Installation und Konfiguration des Shibboleth Identity Provider (IdP) für Cisco Identity Service (IDs) zur Aktivierung der SSO

Inhalt

Einführung

Dieses Dokument beschreibt die Konfiguration des OpenAM Identity Providers (IDP) zur Aktivierung der Single Sign On (SSO).

Cisco IDS-Bereitstellungsmodelle

Produkt	Bereitstellung
UCCX	Co-Resident
PCCE	Co-Resident mit CUIC (Cisco Unified Intelligence Center) und LD (Live-Daten)
UCCE	Resident gemeinsam mit CUIC und LD für 2.000 Bereitstellungen. Standalone für 4.000- und 12.000-Bereitstellungen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco Unified Contact Center Express (UCCX) Version 11.6 oder Cisco Unified Contact Center Enterprise Release 11.6 oder Packaged Contact Center Enterprise (PCCE) Release

11.6.

Hinweis: Dieses Dokument bezieht sich auf die Konfiguration des Cisco Identify Service (IDs) und des Identitätsanbieters (IdP). Das Dokument verweist in den Screenshots und Beispielen auf UCCX, die Konfiguration ähnelt jedoch dem Cisco Identitify Service (UCCX/UCCE/PCCE) und der IdP.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Installieren

Shibboleth ist ein Open-Source-Projekt, das Single Sign-On-Funktionen bietet und es Websites ermöglicht, fundierte Autorisierungsentscheidungen für den individuellen Zugriff auf geschützte Online-Ressourcen unter Wahrung der Privatsphäre zu treffen. Sie unterstützt Security Assertion Markup Language (SAML2). IdS ist ein SAML2-Client und soll Shibboleth mit minimalen oder gar keinen Änderungen an IDs unterstützen. In 11.6 ist IdS für die Arbeit mit Shibboleth IdP qualifiziert.

Hinweis: Dieses Dokument bezieht sich auf Shibboleth Release 3.3.0 als Teil der Qualifizierung mit SSO

Systemanforderungen

Komponente	Details
Shibboleth-Version	Version 3.3.0
Download-Speicherort	http://shibboleth.net/downloads/identity-provider/
Installationsplattform	Ubuntu 14.0.4 Java-Version "1.8.0_121"
LDAP-Version (Lightweight Directory Access Protocol)	Active Directory 2.0
Shibboleth-Webserver	Apache Tomcat/8.5.12

Im Wiki finden Sie Informationen zur Installation von Shibboleth.

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

Konfigurieren

Integration mit einem LDAP-Server

Um einen LDAP-Server mit Shibboleth zu integrieren, müssen die Felder in **$shibboleth_home /conf/ldap.properties** aktualisiert werden, wo**$shibboleth_home** (Standardwert: /opt/shibboleth-idp)

auf das Installationsverzeichnis verweist, das bei der Installation von Shibboleth verwendet wird.

Feld	Erwarteter Wert	Beschreibung
idp.authn.LDAP.trustCertificates	Eine Ressource zum Laden von vertrauenswürdigen Ankern aus einer lokalen Datei in ${idp.home}/Anmeldeinformationen. wobei idp.home eine Umgebungsvariable ist, die in setenv.sh als JAVA_OPTS exportiert wird.	%{idp.home}/credentials/ldap-ser
idp.authn.LDAP.trustStore	Eine Ressource zum Laden eines Java-Keystres mit Vertrauenshinweisen, in der Regel eine lokale Datei in %{idp.home}/Anmeldeinformationen.	%{idp.home}/credentials/ldap-ser
idp.authn.LDAP.returnAttributes	Die kommagetrennte Liste von LDAPAttributen, die zurückgegeben werden müssen. Wenn Sie alle Attribute zurückgeben möchten, fügen Sie "*" hinzu.	*
idp.authn.LDAP.baseDN	Der baseDN, bei dem die LDAP-Suche ausgeführt werden muss	CN=Benutzer, DC=cisco,DC=cor
idp.authn.LDAP.subtreeSuche	Gibt an, ob eine rekursive Suche durchgeführt werden soll.	wahr
idp.authn.LDAP.userFilter	LDAP-Suchfilter	(sAMAccountName={user})*
idp.authn.LDAP.bindDN	DN für die Anbindung bei der Suche	administrator@cisco.com
idp.authn.LDAP.bindDNCredential	Passwort, mit dem bei der Suche verknüpft werden soll	
idp.authn.LDAP.dnFormat	Eine Formatierungszeichenfolge zum Generieren der Benutzer-DNs zum Authentifizieren	%s@adfsserver.cisco.com (%s@domainname)
idp.authn.LDAP.authentifier	Steuert den Workflow für die Art der Authentifizierung mit LDAP	bindSearchAuthenticator
idp.authn.LDAP.ldapURL	Verbindungs-URI für LDAP-Verzeichnis	

