-0149 |

+ + +

| Available packages: | |

| saos-10-01-00-0149 | **activated** |

+ + +

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### SSH Rekeying Configuration

***Objective:***

Configure SSH rekeying and verify configuration.

***Procedure:***

* Configure SSH max time in seconds after which SSH key is renegotiated:

system ssh-server config rekey-time 300

* Configure SSH max data exchanged before SSH key is renegotiated:

system ssh-server config rekey-limit 1G

* Verify rekey configuration is applied:

CN5166-0004-R203> show system ssh-server config

+ SSH SERVER CONFIG +

| Name | Value |

+ + +

| Encryption Algorithm | aes256-cbc |

| Kex Algorithm | diffie-hellman-group14-sha256 |

| MAC Algorithm | hmac-sha2-256 |

| Public Key Algorithm | ssh-rsa |

| Public Key Authentication | enabled |

| Rekey Limit | 1G |

| Rekey Time | 300seconds |

+ + +

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### DNS Client Setup

***Objective:***

Objective is to verify setting up DNS client

***Procedure:***

* Enter the following command on CLI with an example DNS server 192.168.10.100:

config

*oc-sys:system dns dns-client admin-status enabled*

*oc-sys:system dns dns-client domain-name ott.ciena.com oc-sys:system dns dns-client server 192.168.10.100*

* You should see something like the following:

5170-010> show dns

+ DNS-CLIENT +

| Name | Value |

+ + +

| Admin-status | enabled |

| Domain-name | ott.ciena.com |

| Domain-name-scope | user |

| Server-scope | user |

+ + +

+ USER-SERVERS +

| IP Address | Oper-status |

+ + +

| 192.168.10.100 | enabled |

+ + +

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### L3 DHCPv4 Relay Setup

***Objective:***

Objective is to setup L3 DHCP Relay (IPv4 only).

VLAN 51 VLAN 52



192.168.2.15/24

192.168.2.14/24

192.168.1.16/24

51xx,3 5170

DHCP L3 DHCP Server

192.168.1.101

***Procedure:***

* Create the classifier and flow points and forwarding domains on the L3 DHCP Relay :

***#Classifiers***

config

classifiers classifier vlan51 filter-entry vtag-stack vtags 1 vlan-id 51

classifiers classifier vlan52 filter-entry vtag-stack vtags 1 vlan-id 52

exit

***#Forwarding-domains***

config

fds fd FDRelayClient mode vpls fds fd FDRelayServer mode vpls

exit

***#Flow-points***

config fps

fp fp15

fd-name FDRelayClient logical-port 15

classifier-list-precedence 7 stats-collection on classifier-list vlan51

mtu-size 2000

egress-l2-transform push-vid-51 vlan-stack 1

push-tpid tpid-8100 push-vid 51

exit exit exit exit

fps

fp fp16

fd-name FDRelayServer logical-port 16

classifier-list-precedence 7 stats-collection on classifier-list vlan52

mtu-size 2000

egress-l2-transform push-vid-52 vlan-stack 1

push-tpid tpid-8100 push-vid 52

exit exit exit

***#IP interfaces***

oc-if:interfaces interface if15 config name if15 vrfName default cn- if:type ip mtu 2000 admin-status true underlay-binding config fd FDRelayClient

oc-if:interfaces interface if15 ipv4 addresses address 192.168.2.15 config ip 192.168.2.15 prefix-length 24

oc-if:interfaces interface if16 config name if16 vrfName default cn- if:type ip mtu 1500 admin-status true underlay-binding config fd FDRelayServer

oc-if:interfaces interface if16 ipv4 addresses address 192.168.1.16 config ip 192.168.1.16 prefix-length 24

* Configure L3 Relay:

config

l3-relay-agent instance toi\_dtw admin-enabled true

dhcp-server-addresses 192.168.1.101

ip-interfaces if15

flow-points fp15 flow-point-trusted true

cid-string cid-client

ip-interface-enabled true ip-interface-trusted true exit

ip-interfaces if16

flow-points fp16 flow-point-trusted true cid-string cid-server

ip-interface-enabled true ip-interface-trusted true

* Display L3 Relay Configuration:

5170-010> show dhcpl3relay

+---- DHCP L3 RELAY CONFIGURATION +

| Name | Value |

+ + +

| Instance | toi\_dtw |

| Admin State | Enabled |

| Circuit ID Type | String |

| Remote ID Type | String |

| Remote ID String | rid-server |

| Option 82 | On |

| DHCP Server(s) | 192.168.1.101 |

| IP Interface | if15 |

| Circuit ID String | cid-client |

| Admin State | Enabled |

| Trust State | Trusted |

| IP Interface | if16 |

| Circuit ID String | cid-server |

| Admin State | Enabled |

| Trust State | Trusted |

+ + +

+ DHCP L3 RELAY STATUS +

| Name | Value |

+ + +

| Instance | toi\_dtw |

| Status Message | Interface if15 is not configured with an IPv4 address |

| Operational State | Disabled |

+ + +

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### DHCPv6 Client Setup

***Objective:***

Ensure that with DHCPv6 client enabled, the interface will acquire an IPv6 address automatically. **Only stateful DHCPv6 (no SLAAC) is currently supported.**

***Procedure:***

* Dual IPv4 and IPv6 stack on mgmt. interfaces are supported as of 10.3 and onwards. Enable DHCPv6 client on mgmtbr0. Ensure that :
  + config
  + dhcpv6-client client mgmtbr0 admin-enable true
* Configure IPv4 static IP on the mgmtbr0 as well.
  + dhcp-client client mgmtbr0 admin-enable false
  + oc-if:interfaces interface mgmtbr0 ipv4 address address x.x.x.x config ip x.x.x.x prefix-length 20
  + rib vrf default ipv4 x.x.x.x/8 next-hop x.x.x.x description "lab default"

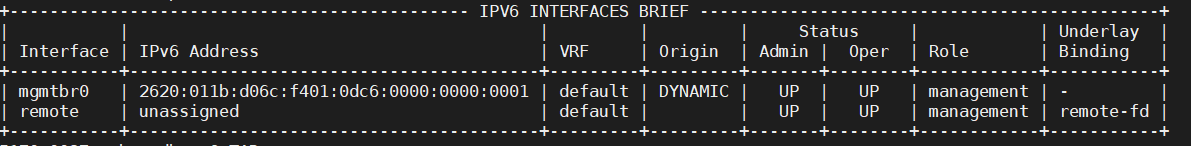
Ex:

dhcp-client client mgmtbr0 admin-enable false

oc-if:interfaces interface mgmtbr0 ipv4 address address 10.181.36.85 config ip 10.181.36.85 prefix-length 20

rib vrf default ipv4 10.0.0.0/8 next-hop 10.181.32.1 description "lab default"

* Display the IPv6 and IPv4 interfaces on the node.
  + 5170-0037> show ipv6 interfaces brief



* + 5170-0037> show ip interfaces brief

A screenshot of a computer

Description automatically generated with medium confidence

5170-0037> show dhcpv6

+-------- DHCPV6 CLIENT CONFIGURATION +

| Name | Value |

+ + +

| Interface Name | mgmtbr0 |

| Admin State | Enabled |

| Rapid Commit | Enabled |

| Requested Preferred Lifetime (s) | 0 |

| Requested Valid Lifetime (s) | 0 |

| Option | |

| DNS Server List | Enabled |

| Domain Search List | Enabled |

| Posix Time Zone | Disabled |

| TZDB Time Zone | Enabled |

| NTP Server | Enabled |

| Bootfile URL | Enabled |

+ + +

| Interface Name | remote |

| Admin State | Enabled |

| Rapid Commit | Enabled |

| Requested Preferred Lifetime (s) | 0 |

| Requested Valid Lifetime (s) | 0 |

| Option | |

| DNS Server List | Enabled |

| Domain Search List | Enabled |

| Posix Time Zone | Disabled |

| TZDB Time Zone | Enabled |

| NTP Server | Enabled |

| Bootfile URL | Enabled |

+ + +

+ DHCPV6 CLIENT STATE +

| Name | Value |

+ + +

| Interface Name | remote |

| Oper State | Enabled |

| DHCPv6 State | preinit |

| Config State | stateful |

| Renewal (T1) Time (s) | |

| Renewal (T1) Time Remaining (s) | |

| Rebinding (T2) Time (s) | |

| Rebinding (T2) Time Remaining (s) | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| |  |  |  | | Preferred Lifetime (s) Preferred Lifetime Remaining Valid Lifetime (s)  Valid Lifetime Remaining (s) | (s) | |  |  |  | |  | |  |  |  | |
| |  |  |  |  |  |  |  |  +  | | DHCPv6 Server DUID Option Value  DNS Server List Domain Search List Posix Time Zone TZDB Time Zone  NTP servers Boot File URL  Interface Name |  | |  |  |  |  |  |  |  |  +  | | mgmtbr0 | |  |  |  |  |  |  |  |  +  | |
| **|**  **|**  **|**  | | **Oper State DHCPv6 State Config State**  Renewal (T1) Time (s) |  | **|**  **|**  **|**  | | **Enabled bound stateful**  302400 | **|**  **|**  **|**  | |
| | | Renewal (T1) Time Remaining | (s) | | | 241733 | | |
| | | Rebinding (T2) Time (s) | | | | 453600 | | |
| | | Rebinding (T2) Time Remaining (s) | | | | 392933 | | |
| | | Preferred Lifetime (s) | | | | 604800 | | |
| | | Preferred Lifetime Remaining (s) | | | | 544133 | | |
| | | Valid Lifetime (s) | | | | 604800 | | |
| | | Valid Lifetime Remaining (s) | | | | 544133 | | |
| |  |  |  |  |  |  |  |  + | DHCPv6 Server DUID Option Value  DNS Server List Domain Search List Posix Time Zone TZDB Time Zone  NTP servers Boot File URL | | |  |  |  |  |  |  |  |  + | 0:1:0:1:25:22:d:24:0:0:5e:0:1:81 | |  |  |  |  |  |  |  |  + |

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Static Mgmt IPv6 Setup

***Objective:***

Static IPv6 address can be added onto management interface.

