###### 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.

Make sure System is configured with Golden config.

* + - 1. Perform reset-to-golden-config on the system. Steps to create golden-config is given in Procedures section below.
      2. Execute ‘show ztp’ and Verify ‘ZTP State’ is ‘activating’.
      3. Executed ‘show software’ and Verify image downloading started successfully.
      4. 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

* + - 1. 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