Installare e configurare il provider di identità di Shibboleth (IdP) per Cisco Identity Service (IdS) per abilitare l'SSO

Sommario

Introduzione

In questo documento viene descritta la configurazione di OpenAM Identity Provider (IdP) per abilitare Single Sign-On (SSO).

Modelli di distribuzione Cisco IdS

Prodotto	Implementazione
UCCX	Coresidente
PCCE	Coresidente con CUIC (Cisco Unified Intelligence Center) e LD (Live Data)
UCCE	Coresidenti con CUIC e LD per installazioni 2k. Standalone per installazioni a 4k e 12k.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Unified Contact Center Express (UCCX) versione 11.6 o Cisco Unified Contact Center Enterprise versione 11.6 o Packaged Contact Center Enterprise (PCCE) versione 11.6, a

seconda dei casi.

> **Nota:** Questo documento fa riferimento alla configurazione di Cisco Identify Service (IdS) e del provider di identità (IdP). Il documento fa riferimento a UCCX negli screenshot ed esempi, tuttavia la configurazione è simile a quella di Cisco Identify Service (UCCX/UCCE/PCCE) e dell'IdP.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Install

Shibboleth è un progetto open-source che fornisce funzionalità Single Sign-On e consente ai siti di prendere decisioni informate sulle autorizzazioni per l'accesso individuale alle risorse online protette in modo da salvaguardare la privacy. Supporta il linguaggio SAML2 (Security Assertion Markup Language). IdS è un client SAML2 e dovrebbe supportare Shibboleth con modifiche minime o nulle in IdS. Nella versione 11.6, IdS è qualificato per lavorare con Shibboleth IdP.

> **Nota:** Questo documento fa riferimento a Shibboleth release 3.3.0 come parte della qualifica con SSO

Requisiti di sistema

Componente	Dettagli
Versione di Shibboleth	v3.3.0
Percorso download	http://shibboleth.net/downloads/identity-provider/
Installa piattaforma	Ubuntu 14.0.4 java versione "1.8.0_121"
Versione LDAP (Lightweight Directory Access Protocol)	Active Directory 2.0
Server Web Shibboleth	Apache Tomcat/8.5.12

Fare riferimento al wiki per l'installazione di Shibboleth

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

Configurazione

Integrazione con un server LDAP

Per integrare un server LDAP con shibboleth, è necessario aggiornare i campi in **$shibboleth_home/conf/ldap.properties** dove**$shibboleth_home**(il valore predefinito è /opt/shibboleth-idp) fa riferimento alla directory di installazione utilizzata durante l'installazione di

shibboleth.

Campo	Valore previsto	Descrizione
idp.authn.LDAP.trustCertificates	Risorsa da cui caricare i trust anchor, generalmente un file locale in ${idp.home}/credentials dove idp.home è una variabile di ambiente esportata come JAVA_OPTS in setenv.sh	%{idp.home}/credentials/ldap-server.crt
idp.authn.LDAP.trustStore	Risorsa per caricare un keystore Java contenente trust anchor, in genere un file locale in %{idp.home}/credentials	%{idp.home}/credentials/ldap-server.trus
idp.authn.LDAP.returnAttributes	Elenco separato da virgole di attributi LDAP da restituire. Per restituire tutti gli attributi, aggiungere "*".	*
idp.authn.LDAP.baseDN	DN di base in cui deve essere eseguita la ricerca LDAP	CN=users,DC=cisco,DC=com
idp.authn.LDAP.subtreeSearch	Se eseguire la ricerca in modo ricorsivo	vero
idp.authn.LDAP.userFilter	Filtro di ricerca LDAP	(sAMAccountName={utente})*
idp.authn.LDAP.bindDN	DN da associare quando viene eseguita la ricerca	administrator@cisco.com
idp.authn.LDAP.bindDNCredential	Password da associare quando viene eseguita la ricerca	
idp.authn.LDAP.dnFormat	Stringa di formattazione per generare i DN utente da autenticare	%s@adfsserver.cisco.com (%s@domainname)
idp.authn.LDAP.authenticator	Controlla il flusso di lavoro relativo alla modalità di autenticazione in base a LDAP	bindSearchAuthenticator
idp.authn.LDAP.ldapURL	URI connessione per la directory LDAP	

Per ulteriori informazioni, fare riferimento a:

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

File di configurazione di esempio

```
# Tempo di attesa in millisecondi perrisposte
#idp.authn.LDAP.responseTimeout = PT3S
## Configurazione SSL, jvmTrust,
certificateTrust o keyStoreTrust
#idp.authn.LDAP.sslConfig =
attendibilitàCertificato
## Se si utilizza certificateTrust, impostare
il percorso del certificato attendibile
idp.authn.LDAP.trustCertificates =
```

```
%{idp.home}/credentials/ldap-server.crt
## Se si utilizza keyStoreTrust, impostare il
percorso del truststore
idp.authn.LDAP.trustStore =
%{idp.home}/credentials/ldap-server.truststore
## Restituisci attributi durante
l'autenticazione
#idp.authn.LDAP.returnAttributes =
nomeEntitàUtente, sAMAccountName
idp.authn.LDAP.returnAttributes = *
## Proprietà risoluzione DN ##
# Risoluzione DN ricerca, utilizzata da
anonSearchAuthenticator,
bindSearchAuthenticator
N. perANNUNCIO: CN=Utenti,DC=esempio,DC=org
idp.authn.LDAP.baseDN =
CN=utenti,DC=cisco,DC=com
idp.authn.LDAP.subtreeSearch = vero
*idp.authn.LDAP.userFilter =
(sAMAccountName={utente})*
# configurazione ricerca binding
N. perANNUNCIO:
idp.authn.LDAP.bindDN=adminuser@dominio.com
idp.authn.LDAP.bindDN =
amministratore@cisco.com
idp.authn.LDAP.bindDNCredential = Cisco@123
# Formato risoluzione DN, utilizzato da
directAuthenticator, adAuthenticator
N. perAD utilizza
idp.authn.LDAP.dnFormat=%s@dominio.com
#idp.authn.LDAP.dnFormat =
%s@adfsserver.cisco.com
# Configurazione degli attributi LDAP, vedere
attribute-resolver.xml
# Nota, questoprobabilmente non verrà
applicato all'utilizzo di configurazioni del
resolver V2 legacy
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:vero}
idp.attribute.resolver.LDAP.trustCertificates
=
%{idp.authn.LDAP.trustCertificates:undefined}
idp.attribute.resolver.LDAP.searchFilter =
(sAMAccountName=$resolutionContext.principal)
```

Consenti richieste da tutti i client

Per garantire che le richieste provenienti da tutti i client vengano soddisfatte, sono necessarie modifiche in **"$shibboleth_home/conf/access-control.xml"**

<entry key="AccessByIPAddress">
<bean 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>

Aggiungere **'0.0.0.0/0'** agli intervalli consentiti. Ciò consente richieste da qualsiasi intervallo IP.

Configurare Shibboleth per l'integrazione con IdS

Configurazione SHA1 (Secure Hash Algorithm) e crittografia in IdS

Per configurare IdS in modo da impostare SHA1 come predefinito, aprire **"$shibboleth_home/conf/idp.properties"** e impostare:

idp.sign.config = shibboleth.SigningConfiguration.SHA1

La configurazione può anche essere modificata:

idp.encryption.optional = true

Se la proprietà viene impostata su true, l'impossibilità di individuare una chiave di crittografia da utilizzare, quando attivata, non determinerà un errore nella richiesta. Questa hconsente di eseguire la crittografia "opportunisticamente", ovvero di crittografare ogni volta che è possibile (una chiave compatibile si trova nei metadati del peer con cui eseguire la crittografia), ma di ignorare la crittografia in caso contrario.

Configurare uid e user_principal per la risposta SAML

AttributeDefinition viene aggiunto in **"$shibboleth_home/conf/attribute-resolver.xml"** per mappare sAMAccountName e userPrincipalName all'uid e all'user_principal nella risposta SAML.

Inoltre, aggiungere le impostazioni del connettore LDAP con il tag <DataConnector>.

> **Nota**: è necessario specificare ReturnAttributes con il valore "**sAMAccountName userPrincipalName**".

> **Nota**: LDAPProperty è obbligatorio in caso di integrazione con Active Directory (AD).

Incorpora le modifiche in **"$shibboleth_home/conf/attribute-filter.xml"**

Modificare **"$shibboleth_home/conf/saml-nameid.xml"** per includere

Metadati IdP

I metadati IdP sono disponibili nella cartella "**$shibboleth_home/metadata**" . Il file idp-metadata.xml può essere caricato in IdS tramite l'API (Application Programming Interface)

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

dove **idsport** non è un'entità configurabile e il valore è **"8553"**

> **Avviso:** I metadati Shibboleth **possono** contenere 2 certificati di firma, il certificato di firma generale e il backchannel. Passare al file **idp-backchannel.crt** in **"$shibboleth_home/credentials"** per identificare il certificato backchannel**.** Se il certificato backchannel è disponibile nei metadati, è necessario rimuovere il certificato backchannel dal file xml dei metadati prima di caricarlo in IdS. Ciò è dovuto al fatto che la libreria Fedlet 12.0 utilizzata da IdS supporta solo un certificato nei metadati. Se è disponibile più di un certificato di firma, viene utilizzato il primo certificato disponibile.

Configura provider di metadati

Ènecessario configurare i provider di metadati con la voce in **$shibboleth_home/metadata-providers.xml.**

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

dove**"id"** può essere qualsiasi nome univoco.

Questa voce indica che un provider di metadati è registrato con l'ID specificato e che i metadati sono disponibili nel file specificato /opt/shibboleth-idp/SP/sp.xml.

I metadati di IdS di Service Provider (SP) devono essere copiati nel metadataFile specificato nella voce.

> **Nota:** i metadati SP di IdS possono essere recuperati tramite **GET https://<idshost>:<idsport>/ids/v1/config/spmetadata,** dove **idsport** non è un'entità configurabile e il valore è **"8553".**

Ulteriore configurazione per SSO

In questo documento viene descritta la configurazione del provider di identità per l'integrazione di SSO con Cisco Identity Service. Per ulteriori informazioni, consultare le guide alla configurazione dei singoli prodotti:

- UCCX
- UCCE
- PCCE