***Procedure:***

* Disabled DHCPv6 client. DHCVPv6 client is enabled by default.

config

* + dhcpv6-client client mgmtbr0 admin-enable false
* Then configure a static IPv6 address:

oc-if:interfaces interface mgmtbr0 ipv6 address address x.x.x.x.x.x.x.x config ip x.x.x.x.x.x.x prefix-length y

rib vrf default ipv6 x.x.x.x.x.x.x.x/y next-hop x.x.x.x.x.x.x.x description "lab default"

* Example :

## Disable DHCPv6 Client

dhcpv6-client client mgmtbr0 admin-enable false

## Setup IPv6 mgmtbr mgmt. interface

oc-if:interfaces interface mgmtbr0 ipv6 addresses address 2620:11b:d06c:f401::2455 config ip 2620:11b:d06c:f401::2455

prefix-length 64

## Setup IPv6 static route to gateway router

rib vrf default ipv6 2620:011b:d06c:f401::2455/64 next-hop 2620:011b:d06c:f401::1

* Check the provisioning:
  + show ipv6 interfaces brief

A picture containing graphical user interface

Description automatically generated

* + show ipv6 route

Graphical user interface, text, website

Description automatically generated

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Verify Backup

***Objective:***

Objective is to verify backup of the node’s configuration.

***Procedure:***

* From CLI, enter:

config backup filename name-of-file.xml

* Once the backup is complete, can display the backup file :

show backup filenames

5144-009> show backup file

+ BACKUP FILES +

| File Name | Backup Time |

+ + +

| backup-5144-daily | 2020-12-20T20:51:54Z |

+ + +

* Once the backup is complete, for reference, user can find the backup file in UI container:
  + Enter “diag shell” to go into UI container.
  + Change to directory where backup file is: /mnt/config/.yumapro/backups
    - diag@5162-002.ui:/mnt/config/.yumapro/backups$ ls
* SFTP the file off the node- using CLI:

config upload url sftp://x.x.x.x/home/ubuntu remote backup- 5144-daily username yyyyy password yyyyy

Test Case Results:

Passed: Yes No Verified by Date/Time

Comments

###### Verify Reset to User Config (RTUC)

***Objective:***

Objective is to restore a configuration file back onto the node. Currently only support same load restore.

***Procedure:***

* Backup the system’s configuration.
  + config backup filename <your-filename>
* Reset to User configuration - RTUC
  + *system reset filename <your-filename>*
* Check the status of the RTUC.
  + system reset user-config status

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Configuration – Golden Configuration

***Objective:***

Objective is to verify backup and restore of the golden configuration. Golden configuration is a backup file which contains pre-staging configuration for xZTP. From CLI, the user can perform a reset to golden-config to put system back to perform xZTP. Hence, this enables the operator to have a failsafe configuration file.

***Procedure:***

* On Valimar cli, perform a backup to golden-config. Normally, the golden config should contain basic infrastructure provisioning such mgmt. interfaces, remote servers such as authentication servers/syslog/SNMP etc….
  + system backup golden-config
* Perform a system reset to factory-default by push button. This can take 15-20minutes to complete. After system is reset, user can login with default login of diag/ciena123 from the console port. The node should only have golden-config provisioning on the system.
* Alternatively, the user can execute a cli command to reset provisioning to golden-config.
  + 3928> system reset golden-config

PRESS <CTRL>C TO ABORT (10 seconds) PRESS <CTRL>C TO ABORT (9 seconds) PRESS <CTRL>C TO ABORT (8 seconds) PRESS <CTRL>C TO ABORT (7 seconds) PRESS <CTRL>C TO ABORT (6 seconds) PRESS <CTRL>C TO ABORT (5 seconds) PRESS <CTRL>C TO ABORT (4 seconds) PRESS <CTRL>C TO ABORT (3 seconds) PRESS <CTRL>C TO ABORT (2 seconds) PRESS <CTRL>C TO ABORT (1 seconds)

proceeding to reboot

* To delete the golden-config, enter the following command:
  + system delete golden-config

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Port Flap Detection

Port flapping results from instability in the network where the ports toggles up and down within a short span of time. The port flapping results in network to re-converge when the state of the port/link changes. Port Flap Detection feature will detect port flaps and apply a hold timer before changing the state of the port to down

***Objective:***

Enable port flap detection and set the necessary parameters.

***Procedure:***

* Enable port flap detection.
  + oc-if:interfaces interface <port-id> config link-flap- detect true
* Set the time window to detect the link flaps.
  + oc-if:interfaces interface <port-id> config link-flap- detect-time <detect-time value> (default = 10s)
* Set the number of link flaps that would occur during the time window that will trigger a port down.
  + oc-if:interfaces interface <port-id> config link-flap- count <flap-count value> (default = 5s)
* Set the amount of time the link should be held down when too many link flaps have been detected.
  + oc-if:interfaces interface <port-id> config link-flap- hold-time <hold-time value> (default = 300s)
* Verify the settings:

5162-001> show ettps ettp 42

+ Ettp +

| KEY | VALUE |

+ + +

| Name | 42 |

| Description | 42 |

| Type | ettp |

| Admin Status | True |

| Mode | auto |

| Link Flap Detect | True |

| Link Flap Count | 5 |

| Link Flap Detect Time | 10 |

| Link Flap Hold Time | 300 |

| Duplex | full |

| Port Speed | 100Gb |

| Flow Control | off |

| Auto Negotiation | False |

| Forward Error Correction | auto |

+ + +

* Verify the statistics:

5162-001> show ettps ettp 2 statis

+ Ettp +

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| | | KEY | | | VALUE | | |
| + |  | + |  | + |
| | | Name | | | 2 | | |
| | |  | | |  | | |
| | |  | In Bytes | | 0 | | |
| | |  | In Unicast Packets | | 0 | | |
| | |  | In Errors | | 0 | | |
| | |  | Out Unicast Pkts | | 0 | | |
| | |  | Out Errors | | 0 | | |
| | |  | In Pkts | | 0 | | |
| | |  | Out Bytes | | 15834974 | | |
| | |  | Out Pkts | | 138696 | | |

| Link Flap Events | 0 |

+ + +

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Low Latency Bypass (currently only available on 5162)

***Objective:***

Enable low latency bypass. LLBP can only be enabled on 5162. This feature enable a specific internal datapath to support performance and scale for features such as IP BFD and CFM.

***Procedure:***

* Unbind the logical port 40.
  + no logical-ports logical-port 40 binding
* Activate interface 40’s LLBP.
  + oc-if:interfaces interface 40 config offload-activate true
* This will enable a lower latency internal data path.

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

* + 1. **SNMP Setup *– Through Netconf/YANG***

***Objective:***

Objective is to enable SNMP through Netconf/Yang. It is much easier to go through Netconf browser to setup SNMP trap notifications/informs than going through the CLI.

***Procedure:***

* Enter the following RPC call to enable SNMP trap notifications from SAOS 10.x nodes. Please ensure that your Netconf browser has the latest SAOS 10.x Yang modules loaded. Replace the highlighted portion with the appropriate SNMP trap collector server’s IP address.

<?xml version="1.0" encoding="utf-8"?>

<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="">

<edit-config>

<target>

<running/>

</target>

<config>

<snmp:snmp xmlns:snmp="urn:ietf:params:xml:ns:yang:ietf-snmp">

<snmp:target>

<snmp:name>TARG</snmp:name>

<snmp:udp>

<snmp:ip>x.x.x.x</snmp:ip>

</snmp:udp>

<snmp:target-params>PARAMS</snmp:target-params>

<snmp:tag>MY\_TAG</snmp:tag>

<snmp:timeout>1000</snmp:timeout>

<snmp:retries>4</snmp:retries>

</snmp:target>

<snmp:target-params>

<snmp:name>PARAMS</snmp:name>

<snmp:v2c>

<snmp:security-name>SEC-NAME</snmp:security-name>

</snmp:v2c>

</snmp:target-params>

<snmp:community>

<snmp:index>t000001</snmp:index>

<snmp:text-name>public</snmp:text-name>

<snmp:security-name>SEC-NAME</snmp:security-name>

</snmp:community>

<snmp:notify>

<snmp:name>TEST\_NOTIFY</snmp:name>

<snmp:tag>MY\_TAG</snmp:tag>

<snmp:type>trap</snmp:type>

</snmp:notify>

<snmp:vacm>

<snmp:group>

<snmp:name>DefaultVacmGroupV2C</snmp:name>

<snmp:member>

<snmp:security-name>SEC-NAME</snmp:security-name>

<snmp:security-model>v2c</snmp:security-model>

</snmp:member>

<snmp:access>

<snmp:context></snmp:context>

<snmp:security-model>v2c</snmp:security-model>

<snmp:security-level>no-auth-no-priv</snmp:security-level>

<snmp:context-match>exact</snmp:context-match>

<snmp:notify-view>NotifyView</snmp:notify-view>

</snmp:access>

</snmp:group>

<snmp:view>

<snmp:name>NotifyView</snmp:name>

<snmp:include>\*</snmp:include>

</snmp:view>

</snmp:vacm>

</snmp:snmp>

</config>

</edit-config>

</rpc>

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Dot1X – Supplicant Setup

***Objective:***

Verify the dot1x supplicant setup.