Weitere Informationen finden Sie unter:

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

Beispielkonfigurationsdatei

```
# Wartezeit in Millisekunden fürAntworten
#idp.authn.LDAP.responseTimeout = PT3S
## SSL-Konfiguration, entweder jvmTrust,
certificateTrust oder keyStoreTrust
#idp.authn.LDAP.sslConfig = certificateTrust
## Wenn certificateTrust oben verwendet wird,
legen Sie den Pfad des vertrauenswürdigen
Zertifikats fest
idp.authn.LDAP.trustCertificates =
%{idp.home}/credentials/ldap-server.crt
## Wenn keyStoreTrust oben verwendet wird,
legen Sie den Pfad für den Truststore fest
idp.authn.LDAP.trustStore =
%{idp.home}/credentials/ldap-server.truststore
## Rückgabeattribute für Authentifizierung
#idp.authn.LDAP.returnAttributes =
```

```
userPrincipalName, sAMAccountName
idp.authn.LDAP.returnAttributes = *
## DN-Auflösungseigenschaften ##
# DN-Auflösung durchsuchen, verwendet von
anonSearchAuthenticator,
bindSearchAuthenticator
# fürAD: CN=Benutzer,DC=Beispiel,DC=org
idp.authn.LDAP.baseDN =
CN=Users,DC=cisco,DC=com
idp.authn.LDAP.subtreeSearch = < wahr
*idp.authn.LDAP.userFilter =
(sAMAccountName={user})*
# Konfiguration der binden-Suche
# fürAD:
idp.authn.LDAP.bindDN=adminuser@domäne.com
idp.authn.LDAP.bindDN =
administrator@cisco.com
idp.authn.LDAP.bindDNCredential = Cisco@123
# Format-DN-Auflösung, verwendet von
directAuthenticator, adAuthenticator
# fürAD verwenden
idp.authn.LDAP.dnFormat=%s@domäne.com
#idp.authn.LDAP.dnFormat =
%s@adfsserver.cisco.com
# LDAP-Attributkonfiguration, siehe attribute
resolver.xml
# Hinweis, diesewird wahrscheinlich nicht auf
die Verwendung von älteren V2-Resolver-
Konfigurationen angewendet
idp.attribute.resolver.LDAP.ldapURL =
%{idp.authn.LDAP.ldapURL}
idp.attribute.resolver.LDAP.connectTimeout =
%{idp.authn.LDAP.connectTimeout:PT3S}
idp.attribute.resolver.LDAP.responseTimeout =
%{idp.authn.LDAP.responseTimeout:PT3S}
idp.attribute.resolver.LDAP.baseDN =
%{idp.authn.LDAP.baseDN:undefined}
idp.attribute.resolver.LDAP.bindDN =
%{idp.authn.LDAP.bindDN:undefined}
idp.attribute.resolver.LDAP.bindDNCredential =
%{idp.authn.LDAP.bindDNCredential:undefined}
idp.attribute.resolver.LDAP.useStartTLS =
%{idp.authn.LDAP.useStartTLS:wahr}
idp.attribute.resolver.LDAP.trustCertificates
=
%{idp.authn.LDAP.trustCertificates:undefined}
idp.attribute.resolver.LDAP.searchFilter =
(sAMAccountName=$resolutionContext.Principal)
```

Anfragen aller Clients zulassen

Um sicherzustellen, dass Anfragen aller Kunden eingehen, sind Änderungen in **"$shibboleth_home/conf/access-control.xml"** erforderlich.

<entry key="AccessByIPAddress">
<bohne id="AccessByIPAddress" parent="shibboleth.IPRangeAccessControl"
p:allowedRanges="#{'127.0.0.1/32',**'0.0.0.0/0'**, '::1/128', '10.78.93.103/32'} }" />
</entry>

Fügen Sie **'0.0.0.0/0'** zu den zulässigen Bereichen hinzu. Dies ermöglicht Anforderungen aus einem beliebigen IP-Bereich.

