Allgemeine Anweisungen für die Installation eines neuen SSL-Zertifikats auf dem BMC-Server

Erstellungsdatum	Aktualisierungsdatum	Betroffene Version	Fix Version
09 Apr 2020	02 Sep 2022	Alle	

Beschreibung

Diese allgemeinen Anweisungen können verwendet werden, um ein neues SSL-Zertifikat auf einem BMC-Server zu installieren.

Schritt-für-Schritt Anleitung

Aktuelles Zertifikat aus BMC Keystore prüfen:

```
keytool -list -v -keystore “C:\Program Files\Blancco\Blancco Management Console\apache-tomcat\conf\keystore.jks”
```

CER

Mit dem Java **keytool.exe** können Sie die folgenden Schritte ausführen, um ein neues SSL-Zertifikat auf Ihrem BMC-Server zu installieren.

Führen Sie Befehle in der Eingabeaufforderung aus, die mit Administratorrechten geöffnet ist.

Schritt 1: Beenden Sie den BMC-Dienst.

Schritt 2: Erstellen Sie den neuen Schlüsselspeicher/das neue Schlüsselpaar.

keytool -keystore "path_to\keystore_name.jks" -genkeypair -keyalg RSA -keysize 2048 -validity #of days -dname "cn=domain name, ou=yourOrgUnit , o=yourOrgOrCompany, l=City/locality, st=State/Canton/Province/Land, c=Country_ISO3166-digraph" -alias "domain name"

DN	Information	Beschreibung	Beispiel
	Validity	Anzahl der Tage, wie lange der Keystore gültig ist.	365
CN	Common Name	Dies ist der vollständig qualifizierte Domänenname, den Sie sichern möchten	example.com
o	Organization Name	In der Regel der juristische Name eines Unternehmens oder einer Einrichtung und sollte alle Suffixe wie Ltd, Inc. oder Corp. enthalten.	Example Inc
OU	Organizational Unit	Interne Organisation Name der Abteilung/Abteilung	IT
l	Locality	Name des Ortes, der Stadt, des Dorfes, usw.	Helsinki
st	State	Provinz, Region, Landkreis oder Bundesland	North Karelia
c	Country	Der zweibuchstabige ISO-Code für das Land, in dem Ihre Organisation ansässig ist	FI

(Optional - wenn "**subject alternative name (SAN)**" verwendet werden soll):

keytool -keystore "path_to\keystore_name.jks" **-ext san=dns:Name1,dns:Name2** -genkeypair -keyalg RSA -keysize 2048 -validity #of days -dname "cn=domain name, ou=yourOrgUnit , o=yourOrgOrCompany, l=City/locality, st=State/Canton/Province/Land, c=Country_ISO3166-digraph" -alias "domain name"

Schritt 3: Erstellen Sie eine neue CSR (Certificate Signing Request) für Ihren neuen Keystore/Schlüsselpaar.

keytool -keystore "path_to\keystore_name.jks" -certreq -alias domain_name -file "path_to\filename.csr"

(Optional - wenn "**subject alternative name (SAN)**" verwendet werden soll):

keytool -keystore "path_to\keystore_name.jks" **-ext san=dns:Name1,dns:Name2** -certreq -alias domain_name -file "path_to\filename.csr"

Schritt 4: Importieren Sie das Root-CA-Zertifikat und dann das Zwischenzertifikat.

keytool -keystore "path_to\keystore_name.jks" -importcert -alias rootCA -file "path_to\root.cer"
keytool -keystore "path_to\keystore_name.jks" -importcert -alias intCA -file "path_to\int.cer"

Schritt 5: Importieren Sie das von einer Zertifizierungsstelle signierte Zertifikat und wenden Sie es auf das Schlüsselpaar an.

keytool -keystore path_to\keystore_name.jks -importcert -alias original_keypair_alias -file path_to\CAsigned.cer

Schritt 6: Aktualisieren Sie die Werte "keystoreFile" und "keystorePass" in der Datei "server.xml", die sich unter "C:\Programme\Blancco\Blancco Management Console\apache-tomcat\conf" befindet, um alle mit dem Schlüssel/Zertifikat verbundenen Änderungen zu berücksichtigen.

keystoreFile="path_to\keystore_name.jks" keystorePass="keystore password"

Schritt 7: Starten Sie den BMC-Dienst.

PFX

1. BMC-Dienst beenden
2. Kopieren Sie die Zertifikatsdatei im .pfx-Format in den Ordner "\Blancco Management Console\apache-tomcat\conf".
3. Öffnen Sie die Datei server.xml in einem Texteditor, der sich in der Blancco-Verwaltungskonsole\apache-tomcat\conf befindet, und bearbeiten Sie die folgenden Details.
    a. keystoreFile="Certificate_name.pfx"
    b. keystorePass="PFX_certificate_Password"
    c. Neuen Wert hinter KeystorePass keystoreType="PKCS12" hinzufügen.
4. Speichern Sie die Datei server.xml.
5. BMC-Dienst starten.

- Installing CA signed certificate to authenticate Management Console AD integration via LDAPS
- License Snapshot
- "Failed to load workflow" when editing or creating a new workflow
- How to export a summary report
- General instructions for installing a new SSL cert on BMC server