Text

Description automatically generated

***Procedure:***

* Enable dot1x globally on system.
  + system dot1x config system-auth-control enabled
* Set the port to “supplicant”.
  + oc-if:interfaces interface 17 config dot1x port- capabilities supplicant true
  + oc-if:interfaces interface 17 config dot1x supplicant admin-status enabled
* Set the identity and password of the Supplicant.
  + oc-if:interfaces interface 17 config dot1x supplicant identity seitoi
  + oc-if:interfaces interface 17 config dot1x supplicant password seitoi
* Display Supplicant information.

5162-0027> show dot1x ports supp port 17

+ DOT1X PORT SUMMARY +

| Name | Value |

+ + +

| Port Name | 17 |

| Admin State | Enabled |

| Start Period (sec) | 30 |

| Held Period (sec) | 60 |

| Auth Period (sec) | 30 |

| Max Start | 3 |

| Username | **seitoi** |

| Password | Set |

| EAP Version | 2 |

| EAP Method | md5 |

| Operational State | **Enabled** |

| Controlled Port Status | Unauthorized |

| PAE State | Held |

| Last EAPOL Frame Version | 0 |

| Last EAPOL Frame Source | 00:00:00:00:00:00 |

+

+

--+

+ +

DOT1X PORT STATISTICS

| | Eapol | Eapol | Eapol Start | Eapol Logoff | Invalid Eapol | Eapol Length |

| Port | Frame Tx | Frame Rx | Frame Tx | Frame Tx | Frame Rx | Error Frames |

+ + + + + + +

--+

| 17 | 5 | 0 | 5 | 0 | 0 | 0

|

+ + + + + + +

--+

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Dot1X – Authenticator Setup

***Objective:***

Verify the dot1x Authenticator setup.

Text

Description automatically generated

***Procedure:***

* Enable dot1x globally on system.
  + system dot1x config system-auth-control enabled
* Set the port to “authenticator”.
  + oc-if:interfaces interface 17 config dot1x port- capabilities authenticator true
  + oc-if:interfaces interface 17 config dot1x authenticator admin-status enabled/disabled
* Display Authenticator information.

5162-0028> show dot1x ports auth port 17

+ DOT1X PORT SUMMARY +

| Name | Value |

+ + +

| Port Name | 17 |

| Admin State | Enabled |

| Port Control | Auto |

| ReAuth Enabled | False |

| Quiet Period (sec) | 60 |

| Server Timeout (sec) | 30 |

| ReAuth Period (sec) | 3,600 |

| Max Retries | 2 |

| EAP Version | 2 |

| Control Direction | Both |

| Operational State | Disabled |

| Controlled Port Status | Unauthorized |

| Last EAPOL Frame Version | 0 |

| Last EAPOL Frame Source | 00:00:00:00:00:00 |

+ + +

+

+

DOT1X PORT STATISTICS

| | Eapol | Eapol | Eapol Start | Eapol Logoff | Eapol Resp | Eapol Resp | Eapol Req | Invalid Eapol | Eapol Req | Eapol Length |

| Port | Frame Tx | Frame Rx | Frame Rx | Frame Rx | Id Rx | Rx | Tx | Frame Rx | Id Tx | Error Frames |

+ + + + + + + +

+ + + +

| 17 | 0 | 0 | 0 | 0 | 0 | 0 | 0

| 0 | 0 | 0 |

+ + + + +

+ + +

+ + +

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Set up LLDP Global Config

***Objective:***

Objective is to verify LLDP configuration

***Procedure:***

* Go to the configuration terminal
  + config
* Enter the following commands

lldp-global-config msg-tx-interval 20

lldp-global-config tx-delay 3

lldp-global-config msg-tx-hold-multiplier 5 lldp-global-config admin-enabled true

lldp-global-config reinit-delay 1

* Go back out of configuration terminal

# exit

* Check the config changes
  + show lldp

You should see something like the following:

+------ LLDP GLOBAL CONFIG +

| Parameter | Value |

+ + +

| admin-enabled | True |

| msg-tx-interval | 20 |

| reinit-delay | 2 |

| tx-delay | 3 |

| msg-tx-hold-multiplier | 5 |

| notification-interval | 5 |

+ + +

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Verify show LLDP for a Connected Port

***Objective:***

Objective is to verify LLDP show

***Procedure:***

* Enter the following command for a connected port, as port 2 here:
  + show lldp neighbours
* You should see something like the following:

+ LLDP NEIGHBORS +

| Parameter | Value |

+ + +

| interface | 1 |

| chassis-id | 2C39C1001530 |

| chassis-id-subtype | mac-address |

| port-desc | SFP 10 Gig Ethernet Port |

| port-id | 1 |

| port-id-subtype | interface-name |

| system-capability-supported | bridge |

| system-capability-enabled | bridge |

| system-description | 5162 |

| system-name | 5162-002 |

| agg-status | capable |

| pair-controlable | False |

| port-class | p-class-pd |

| auto-neg-supported | True |

| mdi-supported | False |

| mdi-enabled | False |

| oper-mau-type | 33 |

| max-frame-size | 1526 |

| auto-neg-enabled | False |

| man-address | 10.181.33.84 |

| man-address-subtype | ipv4 |

| if-subtype | if-index |

+ + +

| interface | 2 |

+ + +

| interface | 3 |

+ + +

| interface | 4 |

+ + +

| interface | 5 |

+ + +

| interface | 6 |

+ + +

| interface | 7 |

+ + +

| interface | 8 |

+ + +

| interface | 9 |

+ + +

| interface | 10 |

+ + +

| interface | 11 |

+ + +

| interface | 12 |

+ + +

| interface | 13 |

+ + +

| interface | 14 |

+ + +

| interface | 15 |

+ + +

| interface | 16 |

+ + +

| interface | 17 |

+ + +

| interface | 18 |

+ + +

| interface | 19 |

+ + +

| interface | 20 |

| chassis-id | 54E032728FC0 |

| chassis-id-subtype | mac-address |

| port-desc | xe-2/2/3 |

| port-id | 583 |

| port-id-subtype | local |

| system-capability-supported | bridge router |

| system-capability-enabled | bridge router |

| system-description | Juniper Networks, Inc. mx960 , version 13.2R2.4 Build date: 2013-11-07 09:54:09 UTC |

| system-name | HeadEnd-Router |

| agg-status | capable |

| oper-mau-type | 0 |

| max-frame-size | 1518 |

| auto-neg-supported | True |

| auto-neg-enabled | False |

| man-address | 10.181.34.79 |

| man-address-subtype | ipv4 |

| if-subtype | if-index |

+ + +

| interface | 21 |

+ + +

| interface | 22 |

+ + +

| interface | 23 |

+ + +

| interface | 24 |

+ + +

| interface | 25 |

+ + +

| interface | 26 |

+ + +

| interface | 27 |

+ + +

| interface | 28 |

+ + +

| interface | 29 |

+ + +

| interface | 30 |

+ + +

| interface | 31 |

+ + +

| interface | 32 |

+ + +

| interface | 33 |

+ + +

| interface | 34 |

+ + +

| interface | 35 |

+ + +

| interface | 36 |

+ + +

| interface | 37 |

+ + +

| interface | 38 |

+ + +

| interface | 39 |

+ + +

| interface | 40 |

+ + +

| interface | 41 |

| chassis-id | 2C39C1001530 |

| chassis-id-subtype | mac-address |

| port-desc | QSFP28 100 Gig Ethernet Port |

| port-id | 42 |

| port-id-subtype | interface-name |

| system-capability-supported | bridge |

| system-capability-enabled | bridge |

| system-description | 5162 |

| system-name | 5162-002 |

| agg-status | capable |

| pair-controlable | False |

| port-class | p-class-pd |

| auto-neg-supported | True |

| mdi-supported | False |

| mdi-enabled | False |

| oper-mau-type | 0 |

| max-frame-size | 1526 |

| auto-neg-enabled | False |

| man-address | 10.181.33.84 |

| man-address-subtype | ipv4 |

| if-subtype | if-index |

+ + +

| interface | 42 |

+ + +

| interface | mgmtbr0 |

+ + +

| interface | remote |

+ + +

| interface | LPB |

+ + +

| interface | INT1 |

+ + +

| interface | INT2 |

+ + +

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

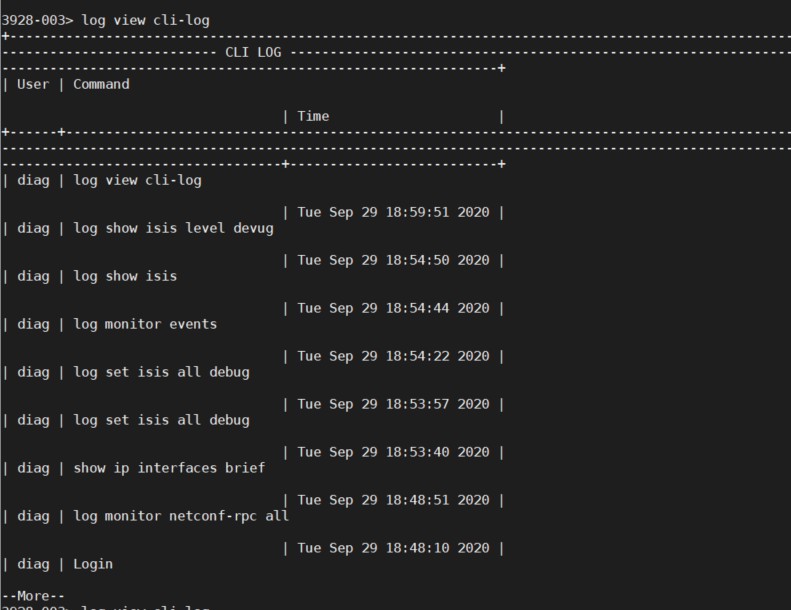
###### Debugging – Log monitoring

***Objective:***

Logs have been enabled in SAOS 10x and can be used for troubleshooting. Objective of this test is to setup and monitor logs for different features.

