TDialog– installation

Inledning

Dokumentet beskriver installationen av TDialog. Installationen och beroendena gör att beskrivningen med nödvändighet blir på en ganska övergripande nivå. Det innebär att en installatör behöver ha tidigare erfarenhet av serverhantering och installation och konfiguration av programvaror som inte bara är Next-next-finish.

Allmänt

TDialog är en Javamiljö, med en MySQL-databas i botten. Den kopplas till en SAML-IDP, och interagerar med en e-postgateway för att skicka notifieringar. Följaktligen behöver vi installera Java och MySQL, och vi kommer behöva koppla oss mot en SAML-IDP och mot en e-postgateway.

Förutsättningar

Följande behöver finnas på plats innan vi kan påbörja den egentliga installationen.

E-postgateway

För att meddelandenotifieringar ska gå iväg så krävs att TDialog är kopplad mot en e-postgateway.

IDP

TDialog behöver koppling till en SAML-IDP för att användare ska kunna logga in.

Brandväggsöppningar

- Port 443 för inkommande trafik
- Port 25 mot e-postgateway

.NET framework 4.5.2

MySQL kräver denna .NET-version från Microsoft. Finns på:
https://www.microsoft.com/sv-se/download/details.aspx?id=42642

MySQL server 5.7

https://dev.mysql.com/downloads/installer/

Välj version 5.7

- Installera enligt standardinställningarna, men mest passande alternativ är ”Server only” och sedan ”Server machine” som config type.
- Skapa en rotanvändare, sätt ett komplext slumpmässigt lösenord (med hjälp av rand-funktionen i OpenSSL, lösenordshanterare eller något annat) och spara på ett säkert ställe.
- MySQL kommer vid behov att installera Microsoft C++ Redistributable pack 2013.

Java

http://www.oracle.com/technetwork/java/javase/downloads/jre8-downloads-2133155.html

Ladda ner och installera en Java 8 JRE.

JCE

TDialog använder Javas avancerade kryptofunktioner, vilket kräver en särskild installation. Ladda ner filerna på:

http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html

Packa upp dem, ta de två jar-filerna och lägg i /lib/security på javainstallationen.

DNS-namn

I beskrivningen förutsätts att det finns ett DNS-namn för TDialog-servern.

Certifikat

I beskrivningen förutsätts att det finns ett certifikat för DNS-namnet ovan.

Installationen

Packa upp installationen

Lägg hela installationens innehåll i `c:\td-install` på servern. Observera att den faktiska installationen kommer att ligga i `c:\trusteddialog` (per default).

Konfigurera och kör installationshjälpmedel

Allmänt

`install.properties` (i installationens rot) är där grundinstallationen konfigureras. install.properties används bara vid installationen och effekten är att installationskonfiguration skjuts ut till databasen och till ett flertal properties-filer.

Endast Windows

Observera att installationsscriptet endast har stöd för Windowsinstallationer, så med Linux så måste förändringarna göras manuellt.

Konfigurationsparametrar

Nedan beskrivs de konfigurationsparametrar som anges i `install.properties`.

- `installationpath`. Dit konfigurationen ska kopieras. `C:/trusteddialog/config` är rekommenderat
- `mysqlbinfilepath`. Path till MySQL bin-folder
- `mysqlrootpwd`. Rotlösenordet du angav vid installation av mysql
- `hostname`. DNS-namnet på installationen
- `entityidfull`. Entity ID på TDialogs Service Provider för interna användare.

- `entityidguest`. Entity ID på TDialogs Service Provider för externa användare.
- `customername`. Namnet på kunden. Används i texter.
- `idpname`. Om syftet är att konfigurera endast en IDP så kan den anges här för automatkonfiguration.

Kör installationsscriptet

Kör installationsscriptet från commandoprompt, så att eventuella felmeddelanden syns innan fönstret stängs.

```
C:\td-install> java –jar serverinstaller.jar
```

application-prod.properties

Server-host och port

Per default svarar TDialog på port 443 på samtliga hostnamn. Det är oftast en bra inställning, med tanke på NAT-konfigurationer, proxies och liknande. Men, med `server.address` respektive `server.port` kan dessa ändras.

Certifikat

- `server.ssl.key-store`. Filsökväg till certifikat. Måste vara i PS12-format, innehållande certifikat, privat nyckel och eventuella överliggande certifikat.
- `server.ssl.key-store-password`. Lösenord på certifikatsfilen.

