How to replace SSL certificates on cluster with external key manager configured

Applies to

- Data ONTAP 8
- ONTAP 9
- external key manager

Description

The external key management server is a third-party system in your storage environment that serves
authentication keys to nodes using the Key Management Interoperability Protocol (KMIP). The cluster and KMIP server use KMIP SSL certificates to verify each other's identity and establish an SSL connection.

**Before you begin:**

- The time must be synchronized on the server creating the certificates, the KMIP server, and the cluster
- Backup the current certificates off box.
- You must use the currently installed NSE private key (client_private.key) to generate the renewal certificate signing request (client.csr) if not generating new authentication keys
- The client.csr file must be sent to the CA for signing and once signed becomes the NSE public certificate (client.pem)
- You must have obtained the CA public certificate for the root certificate authority (CA) of the KMIP server (CA.pem)
- Verify PEM files using any computer that has OpenSSL installed and is able to communicate with the KMIP server.

**Note:** You can install the client and server certificates on the KMIP server before or after installing the certificates on the cluster.