***Procedure:***

* CLI logs can be accessed through the following command:
  + log view cli-log
* CLI commands for the session will be displayed:



* Enter the following command to enable ISIS debug logs – similar provisioning can be used to check for LDP/OSPF/MPLS/BGP logs.
  + log set isis all debug
* Check for ISIS debug logs - for real-time monitoring:
  + log monitor troubleshoot
* Check for ISIS debug logs – for historical logs:
  + log view troubleshoot
* Output of the logs should be similar to below:

Text

Description automatically generated

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Debugging – Port Mirroring

***Objective:***

Port mirroring enables traffic ingressing or egressing a particular port to be mirrored to another port. This can be used for troubleshooting and verification.

Config Parameters:

destination-logical-port

Logical Port which will have traffic mirrored-to. All traffic for this Mirror Session will egress the destination logical port.

egress-mirror-logical-ports

A list of logical-ports whose egress traffic is mirrored to the destination logical-port.

ingress-mirror-logical-ports

A list of logical-ports whose ingress traffic is mirrored to the destination logical-port.

***Procedure:***

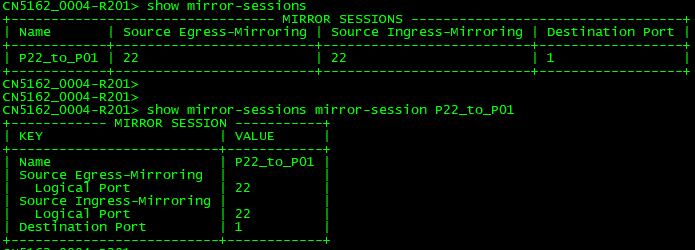
* Configure mirror destination port

mirror-sessions mirror-session P22\_to\_P01 destination-logical-port 1

* Configure mirror source port along with direction (ingress, egress or both)

mirror-sessions mirror-session P22\_to\_P01 egress-mirror-logical-ports 22 mirror-sessions mirror-session P22\_to\_P01 ingress-mirror-logical-ports 22

***Validation:***



Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### NETCONF – RPC commands

***Objective:***

All CLI commands are based on YANG models which are used in NETCONF RPC gets/edits/deletes. This testcase outlines how to use NETCONF logs to get the RPC commands for provisioning.

***Procedure:***

* Open two terminals to a SAOS 10x node.
* On terminal 1, monitor netconf-rpc logs:
  + log monitor netconf-rpc all
* On terminal 2, enter a CLI command such as
  + show ip interfaces
* RPC logs will be displayed on terminal 1, the relevant RPC get for the IP interfaces as depicted in CLI command is – formatting has to be done manually:

<?xml version="1.0" encoding="UTF-8"?>

<rpc message-id="2"

xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">

<**get**>

<filter type="subtree">

<interfaces [xmlns="http://openconfig.net/yang/interfaces">](http://openconfig.net/yang/interfaces)

<interface>

<config>

<type [xmlns="http://ciena.com/ns/yang/ciena](http://ciena.com/ns/yang/ciena-openconfig-)-[openconfig](http://ciena.com/ns/yang/ciena-openconfig-)- interfaces"/>

</config>

</interface>

</interfaces>

</filter>

</get>

</rpc>

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

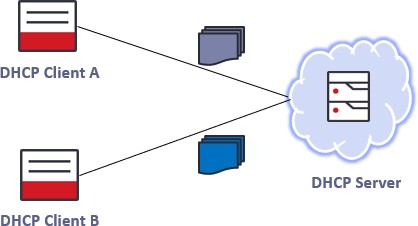
###### DHCP Options (Client Identifier & User Class Options)

***Objective:***

DHCP options are the smart way to configure to configure clients. The DHCP clients can request and receive information from the DHCP server in the form of DHCP options. The requirement of these DHCP options in addition with existing Options is to help DHCP servers to return the configuration parameter & IP allocation more intelligently.

Example: Sending configuration parameters & IP address allocation from a particular address pool to different clients based on the set of options transported I the protocol frame.

Note: In addition to this CATP, you can also refer to 10.6.0 TOI, which may complement in building improved understanding of this topic from conceptual standpoint. However, here in CATP will focus more on CLI & validation of this feature.



***Requirement:***

As per specific customer requirement, there is a request to use DHCP Client Identifier & User Class Options which Ciena 10x SAOS does not support prior to 10.6.0 release.

* SAOS 10x devices must support CLI configurable DHCPv4 Client Identifier Option 61 & DHCPv6 Option 1 as stated in below table.
* Ciena must support DHCP User class Option 77 & Option 15 and it must contain make, model, and software version separated by a delimiter (i.e. Vendor, Model, OS\_Version) & configured/visible in DHCPv4/DHCPv6 packets as per RFC 3004/RFC 3315.

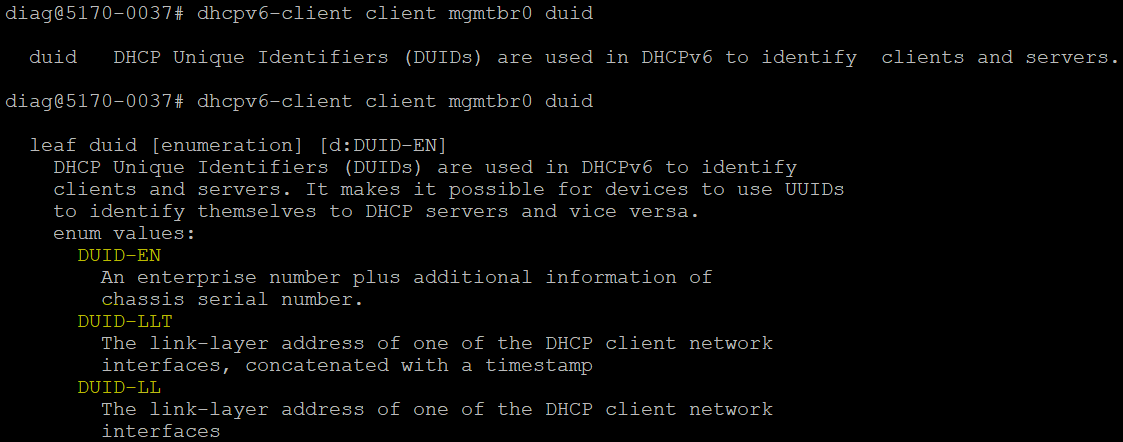
|  |  |  |  |
| --- | --- | --- | --- |
| **DHCP Option** | **Version** | **Option Type** | **Identification Factor** |
| 61 | DHCPv4 | Client Identifier | IAID-DUID/Chassis-ID/Mac-Address |
| 1 | DHCPv6 | Client Identifier | DUID-EN/DUID-LL/DUID-LLT |
| 77 | DHCPv4 | User Class Option | Vendor, Model, OS-Version |
| 15 | DHCPv6 | User Class Option | Vendor, Model, OS-Version |

***Objective:***

Ensure that with DHCPv6 client enabled, the DHCP Client Identifier Option will be configured via VALCLI to specify their unique identifier & User class string will be configured as Vendor, Model, OS\_Version (Visible in packet Capture). The interface will acquire an IPv6 address automatically, **Only stateful DHCPv6 (no SLAAC) is currently supported.**

***Procedure:***

* Dual IPv4 and IPv6 stack on mgmt. interfaces are supported as of 10.3 and onwards. Enable DHCPv6 client on mgmtbr0/Remote. Ensure that:
  + config
  + dhcpv6-client client mgmtbr0 admin-enable true
  + dhcpv6-client client 'mgmtbr0' duid **DUID-LL**
* Display the **Option 1** Dhcpv6-client DUID config on the node.



