TDialog – Installation av Domibus för Säker digital kommunikation

Innehållsförteckning

1. Inledning

Denna guide beskriver installation av Domibus för användande tillsammans med TDialog.

Denna guide är mycket summarisk och håller inte samma kvalitet som övrig TDialog-dokumentation. Detta beror på att SDK och Domibus fortfarande är föränderlig materia och vi därför kan behöva ändra avgörande delar innan projektet går live från Ineras sida. Vidare krävs erfarenhet för att göra installationen på ett effektivt sätt, varför denna guide i nuläget mest är en checklista för de punkter som behöver utföras.

TDialog rekommenderar att en mindre kund (kommun) installerar Domibus och TDialog på samma server. Det blir då lätt att skydda Domibus-installationen, och man sparar en server jämfört med att använda olika. Då krävs dock att man använder en Apache för att dirigera trafiken till Domibus respektive TDialog, då denna trafik går på https (443) i båda fallen. Apache är en Open Source-programvara och installation beskrivs översiktligen i Apache-avsnittet nedan.

2. Vem använder denna guide?

Att installera Domibus är förhållandevis komplext, man bör ha tidigare erfarenhet av att installera Tomcat, Apache mm och framför allt erfarenhet av att arbeta med certifikat med verktyg som OpenSSL och keytool. TDialog rekommenderar att kunden låter sin installations- och uppgraderingspartner sköta installationen av Domibus.

3. Förberedelser

Installera OpenSSL

Om Windows: Installera OpenSSL, exempelvis från: https://slproweb.com/products/Win32OpenSSL.html. Om inte Windows finns troligen openssl redan installerat

Installera Java JDK 8 eller senare

Installera enligt standardinstruktioner.

4. Installation

Installera MySQL

Installera enligt standardinstruktioner. Om installation görs på samma server som TDialog, kan man använda samma MySQL-installation (men olika databaser).

Installera Tomcat

Allmänt

Installera Tomcat 8.5 i /sdk_ap/domibus-tomcat. Ange port 443 som http-port om du planerar att köra Domibus på egen server, annars 8443.

Installera JDBC driver

Ladda ner MySQL JDBC Connector 5.1, lägg jar-filen i lib-mappen i Tomcat.

Installera Domibus

Konfiguration

Hämta konfiguration från exempel.

Databas

Om Windows: Kör i CMD (inte powershell)

```
cd /sdk_ap/domibus-tomcat/sql-scripts
```

```
mysql -h localhost -u root --password=<mysqlrootpwd> -e "drop schema if
exists domibus_schema; create schema domibus_schema; alter database
domibus_schema charset=utf8 collate=utf8_bin; create user
edelivery@localhost identified by '<mysqledeliverypwd>';grant all on
domibus_schema.* to edelivery@localhost;"
```

```
mysql -h localhost -u root --password=<mysqlrootpwd> domibus_schema <
mysql5innoDb-4.1.2.ddl
```

```
mysql -h localhost -u root --password=<mysqlrootpwd> domibus_schema <
mysql5innoDb-4.1.2-data.ddl
```

Installera Domibus som service (Windows)

I kommandoprompten, gå till bin-mappen i Tomcat

(`cd \sdk_ap\domibus-tomcat\bin` eller motsvarande)

Kör: `service.bat install domibus-tomcat`

Nu finns en service installerad, men vi behöver även lägga till parametern domibus.config.location, eftersom setenv.bat inte körs när vi startar som en service.

Kör: `.\tomcat8w.exe //ES/domibus-tomcat`

Du bör nu se ett litet gränssnitt där du kan sätta properties för tjänsten. Gå fliken Java och lägg till följande nederst i rutan ”Java options”:

```
-Ddomibus.config.location=C:\sdk_ap\domibus-tomcat\conf/domibus
```

Dessutom, ange följande minnesinställningar längst ner i rutan (värdena är minimivärden):

Initial memory pool: 128

Maximum memory pool: 1024

Stäng och starta upp. Nu bör Tomcat starta som en service på ett korrekt sätt.

Installera Domibus som service (Linux, systemd)

Skapa systemd-fil.

