Configure SSL for the Storm UI

You can configure SSL for the Storm UI on a secure or non-secure cluster.

If you want to configure SSL for the Storm UI on a secure cluster, the ssl_keystore must be available in the following location: `/opt/mapr/conf` .

1. On a non-secure cluster, complete the following steps to generate the keystore:

    a. Generate a keystore (keystore.jks) with a private key.

    ```
    keytool -genkeypair -alias certificatekey -keyalg RSA -validity 7 -keystore keystore.jks
    ```

    Example output and input when using the keytool to generate a key:

    ```
    Enter keystore password:    mapr123
    Re-enter new password: mapr123
    What is your first and last name?  [Unknown]: localhost (Important! Enter your hostname here)
    What is the name of your organizational unit?  [Unknown]: 1
    What is the name of your organization?  [Unknown]: 2
    What is the name of your City or Locality?  [Unknown]: 3
    What is the name of your State or Province?  [Unknown]: 4
    What is the two-letter country code for this unit?  [Unknown]: UA
    Is CN=mapr50,OU=1, O=2, L=3, ST=4, C=UA correct?  [no]: yes
    Enter key password for <certificatekey> (RETURN if same as keystore password): (Press enter)
    ```

    b. Generate a certificate from the keystore.

    ```
    keytool -export -alias certificatekey -keystore keystore.jks -rfc -file cert.pem
    ```

    Example input and output when generating a certificate:

    ```
    Enter keystore password:  mapr123
    Certificate is stored in file <cert.pem>
    ```

    c. Import the keystore from JKS to PKCS12.
    For example:

    ```
    keytool -importkeystore -srckeystore keystore.jks -destkeystore keystore.p12 -srcstoretype JKS -deststoretype PKCS12 -srcstorepass m
    apr123 -deststorepass mapr123 -srcalias certificatekey -destalias certificatekey -srckeypass mapr123 -destkeypass mapr123 -noprompt
    ```

    d. Convert PKCS12 to PEM using OpenSSL.
    For example:

    ```
    openssl pkcs12 -in keystore.p12 -out keystore.pem -passin pass:mapr123 -passout pass:mapr123
    ```

2. Add the following properties to `/opt/mapr/storm/storm-<version>/conf/storm.yaml`:
    - ui.https.port
    - ui.https.keystore.type
    - ui.https.keystore.path
    - ui.https.keystore.password
    - ui.https.key.password

    For example:

    ```
    # UI SSL
    ui.https.port: 8080
    ui.https.keystore.type: "jks"
    ui.https.keystore.path: "/etc/ssl/keystore.jks"
    ui.https.keystore.password: "mapr123"
    ui.https.key.password: "mapr123"
    ```

    📒 **Note:** On a secure cluster, set `ui.https.keystore.path: "/opt/mapr/conf/ssl_keystore"`

3. Restart Storm Services. See Manage Storm Services (Storm_ManageServices.html)

4. Open the Storm UI in a web browser.
    Navigate to https://<host>:<port> where the <host> is the name of the host where Nimbus is running and the <port> is the value that you assigned to
    `ui.https.port` in the storm.yaml file.

5. Start the topology. See Manage Storm Topologies (Storm_ManageTopologies.html)