* Configure IPv4 static IP on the mgmtbr0 as well.
  + dhcp-client client mgmtbr0 admin-enable false
  + oc-if:interfaces interface mgmtbr0 ipv4 address address

x.x.x.x config ip x.x.x.x prefix-length 20

* + rib vrf default ipv4 x.x.x.x/8 next-hop x.x.x.x description "lab default"

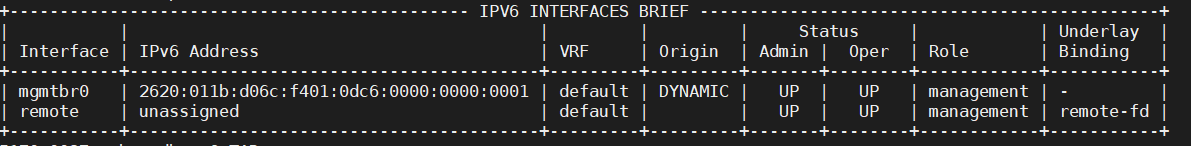
Ex:

dhcp-client client mgmtbr0 admin-enable false

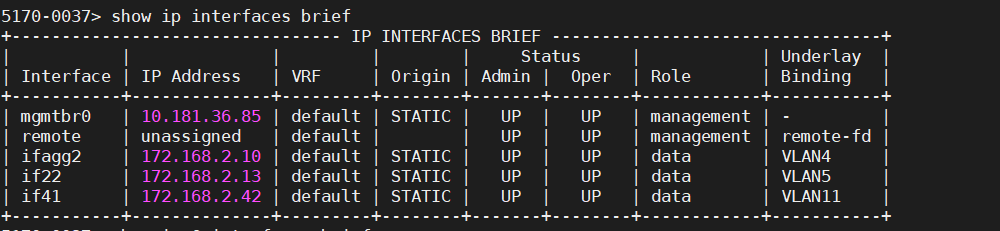
oc-if:interfaces interface mgmtbr0 ipv4 address address 10.181.36.85 config ip 10.181.36.85 prefix-length 20

rib vrf default ipv4 10.0.0.0/8 next-hop 10.181.32.1 description "lab default"

* Display the IPv6 and IPv4 interfaces on the node.
  + 5170-0037> show ipv6 interfaces brief



* + 5170-0037> show ip interfaces brief



5170-0037> show dhcpv6

+-------- DHCPV6 CLIENT CONFIGURATION +

| Name | Value |

+ + +

| Interface Name | **mgmtbr0** |

| Admin State | Enabled |

| Rapid Commit | Enabled |

| Requested Preferred Lifetime (s) | 0 |

| Requested Valid Lifetime (s) | 0 |

**| DUID | DUID-LL |**

| Option | |

| DNS Server List | Enabled |

| Domain Search List | Enabled |

| Posix Time Zone | Disabled |

| TZDB Time Zone | Enabled |

| NTP Server | Enabled |

| Bootfile URL | Enabled |

+ + +

| Interface Name | remote |

| Admin State | Enabled |

| Rapid Commit | Enabled |

| Requested Preferred Lifetime (s) | 0 |

| Requested Valid Lifetime (s) | 0 |

| Option | |

| DNS Server List | Enabled |

| Domain Search List | Enabled |

| Posix Time Zone | Disabled |

| TZDB Time Zone | Enabled |

| NTP Server | Enabled |

| Bootfile URL | Enabled |

+ + +

+ DHCPV6 CLIENT STATE +

| Name | Value |

+ + +

| Interface Name | remote |

| Oper State | Enabled |

| DHCPv6 State | preinit |

| Config State | stateful |

| Renewal (T1) Time (s) | |

| Renewal (T1) Time Remaining (s) | |

| Rebinding (T2) Time (s) | |

| Rebinding (T2) Time Remaining (s) | |

| Preferred Lifetime (s) | |

| Preferred Lifetime Remaining (s) | |

| Valid Lifetime (s) | |

| Valid Lifetime Remaining (s) | |

| DHCPv6 Server DUID | |

| Option Value | |

| DNS Server List | |

| Domain Search List | |

| Posix Time Zone | |

| TZDB Time Zone | |

| NTP servers | |

| Boot File URL | |

+ + +

| Interface Name | mgmtbr0 |

**| Oper State | Enabled |**

**| DHCPv6 State | bound |**

**| Config State | stateful |**

| Renewal (T1) Time (s) | 302400 |

| Renewal (T1) Time Remaining (s) | 241733 |

| Rebinding (T2) Time (s) | 453600 |

| Rebinding (T2) Time Remaining (s) | 392933 |

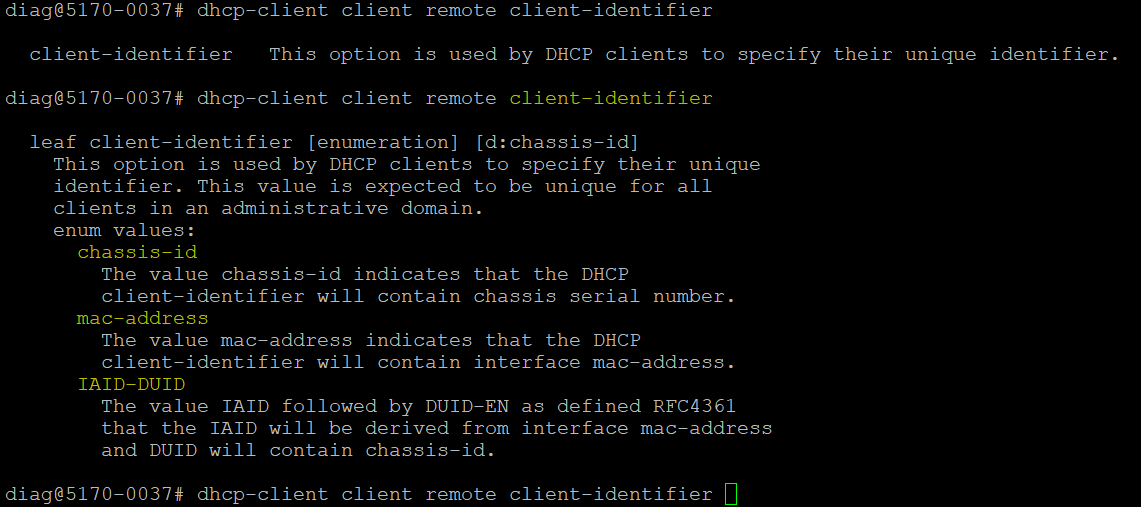
| Preferred Lifetime (s) | 604800 |

| Preferred Lifetime Remaining (s) | 544133 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| | | Valid Lifetime (s) |  | | | 604800 | | |
| | | Valid Lifetime Remaining | (s) | | | 544133 | | |
| | | DHCPv6 Server DUID |  | | | 0:1:0:1:25:22:d:24:0:0:5e:0:1:81 | | |
| | | Option Value |  | | |  | | |
| | | DNS Server List |  | | |  | | |
| | | Domain Search List |  | | |  | | |
| | | Posix Time Zone |  | | |  | | |
| | | TZDB Time Zone |  | | |  | | |
| | | NTP servers |  | | |  | | |
| | | Boot File URL |  | | |  | | |
| + |  |  | + |  | + |

NOTE: The above steps can be also used for dhcpv4-client by configuring the mgmtbr0 or remote interface as dynamic Mgmt IPv4 setup and Static Mgmt IPv6 setup.

* + config
  + dhcp-client client 'remote' admin-enable true
  + dhcp-client client remote client-identifier **IAID-DUID**
* Display the **Option 61** Dhcpv4-client config on the node.



5170-0037> show dhcp

+------------ DHCP CLIENT CONFIGURATION +

| Name | Value |

+ + +

| Interface Name | mgmtbr0 |

| Admin State | Disabled |

| Lease Time (s) | 3600 |

| Client Identifer | chassis-id |

| Option | |

| Subnet Mask | Enabled |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| | | Time Offset |  | | | Enabled | | |
| | | Router |  | | | Enabled | | |
| | | Domain Name | Server | | | Enabled | | |
| | | Log Server |  | | | Enabled | | |
| | | Host Name |  | | | Enabled | | |
| | | Domain Name |  | | | Enabled | | |
| | | NTP Servers |  | | | Enabled | | |
| | | Lease Time |  | | | Disabled | | |
| | | Tftp Server | Name | | | Enabled | | |

