Setting up TLS for ALM Octane and Elasticsearch

Setting up TLS allows ALM Octane to communicate with Elasticsearch in a secure manner.

ALM Octane supports using X-pack security, which is free in version 6.8. Using a version lower than 6.8 will result in the security features not working without a paid license.

Note: ALM Octane currently only supports Elasticsearch 6.x. Do not upgrade to version 7.x.

Note: If you're using https / SSL to secure your web server do not use the same certificate to secure elasticsearch communication. Elasticsearch search should use a dedicated certificate to improve security.

Configure Elasticsearch server

In order to set up a TLS connection between ALM Octane and Elasticsearch please follow the official Elasticsearch instructions.

Here are some guidelines to getting the most out of the official instructions:

- To simplify the installation, ALM Octane supports the pkcs#12 format which is the recommended default for Elasticsearch. If you decide to use the PEM format, you'll need to convert the PEMS into a PKCS#12 store.
- Using the elastic search certutil to generate certificates will make configuration simpler, and no less secure.
- Make sure you set strong passwords on all certificate keys, and make sure you store them in a safe location.
- You only need to follow steps 1 and 2 to get ALM Octane to work. Encrypting http communication is optional, but highly recommended.
- If you enable TLS, you must also configure authentication and use username authentication.
- If possible, use hostname verification as it adds another layer of security. Using hostname verification means you will have to generate a certificate for each host/server that you're setting up including each octane server. If you decide to skip host verification, only one certificate is needed to connect all nodes/servers.

Verify Elasticsearch server configuration

Before you start configuring ALM Octane:

- Verify you can access the cluster over https with the user you configured, before you set up ALM Octane. You can do that by accessing https://<your elastic Server>:9200/_cluster/health with the user you configured. You should be able to see the cluster status and the number of nodes should match the number of nodes you are trying to bring up (typically 3).

- If you don't get to cluster health or the number of number of nodes does not match go over the logs of every node. Make sure they all came up successfully by looking for the line
  [Node name] started
  and if any of the nodes don't show this line, go through the logs and fix any errors that may show up there.

Configure ALM Octane Server

Once you have authentication and TLS set up for Elasticsearch, perform the following steps:

1. Generate / copy TLS certificate to ALM Octane server

Generate an additional certificate/key pair for each ALM Octane server. If you're not using hostname verification, you can use the same certificate you used for the Elasticsearch nodes.

Copy the pkcs#12 file that contains your root certificate (truststore) and the pkcs#12 file that contains your node certificate and key to ALM Octane's "conf" folder. The two certificates can be one file. In that case only copy the single file.

2. Fill in new Elasticsearch TLS values in setup.xml

Fill in the following values in setup.xml:

1. ElasticUserName - The username to use when authenticating against Elasticsearch.
2. ElasticPassword (Encrypted) - The password of the Elasticsearch user.
3. ElasticKeystoreFile - The name of the PKCS12 keystore file. The file should be placed in the configuration folder.
4. ElasticKeystorePassword (optional, encrypted) - The password to use to open the keystore file if the store is password protected.
5. ElasticTruststoreFile - The name of the PKCS12 truststore file. The file should be placed in the configuration folder.
6. ElasticTruststorePassword (optional, encrypted) - The password to use to open the truststore file if the store is password protected.
7. ElasticVerificationMode - none/certificate/full - Determine the level used when verifying the certificate:
   a. none - no certificate verification checks are made. This means that any certificate will be accessed and should only be sued to debug issues.
   b. certificate - only checks that the certificate is signed by a trusted CA. Should be used when hosts are dynamic.
   c. full - in addition to certificate, also checks that the host name reported by the certificate matches the host the request is coming from. Should be used whenever possible and is the default.

3. Start ALM Octane server

Verify ALM Octane Server Configuration

Monitor the wrapper.log to make sure no errors are thrown and the ALM Octane server is coming up properly.

Once the ALM Octane server is up, run a global search and make sure you get results.

Open an “over time” graph and make sure you get results.