Lägg till följande inställning:

```
-Ddomibus.config.location=/opt/sdk_ap/domibus-tomcat/apache-tomcat-8.5.50/conf/domibus
```

Miljövariabler

Lägg till java\bin i PATH

Lägg till openssl\bin i PATH

Lägg till mysql\bin i PATH

Sätt JAVA_HOME till din Java-katalog

Certifikat

Keystore

Angående certifikat och konfiguration: En viktig parameter här är domänen. Den ska användas i konfigurationen av endpointen, men även som alias på certifikatet (det är så man ser vilket certifikat som ska användas). I instruktionen nedan och i konfigurationsfilerna används <! cert alias > för detta, och det måste alltså vara identiskt på samtliga ställen.

Dessutom måste nyckeln vara krypterad med samma lösenord som jks:en, anges med <! key password > nedan

Börja med crt and key

Om du börjar med en p12, gör nedan, och ändra orig_p12.p12 till ditt filnamn:

```
openssl pkcs12 -in orig_p12.p12 -nocerts -out sdk.key
```

```
openssl pkcs12 -in orig_p12.p12 -clcerts -nokeys -out sdk.crt
```

Se till att key har ett lösenord

```
openssl rsa -aes256 -in sdk_orig.key -out sdk.key

<! key password >

Skapa p12 med crt och key

openssl pkcs12 -export -in sdk.crt -inkey sdk.key -out sdk.p12 -
name <! cert alias >

<! key password >
```

Skapa jks från p12

```
keytool -importkeystore -srckeystore sdk.p12 -srcstoretype pkcs12
-srcalias <! cert alias > -destkeystore sdk_keystore.jks -
deststoretype jks -deststorepass <! key password > -destalias <!
cert alias >
```

Döp om filen till gateway_keystore.jks och lägg i: domibus\conf\domibus\keystores

HTTPS-certifikat

Utgå från sdk.key och sdk.crt, men vi måste dessutom lägga till utfärdar-CA.

Hitta ditt utfärdar-CA, spara som ca.crt

```
# Gör till pkcs12

openssl pkcs12 -export -in sdk.crt -inkey sdk.key -out https.p12 -
name tomcat -CAfile ca.crt -caname root -chain
```

OBS: Om felmeddelande, lägg manuellt till rotcertet till ca.crt.

```
keytool -importkeystore -srckeystore https.p12 -srcstoretype
pkcs12 -srcalias tomcat -destkeystore https.jks -deststoretype jks
-deststorepass <! key password > -destalias tomcat
```

Apache, gör en key utan lösen

```
openssl rsa -in sdk.key -out sdk_nopass.key
```

Flytta https.p12 till conf/domibus/keystores

Truststore

Ladda ner SKL:s truststore från:

https://inera.atlassian.net/wiki/spaces/OISDK/pages/4032583/Anslutningsinformation+teknik (filen qa_truststore.jks)

Lösenordet för truststoret är 'password'. Notera att det inte innehåller något hemligt - bara vilka publika certifikat vi ska lita på.

https-cert för TDialog

```
openssl pkcs12 -in td-test.p12 -nocerts -out td-test.key
```

```
openssl pkcs12 -in td-test.p12 -clcerts -nokeys -out td-test.crt
```

5. TDialog och Domibus på samma server

Följande aktiviteter behöver göras om TDialog och Domibus är på samma server.

Domibus-konfiguration

Verifiera att Tomcat i server.xml är inställd på att lyssna på port 8443.

Installera Apache

Installera Apache enligt standardinstruktion.

Lägg till följande konfiguration i httpd.conf. Ändra ”kund” till eget namn, och såklart korrekta pathar.