| Bootfile Name | Enabled |

| Vendor-Identifying Vendor-Specific | Enabled |

+ + +

| Interface Name | remote |

| Admin State | Enabled |

| Lease Time (s) | 3600 |

**| Client Identifer | IAID-DUID |**

| Option | |

| Subnet Mask | Enabled |

| Time Offset | Enabled |

| Router | Enabled |

| Domain Name Server | Enabled |

| Log Server | Enabled |

| Host Name | Enabled |

| Domain Name | Enabled |

| NTP Servers | Enabled |

| Lease Time | Disabled |

| Tftp Server Name | Enabled |

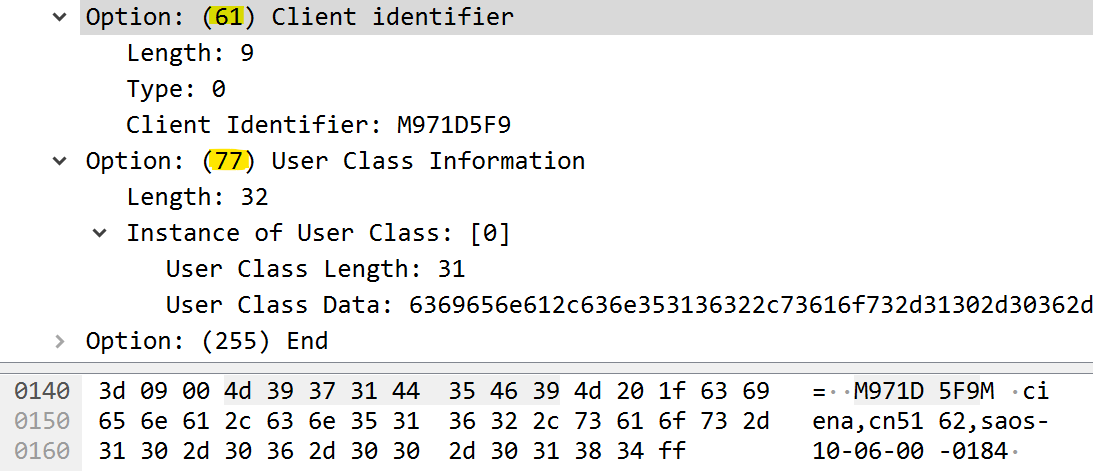
| Bootfile Name | Enabled |

| Vendor-Identifying Vendor-Specific | Enabled |

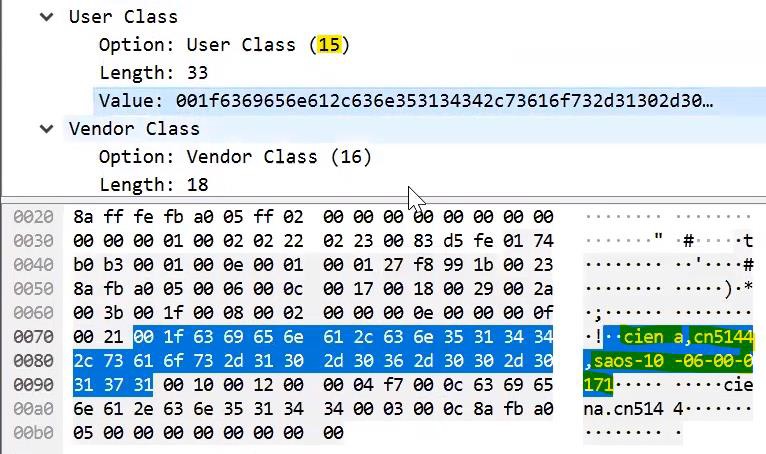
+ + +

* **DHCP User Class Option 77 & 15** will be configured/Visible in DHCPv4/DHCPv6 packets as per RFC 3004/RFC 3315.
* User Class string will be configured as "**ciena,cnXXXX,saos-10-06-00-XXXX**“ Example: "ciena,cn5170,saos-10-06-00-0252".

**Packet Capture of DHCPv4 Client Identifier Option 61 & User Class Option 77:**



**Packet Capture of DHCPv6 User Class Option 15:**



**Test Case Results:**

Passed: Yes No Verified by Date/Time Comments

###### Built in Trial License

Trial License means a License granted to a User or an Organization for a limited duration (90 days), to enable the User or the Organization to evaluate the Software and to do demo of Software Trial Licenses are provided free of charge. This will help FSE and customer to

test devices/software without purchasing the actual license.

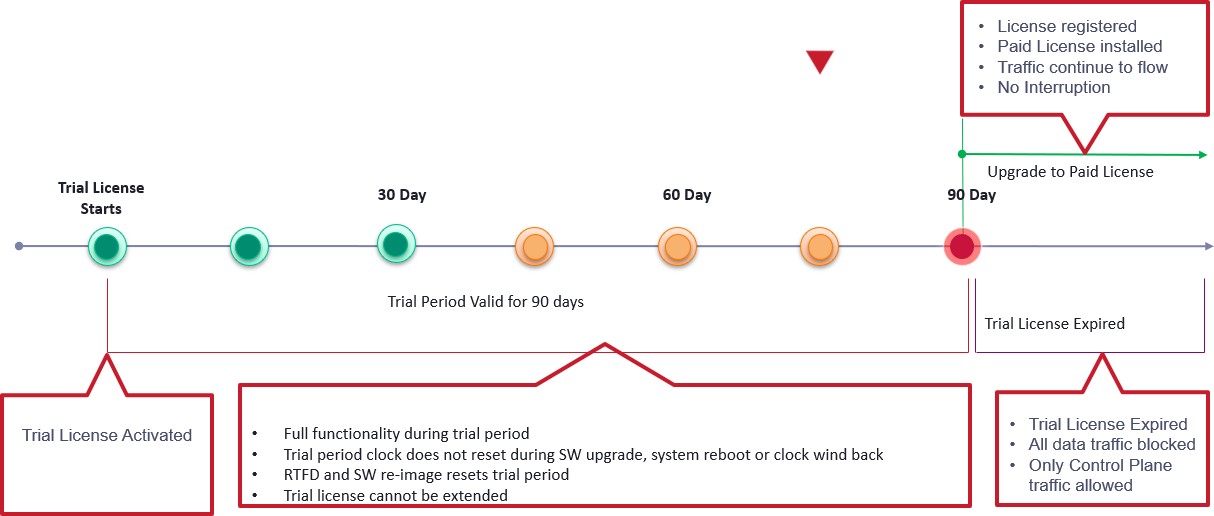
***Objective:***

In earlier releases (SAOS 10.4,SAOS 10.5) we do not have this functionaly. So in order to test device or software we need to register device and purchase license. But now in 10.6 build in trial license support come. A trial license in built come with software which just need to activate and its free. User can use this license for 90 days after that they have to purchage new trial license or permanent license.

On expiration of trial license all data traffic will be block but control traffic will work. User need to purchase license in order to continue services traffic.

Valcli command to activate license on device. Initially no need to download external license:

5164 > license activate built-in-trial-license



#### Functional Behavior

* Temporary, trial/evaluation licenses are built into SW across all Valimar product variants
* Valid only for fixed, pre-defined period (90-Days)
* Enables full feature functionality supported in that SW release for the trial period
* Built-in trial licenses are explicitly activated by user to start the 90-Day trial period
  + Trial period clock does not reset upon clock wind back or SW upgrade or system reboot
  + SW re-image or RTFD on the device will result in a new trial period
* Built-in trial license cannot be extended
  + Extending the trial /period requires a new trial license to be obtained from the portal and installed on the device
  + Moving to paid local(manual)license requires registering the device on the portal, mapping entitlements to device, generating device specific license file and installing it on the device. Once perament license insalled you can not use trial license after that.
* Built-in trial license cannot be extracted out of a SW instance and applied to elsewhere.
* Once the built-in license expires, traffic is blocked in the data plane ;control plane traffic is still allowed
* Acquisition of a paid license(local or server-based) will invalidate the built-in trial license even if the trial period has not expired.

**Note** Event/alarm notification for expiry of built-in license will trigger on 45, 30, 15, 7, 6, 5, 4,

3, 2, 1 day(s) before

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### System gNMI Alarm enhancements

***Requirement:***

* Prior to 10.7.1, the alarm inventory table will show the default severity against each alarm and any user change of severity against each alarm was not displayed.

***Objective:***

* From 10.7.1 onwards, the s/w will display default severity in Alarm Inventory and support Configurable alarm severity as per RFC 8632.
* For each alarm, a maximum of 4 operator state change and 16 system triggered state change history logs will be available for user reference.
* The user can now create multiple alarm shelves with different criteria. The permissible upper limit is 8 shelves.

***Procedure & Configuration:***

* Create alarm profile to configure severity levels of the alarms:
  + alarms alarm-profile <alarm-type-id> <alarm-typequalifier-match>

<resource> alarm-severity-assignmentprofile severity-level <severity- level> <severity-level> <severity-level>

* Configuring alarm history count:
* A. For system triggered alarm state change count:
  + alarms alarm-profile <alarm-type-id> ALL ALL max-alarm-status-changes

<count>

* B. For operator triggered alarm state change count:
  + alarms alarm-profile <alarm-type-id> ALL ALL max-alarm-operator-state- changes <count>
* Set the alarm operator state:
  + alarm set operator-state resource <alarm-resource> type <alarm-type> type-qualifier <alarm-type-qualifier> state <operator-state> text

<text>

***Configuration:***

5164> sh run sec alarms config

alarms control alarm-shelving shelf 'Fan-speed' alarm-type-id fan-max- speed alarm-type-qualifier-match "ALL" resource "r1"

alarms alarm-profile 'interface-fault' 'ALL' 'ALL' description "Test123" max-alarm-status-changes 14 max-alarm-operator-state-changes 3

alarms alarm-profile 'interface-fault' 'ALL' 'ALL' alarm-severity- assignment-profile severity-level critical

5164>

***Verification:***

5164> show alarm inventory alarm-type interface-fault

+

| Type

+

ALARM INVENTORY

| Qualifier | Severity | Description

+

+

+

+

|

+

| interface-fault | | critical | Interface oper state change |

+

5164-201-A>

+

+

+

+

Text

Description automatically generated

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

* + 1. **SNMP Setup *– Through Netconf/YANG***

***Objective:***

Objective is to enable SNMP through Netconf/Yang. It is much easier to go through Netconf browser to setup SNMP trap notifications/informs than going through the CLI.

***Procedure:***

* Enter the following RPC call to enable SNMP trap notifications from SAOS 10.x nodes. Please ensure that your Netconf browser has the latest SAOS 10.x Yang modules loaded. Replace the highlighted portion with the appropriate SNMP trap collector server’s IP address.

