Instale e configurar o fornecedor da identidade do Shibboleth (IdP) para o serviço da identidade de Cisco (IdS) para permitir o SSO

Índice

Introdução

Este documento descreve a configuração no fornecedor da identidade de OpenAM (IdP) para permitir sobre o único sinal (SSO).

Modelos de distribuição do Cisco IDS

Produto	Desenvolvimento
UCCX	Co-residente
PCCE	Co-residente com CUIC (centro unificado Cisco da inteligência) e LD (dados vivos)
UCCE	Co-residente com CUIC e LD para as disposições 2k. Autônomo para as disposições 4k e 12k.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Liberação 11.6 do Cisco Unified Contact Center Express (UCCX) ou liberação 11.6 do Cisco Unified Contact Center Enterprise ou liberação empacotada 11.6 da empresa do centro de

contato (PCCE) como aplicáveis.

Note: Este documento provê a configuração no que diz respeito ao serviço de Cisco Identitify (IdS) e ao fornecedor da identidade (IdP). O documento provê UCCX nos screenshots e nos exemplos, porém a configuração é similar no que diz respeito ao serviço de Cisco Identitify (UCCX/UCCE/PCCE) e ao IdP.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se sua rede está viva, assegure-se de que você compreenda o impacto potencial do comando any.

Instalação

O Shibboleth é um projeto da aberta que forneça único Sinal-em capacidades e permita que os locais façam decisões de autorização informado para o acesso individual de recursos em linha protegidos em uma maneira depreservação. Apoia o linguagem de marcação da afirmação da Segurança (SAML2). Os IdS são um cliente SAML2 e esperado não apoiar o Shibboleth com mínimo ou a nenhuma mudança nos IdS. Em 11.6, os IdS são qualificados para trabalhar com Shibboleth IdP.

Note: Este documento provê a liberação 3.3.0 do Shibboleth como parte da qualificação com SSO

Requisitos do sistema

Componente	Detalhes
Versão do Shibboleth	v3.3.0
Localização do download	http://shibboleth.net/downloads/identity-provide
Instale a plataforma	Ubuntu 14.0.4 versão "1.8.0_121" das Javas
Versão do Lightweight Directory Access Protocol (LDAP)	Diretório ativo 2.0
Web server do Shibboleth	Apache Tomcat/8.5.12

Consulte por favor o wiki para a instalação do Shibboleth

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

Configurar

Integre com um servidor ldap

Para integrar um servidor ldap com shibboleth, os campos precisam de ser atualizados em **$shibboleth_home/conf/ldap.properties onde** $shibboleth_home **(o padrão** é /opt/shibboleth-idp)

refere o diretório da instalação que é usado na instalação do shibboleth.

Campo	Valor esperado	Descrição
idp.authn.LDAP.trustCertificates	Um recurso para carregar âncoras da confiança de, geralmente um arquivo local em $ {idp.home} /credentials onde idp.home é um variável de ambiente exportado como JAVA_OPTS em setenv.sh	% {idp.home} /credentials/ldap-server.crt
idp.authn.LDAP.trustStore	Um recurso para carregar um keystore das Javas que contenha âncoras da confiança, geralmente um arquivo local em % {idp.home} /credentials	% {idp.home} /credentials/ldap-server.truststore
idp.authn.LDAP.returnAttributes	A lista separada vírgula de LDAPAttributes que precisa de ser retornado. Se você quer retornar todos os atributos, adicionar “*”.	*
idp.authn.LDAP.baseDN	O baseDN em que a busca LDAP precisa de ser executada	CN=users, dc=cisco, dc=com
idp.authn.LDAP.subtreeSearch	Se procurar recursively	verdadeiro
idp.authn.LDAP.userFilter	Filtro da busca LDAP	(sAMAccountName= {usuário}) *
idp.authn.LDAP.bindDN	DN a ligar com quando a busca for executada	administrator@cisco.com
idp.authn.LDAP.bindDNCredential	Senha a ligar com quando a busca for executada	
idp.authn.LDAP.dnFormat	Uma corda do formato para gerar o usuário DN para autenticar	% de s@adfsserver.cisco.com (% de s@domainname)
idp.authn.LDAP.authenticator	Controla os trabalhos para como a autenticação ocorre contra o LDAP	bindSearchAuthenticator
idp.authn.LDAP.ldapURL	Conexão URI para o diretório LDAP	

Para mais detalhes, consulte:

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

Arquivo de configuração de exemplo

```
#
h
o
r
a
n
o
s
m
i
l
i
s
```

segundos de espera para respostas

#idp.authn.LDAP.responseTimeout =

PT3S Configuração de SSL do ##, jvm Trust, certificate Trust, ouk ey Store Tr

ust
#idp.authn.LDAP.sslConfig = certificateTrust
##seusandoocertifi

cateTrustacima,grupoaotrajetodocertificadoconfiável
idp.authhn.LDA

```
P
.
t
r
u
s
t
C
e
r
t
i
f
i
c
a
t
e
s

=

%

{
i
d
p
.
h
o
m
e
}
/
c
r
e
d
e
n
t
i
a
l
s
/
l
d
a
p
-
s
e
r
v
e
r
.
c
r
t
#
#
```

seusandookeyStoreTrustacima,grupoaotrajetododotrustststoreidp.authn.

