Installeer en Configureer de chassisprovider (IDP) voor Cisco Identity Services (IDs) zodat deze de SBBO kan inschakelen

Inhoud

Inleiding

In dit document wordt de configuratie op de IDP (OpenAM Identity Provider) beschreven om Single Sign On (SSO) in te schakelen.

Cisco IDs-implementatiemodule

Product	Plaatsing
UCCX	Medeingezetene
PCCE	Gelijktijdige inwoner met CUIC (Cisco Unified Intelligence Center) en LD (Live Data)
UCCES	Gelijktijdige inwoner met CUIC en LD voor 2k implementaties. Standalone voor 4k- en 12k-implementaties.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Unified Contact Center Express (UCCX) release 11.6 of Cisco Unified Contact Center Enterprise release 11.6 of Packaged Contact Center Enterprise (PCCE) release 11.6 indien

van toepassing.

> Opmerking: Dit document verwijst naar de configuratie met betrekking tot de Cisco Identifier Service (IDS) en de Identity Provider (IDP). Het document verwijst naar UCCX in de screenshots en voorbeelden, maar de configuratie is vergelijkbaar met betrekking tot Cisco Identifier Service (UCCX/UCCE/PCCE) en de IDP.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Installeren

Shibboleth is een opensource-project dat Single Sign On-capaciteiten biedt en sites in staat stelt om gefundeerde vergunningsbeslissingen te nemen voor individuele toegang van beschermde online bronnen op een manier die de privacy beschermt. Het ondersteunt Security Assertion Markup Language (SAML2). IDS is een SAML2-client en wordt geacht Shibboleth te ondersteunen met minimale of geen wijzigingen in IDs. In 11.6 kan IDs met Shibboleth IDP werken.

> Opmerking: In dit document wordt verwezen naar "Shibboleth release 3.3.0" als onderdeel van de kwalificatie als SSO

Systeemvereisten

Samengesteld	Details
Sjiitische versie	v3.3.0
Downloadlocatie	http://shibboleth.net/downloads/identity-provider/
Installatieplatform	Ubuntu 14.0.4 java versie "1.8.0_121"
LDAP-versie (Lichtgewicht Directory Access Protocol)	Active Directory 2.0
Sjiitische webserver	Apache Tomcat/8.5.12

Raadpleeg de wiki voor installatie van de sjiieten

https://wiki.shibboleth.net/confluence/display/IDP30/Installation

Configureren

Integreren met een LDAP server

Om een LDAP server te integreren met shibboleth moeten de velden geüpdatet worden in **$shibboleth_home/conf/ldap.properties** waar**$shibboleth_home** (standaard is /opt/shibboleth-idp) verwijst naar de installatiedirectory van de shibboleth.

Veld	Verwachte waarde	Beschrijving
idp.autorn.LDAP.trustCertificaten	Een middel om vertrouwensankers van, gewoonlijk een lokaal dossier in $ {idp.home}/geloofsbrieven te laden waar idp.home een 'environment' variabele is die wordt geëxporteerd als JAVA_OPTS in setenv.sh	% {idp.home} /credentials/ldap-server.crt
idp.autorn.LDAP.trustStore	Een middel om een toetsenbord van Java te laden dat vertrouwensankers bevat, gewoonlijk een lokaal bestand in % {idp.home}/geloofsbrieven	% {idp.home} /credentials/ldap-server.truststore
idp.autorn.LDAP.returnAttributes	De komma gescheiden lijst van LDAPAversies die terug moeten worden gegeven. Als u alle eigenschappen wilt teruggeven, voeg "*" toe.	*
idp.autorn.LDAP.baseDN	De basisDN waarop de LDAP-zoekfunctie moet worden uitgevoerd	CN=gebruikers, DC=cisco,DC=com
idp.autorn.LDAP.subtreeSearch	Of u nu recursief zoekt	reëel
idp.autorn.LDAP.userFilter	LDAP-zoekfilter	(sAMAaccountName= {gebruiker}*)
idp.autorn.LDAP.bindDN	DNA binden met wanneer zoekopdracht wordt uitgevoerd	administrator@cisco.com
idp.autorn.LDAP.bindDNCredential	Wachtwoord om mee te verbinden wanneer zoekactie wordt uitgevoerd	
idp.autorn.LDAP.dnFormat	Een opmaakstring die de gebruiker DNA's moet genereren om te authenticeren	%s@adfsserver.cisco.com (%s@domainname)
IDP.autorn.LDAP.authenticator	Bestuurt de werkschema's voor de wijze waarop authenticatie plaatsvindt tegen de LDAP	bindSearchAuthenticator
idp.autorn.LDAP.ldapURL	Connection URI voor LDAP-directory	