<?xml version="1.0" encoding="utf-8"?>

<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="">

<edit-config>

<target>

<running/>

</target>

<config>

<snmp:snmp xmlns:snmp="urn:ietf:params:xml:ns:yang:ietf-snmp">

<snmp:target>

<snmp:name>TARG</snmp:name>

<snmp:udp>

<snmp:ip>x.x.x.x</snmp:ip>

</snmp:udp>

<snmp:target-params>PARAMS</snmp:target-params>

<snmp:tag>MY\_TAG</snmp:tag>

<snmp:timeout>1000</snmp:timeout>

<snmp:retries>4</snmp:retries>

</snmp:target>

<snmp:target-params>

<snmp:name>PARAMS</snmp:name>

<snmp:v2c>

<snmp:security-name>SEC-NAME</snmp:security-name>

</snmp:v2c>

</snmp:target-params>

<snmp:community>

<snmp:index>t000001</snmp:index>

<snmp:text-name>public</snmp:text-name>

<snmp:security-name>SEC-NAME</snmp:security-name>

</snmp:community>

<snmp:notify>

<snmp:name>TEST\_NOTIFY</snmp:name>

<snmp:tag>MY\_TAG</snmp:tag>

<snmp:type>trap</snmp:type>

</snmp:notify>

<snmp:vacm>

<snmp:group>

<snmp:name>DefaultVacmGroupV2C</snmp:name>

<snmp:member>

<snmp:security-name>SEC-NAME</snmp:security-name>

<snmp:security-model>v2c</snmp:security-model>

</snmp:member>

<snmp:access>

<snmp:context></snmp:context>

<snmp:security-model>v2c</snmp:security-model>

<snmp:security-level>no-auth-no-priv</snmp:security-level>

<snmp:context-match>exact</snmp:context-match>

<snmp:notify-view>NotifyView</snmp:notify-view>

</snmp:access>

</snmp:group>

<snmp:view>

<snmp:name>NotifyView</snmp:name>

<snmp:include>\*</snmp:include>

</snmp:view>

</snmp:vacm>

</snmp:snmp>

</config>

</edit-config>

</rpc>

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

* + 1. **SNMP Setup *– Through Netconf/YANG***

***Objective:***

Objective is to enable SNMP through Netconf/Yang. It is much easier to go through Netconf browser to setup SNMP trap notifications/informs than going through the CLI.

***Procedure:***

* Enter the following RPC call to enable SNMP trap notifications from SAOS 10.x nodes. Please ensure that your Netconf browser has the latest SAOS 10.x Yang modules loaded. Replace the highlighted portion with the appropriate SNMP trap collector server’s IP address.

<?xml version="1.0" encoding="utf-8"?>

<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="">

<edit-config>

<target>

<running/>

</target>

<config>

<snmp:snmp xmlns:snmp="urn:ietf:params:xml:ns:yang:ietf-snmp">

<snmp:target>

<snmp:name>TARG</snmp:name>

<snmp:udp>

<snmp:ip>x.x.x.x</snmp:ip>

</snmp:udp>

<snmp:target-params>PARAMS</snmp:target-params>

<snmp:tag>MY\_TAG</snmp:tag>

<snmp:timeout>1000</snmp:timeout>

<snmp:retries>4</snmp:retries>

</snmp:target>

<snmp:target-params>

<snmp:name>PARAMS</snmp:name>

<snmp:v2c>

<snmp:security-name>SEC-NAME</snmp:security-name>

</snmp:v2c>

</snmp:target-params>

<snmp:community>

<snmp:index>t000001</snmp:index>

<snmp:text-name>public</snmp:text-name>

<snmp:security-name>SEC-NAME</snmp:security-name>

</snmp:community>

<snmp:notify>

<snmp:name>TEST\_NOTIFY</snmp:name>

<snmp:tag>MY\_TAG</snmp:tag>

<snmp:type>trap</snmp:type>

</snmp:notify>

<snmp:vacm>

<snmp:group>

<snmp:name>DefaultVacmGroupV2C</snmp:name>

<snmp:member>

<snmp:security-name>SEC-NAME</snmp:security-name>

<snmp:security-model>v2c</snmp:security-model>

</snmp:member>

<snmp:access>

<snmp:context></snmp:context>

<snmp:security-model>v2c</snmp:security-model>

<snmp:security-level>no-auth-no-priv</snmp:security-level>

<snmp:context-match>exact</snmp:context-match>

<snmp:notify-view>NotifyView</snmp:notify-view>

</snmp:access>

</snmp:group>

<snmp:view>

<snmp:name>NotifyView</snmp:name>

<snmp:include>\*</snmp:include>

</snmp:view>

</snmp:vacm>

</snmp:snmp>

</config>

</edit-config>

</rpc>

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### SNMP v2c Inform Configuration

***SNMP v2c Inform:***

* + - * Informs are same as Traps but the main difference is that the Informs are acknowledged back by the SNMP Manager.
      * SNMP Inform are enabled by specifying the type as ‘inform’ whereas type ‘trap’ will be used

for SNMP traps.

***Procedure:***

snmp community t1 security-name cienaSecurityV2c text-name cienaV2cCommunity snmp vacm view cienaAll include internet

snmp vacm group cienaGroup access "" v2c no-auth-no-priv context-match exact notify-view cienaAll

snmp vacm group cienaGroup member cienaSecurityV2c security-model v2c snmp target TestTarget1 target-params TestParamsV2c udp ip 10.176.137.38 snmp target-params TestParamsV2c v2c security-name cienaSecurityV2c snmp target TestTarget1 tag TestTag

snmp notify Test-NOTIFY1 type inform tag TestTag

***Output:***

* show snmp

+

SNMP NOTIFY +

| Notification Name | Notification Tag | Notification Type |

+ + + +

| Test-NOTIFY1 | TestTag | inform |

+ + + +

+ SNMP COMMUNITY +

| Community Index | Community Name | Security Name | Transport Tag |

+ + + + +

| t1 | cienaV2cCommunity | cienaSecurityV2c | |

+ + + + +

+ SNMP TARGET-PARAMS +

| Target Param Name | Security Name | User Name | Security Model | Security Level |

+ + + + + +

| TestParamsV2c | cienaSecurityV2c | | v2c | no-auth-no-priv |

+ + +

+

+ + +

SNMP TARGET +

| Target Name | IP Address | Param Name | Tags | UDP Port | Retry Count | Timeout | Prefix Length |

+ + + + + + + + +

| TestTarget1 | 10.176.137.38 | TestParamsV2c | TestTag | 162 | 3 | 1500 | 32 |

+ + + + + + + + +

+ SNMP VACM VIEW +

| Viewtree Name | Subtree | Type |

+ + + +

| cienaAll | internet | include |

+ + + +

+------------ SNMP VACM GROUP MEMBER +

| Group Name | Security Model | Security Name |

+ + + +

| cienaGroup | v2c | cienaSecurityV2c |

+ + +

+

+

SNMP VACM GROUP ACCESS +

| Group Name | Context | Context Match | Security Model | Security Level | Read View | Notify View |

+ + + + + + + +

| cienaGroup | | exact | v2c | no-auth-no-priv | | cienaAll |

+ + + + + + + +

***Test Case Results:***

Passed: Yes No Verified by Date/Time Comments

###### SNMP v2c Inform Configuration

***SNMP v2c Inform:***

* + - * Informs are same as Traps but the main difference is that the Informs are acknowledged back by the SNMP Manager.
      * SNMP Inform are enabled by specifying the type as ‘inform’ whereas type ‘trap’ will be used

for SNMP traps.

***Procedure:***

snmp community t1 security-name cienaSecurityV2c text-name cienaV2cCommunity snmp vacm view cienaAll include internet

snmp vacm group cienaGroup access "" v2c no-auth-no-priv context-match exact notify-view cienaAll

snmp vacm group cienaGroup member cienaSecurityV2c security-model v2c snmp target TestTarget1 target-params TestParamsV2c udp ip 10.176.137.38 snmp target-params TestParamsV2c v2c security-name cienaSecurityV2c snmp target TestTarget1 tag TestTag

snmp notify Test-NOTIFY1 type inform tag TestTag

***Output:***

* show snmp

+

SNMP NOTIFY +

| Notification Name | Notification Tag | Notification Type |

+ + + +

| Test-NOTIFY1 | TestTag | inform |

+ + + +

+ SNMP COMMUNITY +

| Community Index | Community Name | Security Name | Transport Tag |

+ + + + +

| t1 | cienaV2cCommunity | cienaSecurityV2c | |

+ + + + +

+ SNMP TARGET-PARAMS +

| Target Param Name | Security Name | User Name | Security Model | Security Level |

+ + + + + +

| TestParamsV2c | cienaSecurityV2c | | v2c | no-auth-no-priv |

+ + +

+

+ + +

SNMP TARGET +

| Target Name | IP Address | Param Name | Tags | UDP Port | Retry Count | Timeout | Prefix Length |

+ + + + + + + + +

| TestTarget1 | 10.176.137.38 | TestParamsV2c | TestTag | 162 | 3 | 1500 | 32 |

+ + + + + + + + +

+ SNMP VACM VIEW +

| Viewtree Name | Subtree | Type |

+ + + +

| cienaAll | internet | include |

+ + + +

+------------ SNMP VACM GROUP MEMBER +

| Group Name | Security Model | Security Name |

+ + + +

| cienaGroup | v2c | cienaSecurityV2c |

+ + +

+

+

SNMP VACM GROUP ACCESS +

| Group Name | Context | Context Match | Security Model | Security Level | Read View | Notify View |

+ + + + + + + +

| cienaGroup | | exact | v2c | no-auth-no-priv | | cienaAll |

+ + + + + + + +

***Test Case Results:***

Passed: Yes No Verified by Date/Time Comments

###### SNMP v3 Trap Configuration

***Objective:***

The objective of this section is to configure SNMP v3 Trap on the SAOS cli.

***SNMPv3 Trap:***

* + - * Same as the SNMP GET parameters but additional fields are added to specify the Trap target IP.

