CloudCenter-Zertifikat in Jenkins Java Keystore importieren

Inhalt

Einführung

Dieses Dokument beschreibt, wie das CloudCenter-Zertifikat in Jenkins Java-Keystore importiert wird.

Unterstützt von Deepak Sukhiya, Cisco TAC Engineer.

Anwendungsversion

CloudCenter Manager 4.0 / 4.2.x /4.4.x /4.5.x / 4.6.x/ 4.7.x / 4.8.0

Problem

Importieren des CloudCenter-Zertifikats in Jenkins Java-Keystore

oder

Validieren der Verbindung aus dem Menü **Projekt > Konfigurieren** schlägt fehl, wenn der Fehler im Jenkins-Protokoll auftritt:

```
Building in workspace /var/lib/jenkins/workspace/C3-Cent7
ERROR: Build step failed with exception
javax.ws.rs.ProcessingException: javax.net.ssl.SSLHandshakeException:
sun.security.validator.ValidatorException: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification
path to requested target
at org.glassfish.jersey.client.HttpUrlConnector.apply(HttpUrlConnector.java:229)
at org.glassfish.jersey.client.ClientRuntime.invoke(ClientRuntime.java:224)
at org.glassfish.jersey.client.JerseyInvocation$1.call(JerseyInvocation.java:656)
at org.glassfish.jersey.client.JerseyInvocation$1.call(JerseyInvocation.java:653)
at org.glassfish.jersey.internal.Errors.process(Errors.java:315)
at org.glassfish.jersey.internal.Errors.process(Errors.java:297)
at org.glassfish.jersey.internal.Errors.process(Errors.java:228)
at org.glassfish.jersey.process.internal.RequestScope.runInScope(RequestScope.java:424)
at org.glassfish.jersey.client.JerseyInvocation.invoke(JerseyInvocation.java:653)
at org.glassfish.jersey.client.JerseyInvocation$Builder.method(JerseyInvocation.java:388)
at org.glassfish.jersey.client.JerseyInvocation$Builder.get(JerseyInvocation.java:292)
at cliqr.jenkins.plugin.CliQrJenkinsClient.RestUtils.getAppDetails(RestUtils.java:156)
at
cliqr.jenkins.plugin.CliQrJenkinsClient.CliQrJenkinsClientBuilder.perform(CliQrJenkinsClientBuil
der.java:243)
```

```
at hudson.tasks.BuildStepMonitor$1.perform(BuildStepMonitor.java:20)
at hudson.model.AbstractBuild$AbstractBuildExecution.perform(AbstractBuild.java:779)
at hudson.model.Build$BuildExecution.build(Build.java:205)
at hudson.model.Build$BuildExecution.doRun(Build.java:162)
at hudson.model.AbstractBuild$AbstractBuildExecution.run(AbstractBuild.java:534)
at hudson.model.Run.execute(Run.java:1728)
at hudson.model.FreeStyleBuild.run(FreeStyleBuild.java:43)
at hudson.model.ResourceController.execute(ResourceController.java:98)
at hudson.model.Executor.run(Executor.java:404)
Caused by: javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: PKIX
path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find
valid certification path to requested target
at sun.security.ssl.Alerts.getSSLException(Alerts.java:192)
```

Lösung

1. Melden Sie sich über Firefox beim CloudCenter Manager-Computer (CCM) an.
2. Zeigen Sie das CloudCenter-Zertifikat mit dem Vorhängeschlosssymbol im Browser an, und speichern Sie es.
3. Kopieren Sie das Zertifikat auf den Jenkins-Rechner.
4. Melden Sie sich über Secure Shell (SSH) beim Jenkins-System an.
5. Führen Sie diesen Befehl auf dem Jenkins-Computer aus: **keytool -import -trustcacerts -alias example -keystore <Pfad zum Java-Pfad ersetzen>/jre/lib/security/cacerts -file <Ort der gespeicherten Zertifikatsdatei>.**
6. Die Authentifizierung des CloudCenter wird ordnungsgemäß validiert.