###### 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

###### 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

###### 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 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

###### 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

###### 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

###### 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"

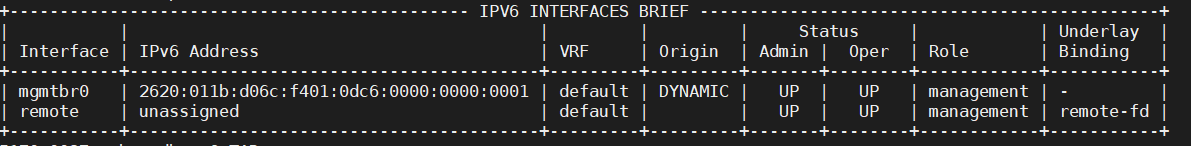
Ex:

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

###### 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

###### 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

###### **SNMP Configuration - CLI**

***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 Configuration - CLI**

***Objective:***

The objective of this section is to configure SNMP v1, v2c and v3 on the SAOS cli.

***SNMP v1 Get:***

* + - * Configure a community of your choice for authentication.
      * Define the MIB views and set the read access permissions.
      * Finally set the security model as v1 for setting up SNMPv1.

***Procedure:***

snmp community t0 security-name cienaSecurityV1 text-name cienaV1Community snmp vacm view cienaAll include internet

snmp vacm group cienaGroup access "" v1 no-auth-no-priv context-match exact read-view cienaAll snmp vacm group cienaGroup member cienaSecurityV1 security-model v1

***Output:***

* show snmp

+

SNMP COMMUNITY +

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

+ + + + +

| t0 | cienaV1Community | cienaSecurityV1 | |

+ + + + +

+ SNMP VACM VIEW +

| Viewtree Name | Subtree | Type |

+ + + +

| cienaAll | internet | include |

+ + + +

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

| Group Name | Security Model | Security Name |

+ + + +

| cienaGroup | v1 | cienaSecurityV1 |

+ + +

+

+

SNMP VACM GROUP ACCESS +

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

+ + + + + + + +

| cienaGroup | | exact | v1 | no-auth-no-priv | cienaAll | |

+ + + + + + + +

***Test Case Results:***

Passed: Yes No Verified by Date/Time Comments

***SNMP v1 Trap:***

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

***Procedure:***

snmp community t0 security-name cienaSecurityV1 text-name cienaV1Community snmp vacm view cienaAll include internet

snmp vacm group cienaGroup access "" v1 no-auth-no-priv context-match exact notify-view cienaAll snmp vacm group cienaGroup member cienaSecurityV1 security-model v1

snmp target-params TestParams v1 security-name cienaSecurityV1 snmp target TestTarget target-params TestParams udp ip 10.176.137.38 snmp target TestTarget tag TestTag

***Output:***

* show snmp

+

SNMP COMMUNITY +

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

+ + + + +

| t0 | cienaV1Community | cienaSecurityV1 | |

+ + + + +

+ SNMP TARGET-PARAMS +

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

+ + + + + +

| TestParams | cienaSecurityV1 | | v1 | no-auth-no-priv |

+ + +

+

+ + +

SNMP TARGET +

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

+ + + + + + + + +

| TestTarget | 10.176.137.38 | TestParams | 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 | v1 | cienaSecurityV1 |

+ + +

+

+

SNMP VACM GROUP ACCESS +

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

+ + + + + + + +

| cienaGroup | | exact | v1 | 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

###### 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

###### 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

###### 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

###### 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

###### WebGUI – Management of Sessions

***Objective:***

Validate WebGUI can be enabled and disabled. Please note that WebGUI is not supported on all platforms, for example 3926 and 3928 platforms do not support WebGUI.

***Procedure:***

* Display current web-gui state:

show web-gui state

5166-004> show web-gui state

+----- WEBGUI +

| Name | Value |

+ + +

| State | Disabled |

+ + +

* Enable Web GUI. This Web GUI can take a couple of minutes before it is fully enabled.

set web-gui state enable

* Display the Web GUI state again, after waiting for a couple of minutes.

5166-004> show web-gui state

+----- WEBGUI +

| Name | Value |

+ + +

| State | Enabled |

+ + +

* Go to a web browser and enter the node’s IP address. This may take a few minutes before

the GUI becomes available.

Enter URL https://x.x.x.x/

Graphical user interface

Description automatically generated

* Login using default or created user account – default is : **diag/ciena123.** Wait for GUI to launch. This may take a few minutes.
* Display the webUI sessions on the CLI. Up to 3 concurrent sessions are supported. Show web-gui session

5166-004> show web-gui session

+ WEBGUI SERVER SESSIONS +

| ID | Client | User | Last Access |

+ + + + +

| 1 | 169.254.160.50 | diag | 2020-12-16 07:22:14 PM |

+ + + + +

* Use the following command to kill a session. **unset web-gui session id 1** 5166-004> unset web-gui session id 1

+ WEBGUI SERVER SESSIONS +

| ID | Message |

+ + +

| 1 | User ID 1 killed. |

+ + +

The webGUI session was logged out.

Graphical user interface, website

Description automatically generated

* To disable the web GUI, enter the following command :

set web-gui state disable

* Display the state of the WEB GUI to ensure that it is disabled.

show web-gui state

5166-004> show web-gui state

+----- WEBGUI +

| Name | Value |

+ + +

| State | Disabled |

+ + +

\*\*For more WebGUI examples, please see Appendix A.

Test Case Results:

Passed: Yes No Verified by Date/Time Comments