***Procedure:***

snmp usm local user cienaNoAuthNoPrivUser exit

exit exit exit

snmp usm local user cienaAuthNoPrivUser auth md5 key 63:69:65:6e:61:41:75:74:68:4b:65:79 snmp usm local user cienaAuthPrivUser auth md5 key 63:69:65:6e:61:41:75:74:68:4b:65:79 snmp usm local user cienaAuthPrivUser priv des key 63:69:65:6e:61:50:72:69:76:4b:65:79

snmp vacm group cienaV3Group access "" usm no-auth-no-priv context-match exact notify-view cienaAll

snmp vacm group cienaV3Group access "" usm auth-no-priv context-match exact notify-view cienaAll

snmp vacm group cienaV3Group access "" usm auth-priv context-match exact notify-view cienaAll snmp vacm group cienaV3Group member cienaNoAuthNoPrivUser security-model usm

snmp vacm group cienaV3Group member cienaAuthNoPrivUser security-model usm snmp vacm group cienaV3Group member cienaAuthPrivUser security-model usm snmp target TestTarget2 target-params TestUsmNoAuthNoPriv udp ip 10.176.137.38 snmp target TestTarget2 tag TestTag

snmp target TestTarget3 target-params TestUsmAuthNoPriv udp ip 10.176.137.38 snmp target TestTarget3 tag TestTag

snmp target TestTarget4 target-params TestUsmAuthPriv udp ip 10.176.137.38 snmp target TestTarget4 tag TestTag

snmp target-params TestUsmNoAuthNoPriv usm security-level no-auth-no-priv user-name cienaNoAuthNoPrivUser

snmp target-params TestUsmAuthNoPriv usm security-level auth-no-priv user-name cienaAuthNoPrivUser

snmp target-params TestUsmAuthPriv usm security-level auth-priv user-name cienaAuthPrivUser snmp vacm view cienaAll include internet

snmp notify Test-NOTIFY tag TestTag type trap

***Output:***

* show snmp

+

SNMP NOTIFY +

| Notification Name | Notification Tag | Notification Type |

+ + + +

| Test-NOTIFY | TestTag | trap |

+ + +

+

+

SNMP USM +

| User Name | Type | Auth Protocol | Priv Protocol | Engine ID |

+ + + + + +

| cienaNoAuthNoPrivUser | local | | | 80:00:05:23:01:0A:78:67:F8:00:00 |

| cienaAuthNoPrivUser | local | md5 | | 80:00:05:23:01:0A:78:67:F8:00:00 |

| cienaAuthPrivUser | local | md5 | des | 80:00:05:23:01:0A:78:67:F8:00:00 |

+ + +

+

+ + +

SNMP TARGET-PARAMS +

| Target Param Name | Security Name | User Name | Security Model | Security Level |

+ + + + + +

| TestUsmNoAuthNoPriv | | cienaNoAuthNoPrivUser | usm | no-auth-no-priv |

| TestUsmAuthNoPriv | | cienaAuthNoPrivUser | usm | auth-no-priv |

| TestUsmAuthPriv | | cienaAuthPrivUser | usm | auth-priv |

+ + +

+

+ + +

SNMP TARGET +

| Target Name | IP Address | Param Name | Tags | UDP Port | Retry Count | Timeout | Prefix Length |

+ + + + + + + + +

| TestTarget2 | 10.176.137.38 | TestUsmNoAuthNoPriv | TestTag | 162 | 3 | 1500 | 32 |

| TestTarget3 | 10.176.137.38 | TestUsmAuthNoPriv | TestTag | 162 | 3 | 1500 | 32 |

| TestTarget4 | 10.176.137.38 | TestUsmAuthPriv | TestTag | 162 | 3 | 1500 | 32 |

+ + +

+ SNMP VACM VIEW +

+ + + + + +

| Viewtree Name | Subtree | Type |

+ + + +

| cienaAll | internet | include |

+ + + +

+ SNMP VACM GROUP MEMBER +

| Group Name | Security Model | Security Name |

+ + + +

| cienaV3Group | usm | cienaNoAuthNoPrivUser |

| cienaV3Group | usm | cienaAuthNoPrivUser |

| cienaV3Group | usm | cienaAuthPrivUser |

+ + +

+

+

SNMP VACM GROUP ACCESS +

| Group Name | Context | Context Match | Security Model | Security Level | Read View | Notify View |

+ + + + + + + +

| cienaV3Group | | exact | usm | no-auth-no-priv | | cienaAll |

| cienaV3Group | | exact | usm | auth-no-priv | | cienaAll |

| cienaV3Group | | exact | usm | auth-priv | | cienaAll |

+ + + + + + + +

***Test Case Results:***

Passed: Yes No Verified by Date/Time Comments

###### SNMP v3 Trap Configuration

***Objective:***

The objective of this section is to configure SNMP v3 Trap on the SAOS cli.

***SNMPv3 Trap:***

* + - * Same as the SNMP GET parameters but additional fields are added to specify the Trap target IP.

***Procedure:***

snmp usm local user cienaNoAuthNoPrivUser exit

exit exit exit

snmp usm local user cienaAuthNoPrivUser auth md5 key 63:69:65:6e:61:41:75:74:68:4b:65:79 snmp usm local user cienaAuthPrivUser auth md5 key 63:69:65:6e:61:41:75:74:68:4b:65:79 snmp usm local user cienaAuthPrivUser priv des key 63:69:65:6e:61:50:72:69:76:4b:65:79

snmp vacm group cienaV3Group access "" usm no-auth-no-priv context-match exact notify-view cienaAll

snmp vacm group cienaV3Group access "" usm auth-no-priv context-match exact notify-view cienaAll

snmp vacm group cienaV3Group access "" usm auth-priv context-match exact notify-view cienaAll snmp vacm group cienaV3Group member cienaNoAuthNoPrivUser security-model usm

snmp vacm group cienaV3Group member cienaAuthNoPrivUser security-model usm snmp vacm group cienaV3Group member cienaAuthPrivUser security-model usm snmp target TestTarget2 target-params TestUsmNoAuthNoPriv udp ip 10.176.137.38 snmp target TestTarget2 tag TestTag

snmp target TestTarget3 target-params TestUsmAuthNoPriv udp ip 10.176.137.38 snmp target TestTarget3 tag TestTag

snmp target TestTarget4 target-params TestUsmAuthPriv udp ip 10.176.137.38 snmp target TestTarget4 tag TestTag

snmp target-params TestUsmNoAuthNoPriv usm security-level no-auth-no-priv user-name cienaNoAuthNoPrivUser

snmp target-params TestUsmAuthNoPriv usm security-level auth-no-priv user-name cienaAuthNoPrivUser

snmp target-params TestUsmAuthPriv usm security-level auth-priv user-name cienaAuthPrivUser snmp vacm view cienaAll include internet

snmp notify Test-NOTIFY tag TestTag type trap

***Output:***

* show snmp

+

SNMP NOTIFY +

| Notification Name | Notification Tag | Notification Type |

+ + + +

| Test-NOTIFY | TestTag | trap |

+ + +

+

+

SNMP USM +

| User Name | Type | Auth Protocol | Priv Protocol | Engine ID |

+ + + + + +

| cienaNoAuthNoPrivUser | local | | | 80:00:05:23:01:0A:78:67:F8:00:00 |

| cienaAuthNoPrivUser | local | md5 | | 80:00:05:23:01:0A:78:67:F8:00:00 |

| cienaAuthPrivUser | local | md5 | des | 80:00:05:23:01:0A:78:67:F8:00:00 |

+ + +

+

+ + +

SNMP TARGET-PARAMS +

| Target Param Name | Security Name | User Name | Security Model | Security Level |

+ + + + + +

| TestUsmNoAuthNoPriv | | cienaNoAuthNoPrivUser | usm | no-auth-no-priv |

| TestUsmAuthNoPriv | | cienaAuthNoPrivUser | usm | auth-no-priv |

| TestUsmAuthPriv | | cienaAuthPrivUser | usm | auth-priv |

+ + +

+

+ + +

SNMP TARGET +

| Target Name | IP Address | Param Name | Tags | UDP Port | Retry Count | Timeout | Prefix Length |

+ + + + + + + + +

| TestTarget2 | 10.176.137.38 | TestUsmNoAuthNoPriv | TestTag | 162 | 3 | 1500 | 32 |

| TestTarget3 | 10.176.137.38 | TestUsmAuthNoPriv | TestTag | 162 | 3 | 1500 | 32 |

| TestTarget4 | 10.176.137.38 | TestUsmAuthPriv | TestTag | 162 | 3 | 1500 | 32 |

+ + +

+ SNMP VACM VIEW +

+ + + + + +

| Viewtree Name | Subtree | Type |

+ + + +

| cienaAll | internet | include |

+ + + +

+ SNMP VACM GROUP MEMBER +

| Group Name | Security Model | Security Name |

+ + + +

| cienaV3Group | usm | cienaNoAuthNoPrivUser |

| cienaV3Group | usm | cienaAuthNoPrivUser |

| cienaV3Group | usm | cienaAuthPrivUser |

+ + +

+

+

SNMP VACM GROUP ACCESS +

| Group Name | Context | Context Match | Security Model | Security Level | Read View | Notify View |

+ + + + + + + +

| cienaV3Group | | exact | usm | no-auth-no-priv | | cienaAll |

| cienaV3Group | | exact | usm | auth-no-priv | | cienaAll |

| cienaV3Group | | exact | usm | auth-priv | | cienaAll |

+ + + + + + + +

***Test Case Results:***

Passed: Yes No Verified by Date/Time Comments