Konfiguration von Shibboleth zur Integration mit IDs

Secure Hash Algorithm (SHA1) und Verschlüsselungskonfiguration in IDs

Um die Standardeinstellung für IDs auf SHA1 festzulegen, öffnen Sie **"$shibboleth_home/conf/idp.properties"** und legen Sie Folgendes fest:

idp.sign.config = shibboleth.SigningConfiguration.SHA1;

Diese Konfiguration kann auch geändert werden:

idp.encryption.optional = true

Wenn Sie den Wert auf true festlegen, wird bei aktiviertem Fehler bei der Suche nach einem zu verwendenden Verschlüsselungsschlüssel keine Anforderung ausfallen. Dies hunterstützt die Verschlüsselung "opportunistisch", d. h., wenn möglich zu verschlüsseln (ein kompatibler Schlüssel ist in den Metadaten des Peers zu verschlüsseln mit), aber die Verschlüsselung andernfalls zu überspringen.

Konfigurieren von uid und user_main für die SAML-Antwort

Die AttributeDefinition wird in **"$shibboleth_home/conf/attribute-resolver.xml"** hinzugefügt, um in der SAML-Antwort sAMAccountName und userPrincipalName der Datei zu uid und user_principal zuzuordnen.

Fügen Sie darüber hinaus die LDAP-Connector-Einstellungen mit dem Tag <DataConnector> hinzu.

> **Hinweis**: ReturnAttributes muss mit dem Wert "**sAMAccountName userPrincipalName**" angegeben werden.

> **Hinweis**: Bei Integration in ein Active Directory (AD) ist LDAPProperty zwingend erforderlich.

Nehmen Sie die Änderungen in **"$shibboleth_home/conf/attribute-filter.xml" auf.**

Ändern Sie die **"$shibboleth_home/conf/saml-nameid.xml"** in

IDP-Metadaten

IDP-Metadaten sind im Ordner "**$shibboleth_home/metadaten**" verfügbar. Die Datei "idp-metadaten.xml" kann über die API (Application Programming Interface) auf IdS hochgeladen werden.

PUT https://<idshost>:<idsport>/ids/v1/config/idpmetadaten

wobei **idsport** keine konfigurierbare Entität ist und der Wert **"8553" ist.**

> **Warnung**: Shibboleth-Metadaten **können** zwei Signaturzertifikate, das allgemeine Signaturzertifikat und den Backchannel enthalten. Navigieren Sie zur Datei **idp-backchannel.crt** in **"$shibboleth_home/dentials"**, um das Backchannel-Zertifikat zu identifizieren**.** Wenn das Back-Channel-Zertifikat in den Metadaten verfügbar ist, sollten Sie das Back-Channel-Zertifikat aus den Metadaten xml entfernen, bevor Sie es an IdS hochladen. Dies liegt daran, dass die von IdS verwendete Fedlet 12.0-Bibliothek nur ein Zertifikat in den Metadaten unterstützt. Wenn mehr als ein Signaturzertifikat verfügbar ist, verwendet Fedlet das erste verfügbare Zertifikat.

Metadatenanbieter konfigurieren

Der Eintrag in **$shibboleth_home/metadata-providers.xml** muss für die Metadatenanbieter konfiguriert werden**.**

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

wobei**"id"**-Attribut ein beliebiger eindeutiger Name sein kann.

Dieser Eintrag gibt an, dass ein Metadatenanbieter bei der angegebenen ID registriert ist und die Metadaten in der angegebenen Datei /opt/shibboleth-idp/SP/sp.xml verfügbar sind.

Service Provider (SP)-Metadaten von IdS müssen in die im Eintrag angegebene Metadatendatei kopiert werden.

> **Hinweis**: SP-Metadaten von IdS können über **GET https://<idshost>:<idsport>/ids/v1/config/spmetadaten** abgerufen werden, wobei **idsport** keine konfigurierbare Einheit ist und der Wert "8553" lautet.

Weitere Konfiguration für SSO

Dieses Dokument beschreibt die Konfiguration aus dem IdP-Aspekt für SSO zur Integration in den Cisco Identity Service. Weitere Informationen finden Sie in den einzelnen Produktkonfigurationsleitfäden:

- UCCX
- UCCE
- PCCE