OBS: Nedan exempel innehåller även skydd av Domibus (Location-taggarna för backend och login). Det är en bra idé att börja med att installera dem bortkommenterat för att verifiera att allt fungerar och sedan lägga på dem. Vad gäller login behöver man bestämma sig för varifrån login-sidan ska vara tillgänglig.

```
<VirtualHost *:443>
 ServerName sdk-test.kund.se
```

```
 SSLCertificateFile /sdk_ap/httpd-2.4.41-o111c-x86-vc15-
r2/Apache24/credentials/sdk.crt
 SSLCertificateKeyFile /sdk_ap/httpd-2.4.41-o111c-x86-vc15-
r2/Apache24/credentials/sdk_nopass.key
 SSLProxyCheckPeerExpire on
 SSLProxyEngine on
 SSLProxyVerify none
 SSLProxyCheckPeerCN off
 SSLProxyCheckPeerName off
# Protect backend WS endpoint
<Location /domibus/services/backend>
  order deny,allow
  deny from all
  allow from 127.0.0.1 ::1
  allow from <server IP>
  ProxyPreserveHost On
  ProxyPass https://localhost:8443/domibus/services/backend
  ProxyPassReverse https://localhost:8443/domibus/services/backend
 </Location>
 # Protect Dombius login
 <Location /domibus/login>
  order deny,allow
  deny from all
  allow from 127.0.0.1 ::1
  allow from <allowed IP:s>
  ProxyPreserveHost On
  ProxyPass https://localhost:8443/domibus/login
  ProxyPassReverse https://localhost:8443/domibus/login
 </Location>
<Location />
  ProxyPreserveHost On
  ProxyPass https://localhost:8443/
  ProxyPassReverse https://localhost:8443/
 </Location>
</VirtualHost>
<VirtualHost *:443>
 ServerName sakrameddelanden.kund.se
 SSLCertificateFile /sdk_ap/httpd-2.4.41-o111c-x86-vc15-
r2/Apache24/credentials/td-test.crt
 SSLCertificateKeyFile /sdk_ap/httpd-2.4.41-o111c-x86-vc15-
r2/Apache24/credentials/td-test_nopass.key
 SSLProxyCheckPeerExpire on
 SSLProxyEngine on
 SSLProxyVerify none
 SSLProxyCheckPeerCN off
 SSLProxyCheckPeerName off
 <Location />
  ProxyPreserveHost On
  ProxyPass https://localhost:9443/
  ProxyPassReverse https://localhost:9443/
```

```
 </Location>
</VirtualHost>
```

TDialog-konfiguration

För TDialog behöver följande ändras för att köra på samma server som Domibus, enligt ovan.

server.port=9443

server.use-forward-headers=true

6. Säkra installationen

Portsäkerhet

Verifiera att port 9443 och 8443 endast är åtkomliga lokalt

Tomcat-säkerhet

Genomför punkterna i:

https://www.upguard.com/articles/15-ways-to-secure-apache-tomcat-8

Apache-säkerhet

Ange följande i Apache-konfigurationen, både för TDialog och Domibus:

```
# Restrict cipher suites, implement forward secrecy and allow only
protcols without known vulnerabilities

SSLCipherSuite EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:ECDHE-RSA-AES128-
SHA:DHE-RSA-AES128-GCM-SHA256:AES256+EDH:ECDHE-RSA-AES256-GCM-
SHA384:ECDHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-
AES256-SHA384:ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES256-SHA:DHE-RSA-
AES256-SHA256:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA:DHE-RSA-AES128-
SHA:ECDHE-RSA-DES-CBC3-SHA:EDH-RSA-DES-CBC3-SHA:AES256-GCM-
SHA384:AES128-GCM-SHA256:AES256-SHA256:AES128-SHA256:AES256-SHA:AES128-
SHA:DES-CBC3-SHA:HIGH:!aNULL:!eNULL:!EXPORT:!DES:!MD5:!PSK:!RC4

SSLProtocol TLSv1.2

SSLHonorCipherOrder on
```

7. Installationsverifiering

Säkerhet Apache

Verifiera att 9443 och 8443 på servern ej är åtkomliga utifrån.

Gå till www.ssllabs.com och ange Domibus-hosten och TDialog-hosten för att verifiera att certifikat och TLS är uppsatta på ett korrekt och säkert sätt. Organisationen kan själv bestämma vilken rating som ska krävas, men med konfigurationen ovan kan en rating på A+ uppnås.

8. Annan information

E-delivery, dvs den standard som Domibus följer och som Inera profilerat med SDK.

https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery

Domibus administrator guide:

https://ec.europa.eu/cefdigital/wiki/download/attachments/110494698/%28eDelivery%29%28AP%29%28AG%29%284.1%29%284.0%29.pdf?version=1&modificationDate=1564575688989&api=v2

Inera projektinformation SDK:

https://inera.atlassian.net/wiki/spaces/OISDK/overview

Under ”teknisk dokumentation och specifikationer finns SDK-projektets profilering av eDelivery-standarden för Säker digital kommunikation