MySQL-koppling

- `spring.datasource.url`. JDBC-URL till MySQL. Default bör fungera i de flesta vanliga scenarion.
- `spring.datasource.username`. Installationsprogrammet har automatiskt skapat en databasanvändare för TDialog, så denna behöver inte ändras.
- `spring.datasource.password`. Installationsprogrammet har automatiskt genererat ett lösenord för TDialog-användaren, så denna behöver inte ändras.

E-postgateway

`server.mail.host`. Hostnamn till den SMTP-server som hanterar notifieringsmeddelande. Om servern kräver autentisering så anges den i angränsande properties, annars lämnas dessa tomma.

Hantering av externa och interna användare

Interna användardomäner. `server.auth.internalEmailDomains`. När TDialog ska skicka ett meddelande så behöver den veta om mottagaren är en intern eller extern användare. Det bestämmer den genom att titta på e-postadressen, och om slutet på e-postadressen är enligt det som anges i `internalEmailDomains` så betraktas det som en intern adress.

Attribut

Per default förväntar sig TDialog följande attribut av IDP:n. Om det är andra attributnamn så behöver attributkonfigurationen ändras.

- Användaridentifierare. Per default detta attribut flera värden, nämligen `urn:oid:0.9.2342.19200300.100.1.1;Subject_SerialNumber`, vilket dels är EPPN enligt federationsstandard och dels CGI:s sätt att lägga in personnummer efter inloggning med e-legitimation. Andra IDP:er rekommenderas alltså använda `urn:oid:0.9.2342.19200300.100.1.1` som attributnamn.
- E-postadress. `urn:oid:0.9.2342.19200300.100.1.3`
- Namn. Detta attribut har ingen teknisk betydelse, men det är obligatoriskt och det används för att skriva ut användarens namn. `urn:oid:2.16.840.1.113730.3.1.241`
- Adminstratör. Om detta attribut är satt till ett visst värde så betyder det att användaren är administratör. `urn:oid:1.3.6.1.4.1.5923.1.8`

Övrig konfiguration

Tmp-mapp i Linux

Tomcat behöver en mapp för att spara sina temporärfiler. I en Linux-server är detta per default i /tmp, vilket leder till problem eftersom denna mapp rensas av operativsystemet medan Tomcat körs. En bättre lösning är att sätta tmp-mappen till en sökväg i TDialog, detta genom att ange följande i application.properties.

spring.http.multipart.location=<path där man vill att dessa filer ska läggas>

Kryptering?

Ska installationen kryptera filer och texter i applikationen? Om ja, ange server.encryption.enabled=true. Krypteringsnycklar sätts av en administratör inuti applikationen.

Gästanvändares behörigheter

Det finns tre nivåer av behörigheter för gästanvändare

- 10. Gästanvändare kan inte självregistrera, och kan inte kommunicera med någon som inte initierat kommunikation med dem.
- 50. Gästanvändare kan inte självregistrera, men när de väl bjudits in kan de kommunicera med vem de vill.
- 70 Gästanvändare kan självregistrera, och efter självregistrering så kan de kommunicera med vem de vill.

Propertyn heter server.guestUser.permission, default är 70.

Ska filvyn finnas?

Förutom att skicka meddelanden så har TDialog även stöd för en filarea per användare. Per default är filarean aktiverad, men ange server.gui.showFilesView=false för att deaktivera.

Lägg till externt metadata

Fil: config/securityContext.xml

Sök på fileSystemMetadataProvider i securityContext.xml. XML:en som börjar med <bean> och slutar med </bean> är för att koppla till en IDP. Normalt bör det bara handla om att kopiera XML-fragmentet och byta filnamn. Självklart behöver filen också läggas till för att det ska fungera.

Konfigurera inloggningssidan

Inloggningssidan kan konfigureras hur som helst, men det finns några grundscenarion som man kan välja på.

Default

Visar en inloggningssida där man själv kan ange länkar till inloggningar.

En IDP

Går omedelbart till denna IDP när användare försöker ansluta till TDialog. Det är det vanligaste scenariot, exempelvis med alla kunder som vill koppla till HAG.

För att åstadkomma detta, kopiera html/ds-index.html.singleidp till html/ds-index.html

Installera TDialog som en service

Gå till installationsmappen och skriv:

trusteddialog.exe install

Nu installeras TDialog som en service.

Att felsöka installationen

EventViewer och trusteddialog\logs är dina vänner.