Raadpleeg voor meer informatie:

https://wiki.shibboleth.net/confluence/display/IDP30/LDAPAuthnConfiguration

Configuratiebestand

```
# Tijd in milliseconden om te
wachten voorreacties
#idp.autorn.LDAP.responseTime-out = PT3S
# SSL-configuratie, of jvmTrust,
certificaatTrust, of keyStoreTrust
#idp.autorn.LDAP.sslConfig = certificaatTrust
## Als u certificaatTrust hierboven gebruikt,
stelt u het pad van het vertrouwde certificaat
in
idp.autorn.LDAP.trustCertificates = % {idp.home}
/credentials/ldap-server.crt
## Als u keyStoreTrust hierboven gebruikt,
selecteert u het trustopslagpad
idp.autorn.LDAP.trustStore = % {idp.home}
```

```
/credentials/ldap-server.truststore
## Return-eigenschappen tijdens verificatie
#idp.autorn.LDAP.returnAttributes =
userPrincipalName, sAMAcountName
idp.autorn.LDAP.returnAttributen = *
## DN-afwikkelingseigenschappen ##
# Zoeken van DNA-resolutie, gebruikt door
anonSearchAuthenticator, bindSearchAuthenticator
# voorAD: CN=Gebruikers, DC=voorbeeld, DC=org
idp.autorn.LDAP.baseDN = CN=gebruikers,
DC=cisco,DC=com
idp.autorn.LDAP.subtreeSearch = reëel
*idp.autorn.LDAP.userFilter = (sAMAcountName=
{gebruiker}*)
#-zoekconfiguratie
# voorAD:
idp.autorn.LDAP.bindDN=adminuser@domain.com
idp.autorn.LDAP.bindDN = beheerder@cisco.com
idp.autorn.LDAP.bindDNCredential = Cisco@123
#Format DN-resolutie, gebruikt door
directAuthenticator, en verificator
# voorAD gebruik
idp.autorn.LDAP.dnFormat=%s@domain.com
#idp.autorn.LDAP.dnFormat =
%s@adfsserver.cisco.com
# LDAP attribuutconfiguratie, zie attribuut-
resolver.xml
# Opmerking ditwaarschijnlijk niet van
toepassing op het gebruik van oudere V2 resoluut
configuraties
idp.attribuut.resolver.LDAP.ldapURL = %
{idp.autorn.LDAP.ldapURL}
idp.attribuut.resolver.LDAP.connectTime out = %
{idp.autorn.LDAP.connectTime-out:PT3S}
idp.attribuut.resolver.LDAP.responseTime out = %
{idp.autorn.LDAP.responseTime-out:PT3S}
idp.attribuut.resolver.LDAP.baseDN = %
{idp.autorn.LDAP.baseDN:niet gedefinieerd}
idp.attribuut.resolver.LDAP.bindDN = %
{idp.autorn.LDAP.bindDN:niet gedefinieerd}
idp.attribuut.resolver.LDAP.bindDNCredential = %
{idp.autorn.LDAP.bindDNCredential:undefined}
idp.attribuver.LDAP.useStartTLS = %
{idp.autorn.LDAP.useStartTLS:reëel>
idp.attribuut.resolver.LDAP.trustCertificates =
% {idp.autorn.LDAP.trustCertificates:niet
gedefinieerd}
idp.attribuut.resolver.LDAP.searchFilter =
(sAMAcountName=$afwikkelingscontextContext.main)
```

Aanvragen van alle klanten toestaan

Om ervoor te zorgen dat verzoeken van alle klanten bereiken, worden veranderingen vereist in **"$shibboleth_home/conf/access-control.xml"**

<entry key="AccessByIPAdjurk">
<boon id="AccessByIPAdjurk" ouder="shibboleth.IPRangeAccessControl"
p:allowRanges="# {'127.0.0.1/32',**'0.0.0.0/0'**, '::1/128', '10.78.93.103/32'} " />
</entry>

Voeg **'0.0.0.0/0'** toe aan de toegestane bereik. Dit staat verzoeken van om het even welk ip bereik toe.

Shibboleth configureren om te integreren met IDs

Secure Hash Algorithm (SHA1) en encryptie-configuratie in IDS

Om IDS te configureren naar default SHA1 opent u **"$shibboleth_home/conf/idp.properties"** en stelt u in:

idp.sign.fig = shibboleth.SigningConfiguration.SHA1

Deze configuratie kan ook worden gewijzigd:

idp.encryptie.optioneel = echt

Als u deze instelt op waar, zal het niet vinden van een encryptiesleutel om te gebruiken, wanneer ingeschakeld, niet resulteren in het mislukken van het verzoek. Deze hHelp mee om encryptie "opportunistisch" te doen, d.w.z. om encryptie zoveel mogelijk te versleutelen (een compatibele sleutel is in de metadata van de peer gevonden om mee te versleutelen) maar om anders encryptie te overslaan.

Uid en user_main instellen op de SAML Respons

The AttributionDefinition wordt in **"$shibboleth_home/conf/attribute-resolver.xml" toegevoegd** om sAMAAccountName en userPrincipalName in kaart te brengen in de to uid en user_main in de SAML respons.

Voeg bovendien de ldap-instellingen toe met de tag <DataConnector>.

> **Opmerking**: ReturnAttributes moeten worden gespecificeerd met waarde "**sAMAAccountName userPrincipalName**".

> **Opmerking**: LDAPProperty is verplicht als er een integratie is met een Active Directory (AD).

De veranderingen in **"$shibboleth_home/conf/attribute-filter.xml" opnemen**

Wijzig de **"$shibboleth_home/conf/saml-nameid.xml"** om het volgende te doen

IDp-metadata

IDP-metadata is beschikbaar in de map "**$shibboleth_home/metadata**". Het bestand idp-

metadata.xml kan aan IDS worden geüpload via de API voor programmeerprogramma's (Application Programming Interface)

PUT https://<id-shost>:<idsport>/ids/v1/configuratie/metadata

waarbij de distributie geen aanpasbare entiteit is en de waarde **"8553" is**

> **Waarschuwing**: De Scheepsmetagegevens **kunnen** twee gebarentakens, het algemeen ondertekeningscertificaat en het backchannel bevatten. Navigeer naar het bestand **idp-backchannel.crt** in **"$shibboleth_home/Credentials"** om het backchannel certificaat te identificeren**.** Als het back-kanaal certificaat beschikbaar is in de metadata, moet u het back-kanaal certificaat verwijderen van de metadata xml alvorens te uploaden naar IDS. Dit komt doordat de bibliotheek fedlet 12.0 die IDS gebruikt slechts één certificaat in de metagegevens ondersteunt. Als er meer dan één ondertekeningscertificaat beschikbaar is, gebruikt Fedlet het eerste beschikbare certificaat.

metagegevensleveranciers configureren

We moeten de metagegevensleveranciers configureren met de vermelding in **$shibboleth_home/metadata-providers.xml.**

```
<MetadataProvider id="smart-86"  xsi:type="FilesystemMetadataProvider"
metadataFile="/opt/shibboleth-idp/SP/sp.xml"/>
```

waarin **de** eigenschap "id" **een** unieke naam kan zijn.

Deze ingang geeft aan dat een metagegevensaanbieder bij de gegeven id is geregistreerd en de metagegevens beschikbaar zijn in het gespecificeerde bestand /opt/shibboleth-idp/SP/sp.xml.

De metagegevens van serviceproviders (SP) van IDS moeten worden gekopieerd naar de metagegevens die in de ingang zijn gespecificeerd.

> **Opmerking**: SP-metagegevens van IDS kunnen via **GET https://<idshost>:<idsport>/ids/v1/fig/spmetadata**, waar **sport** geen configureerbare entiteit is en de waarde "853" is.

Aanvullende configuratie voor SSO

In dit document wordt de configuratie vanuit het IDP-aspect beschreven zodat de BF kan integreren met de Cisco Identity Services. Raadpleeg de afzonderlijke productconfiguratiehandleidingen voor meer informatie:

- UCCX
- UCCES
- PCCE