LDAP.trustStore=%{idp.home}/credentials/ldap-server.truststor

e
A
t
r
i
b
u
t
o
s
d
o
r
e
t
o
r
n
o
d
o
#
#
d
u
r
a
n
t
e
a
a
u
t
e
n
t
i
c
a
ç
ã
o
#
i
d
p
.
a
u
t
h
n
.
L
D
A
P
.
r
e
t
u
r
n

```
Attributes = userPrincipalName,sAMAccountName
idp.authn.LDAP.retu
```

```
r
n
A
t
t
r
i
b
u
t
e
s

=

*
#
#
d
a
s
p
r
o
p
r
i
e
d
a
d
e
s
d
a
d
e
f
i
n
i
ç
ã
o
d
o
#
#
D
N
#
d
e
f
i
n
i
ç
ã
o
d
a
b
u
s
```

caDN,usadapeloanonSearchAuthenticator,bindSearchAuthenticator#

f

olAD:Cn=Users,DC=example,DC=orgldp.authn.LDAP.baseDN = CN=users,

dc=cisco,dc=com
idp.authhn.LDAP.subtreeSearch=retificam*idp.auth

n
.
L
D
A
P
.
u
s
e
r
F
i
l
t
e
r

=

(
s
A
M
A
c
c
o
u
n
t
N
a
m
e
=

{
u
s
u
á
r
i
o
}
)
*
#
c
o
n
f
i
g
u
r
a
ç
ã
o
d
a
b

uscadoligamento#

forAD:idp.authn.LDAP.bindDN=adminuser@domain.co

midp.authn.LDAP.bindDN

=

administrator@cisco.com
midp.authn.LDAP.bi

ndDNCredential =

Cisco@123
#definição do formato DN, usada pelo diretA

uthenticator,adAuthenticator
#

usoidp.authn.LDAP.dnFormat=%s@doma

in.comdoforADC
#idp.authn.LDAP.dnFormat=%des@adfsserver.ciscco.c

o m # a c o n f i g u r a ç ã o d o a t r i b u t o L D A P , c o n s i d e r a a t t r i b u t e - r e s o l v e r . x m l # a n

o
t
a
,

t
h
i
s
l
i
k
e
l
y
n
ã
o
s
e
a
p
l
i
c
a
r
á
a
o
u
s
o
d
e
c
o
n
f
i
g
u
r
a
ç
õ
e
s
d
o
r
e
s
o
l
v
e
r
d
o
l
e
g
a

dov2idp.attribute.resolver.LDAP.ldapURL=

%{idp.auththn.LDAP.ldapUR

```
L
}
idp.attribute.resolver.LDAP.connectTimeout=%{idp.authn.LDAP.co
```

nnectTimeout:PT3S}
idp.attribute.resolver.LDAP.responseTimeout=%{

idp.authn.LDAP.responseTimeout:PT3S}
idp.attribute.resolver.LDAP.

baseDN =

%{idp.authn.LDAP.baseDN:indeterminadoi}
idp.attribute.res

olver.LDAP.bindDN = %{idp.authn.LDAP.bindDN:indeterminadoi}
idp.at

t
r
i
b
u
t
e
.
r
e
s
o
l
v
e
r
.
L
D
A
P
.
b
i
n
d
D
N
C
r
e
d
e
n
t
i
a
l
=
%
{
i
d
p
.
a
u
t
h
n
.
L
D
A
P
.
b
i
n
d
D
N
C
r

edential:indeterminado}idp.attribute.resolver.LDAP.useStartTLS=%

{idp.authn.LDAP.useStartTLS:verdadeiro}
idp.attribute.resolver.LD

AP.trustCertificates=%{idp.authn.LDAP.trustCertificates:indeterm

inado}
idp.attribute.resolver.LDAP.searchFilter=(sAMAccountName=$

```
r
e
s
o
l
u
t
i
o
n
C
o
n
t
e
x
t
.
p
r
i
n
c
i
p
a
l
)
```

Permita pedidos de todos os clientes

Para assegurar-se de que os pedidos de todos os clientes alcancem, as mudanças são exigidas em **"$shibboleth_home/conf/access-control.xml"**

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

Adicionar **'0.0.0.0/0' às** escalas permitidas. Isto permite pedidos de toda a escala IP.

Configurar o Shibboleth para integrar com IdS

Algoritmo de mistura segura (SHA1) e configuração de criptografia nos IdS

Para configurar IdS para optar o SHA1, **"$shibboleth_home/conf/idp.properties** aberto**" e** grupo:

idp.signing.config = shibboleth.SigningConfiguration.SHA1

Esta configuração pode igualmente ser mudada:

idp.encryption.optional = retificam

Se você a ajusta para retificar, a falha encontrar uma chave de criptografia para usar-se, quando permitida, não conduzirá à falha do pedido. Isto ajuda a fazer "oportunistamente" a criptografia, isto é, para cifrar sempre que possível (uma chave compatível é encontrada nos metadata do par

para cifrar com) mas para saltar de outra maneira a criptografia.

Configurar o uid e user_principal à resposta de SAML

O AttributeDefinition é adicionado em **"$shibboleth_home/conf/attribute-resolver.xml"** para traçar o sAMAccountName e o userPrincipalName ao ao uid e user_principal na resposta de SAML.

Além, adicionar os ajustes do conector do ldap com o <DataConnector> da etiqueta.

> **Note**: ReturnAttributes precisa de ser especificado com valor do "**userPrincipalName sAMAccountName**".

> **Note**: LDAPProperty é imperativo caso que se há uma integração com um diretório ativo (AD).

```
<AttributeDefinition xsi:type="Simple" id="ciscoUPN" sourceAttributeID="userPrincipalName">
 <Dependency ref="LDAP" />
 <AttributeEncoder xsi:type="SAML1String" name="user_principal" />
 <AttributeEncoder xsi:type="SAML2String" name="user_principal" friendlyName="user_principal" />
</AttributeDefinition>

<AttributeDefinition xsi:type="Simple" id="ciscoUID" sourceAttributeID="sAMAccountName">
 <Dependency ref="LDAP" />
 <AttributeEncoder xsi:type="SAML1String" name="uid" />
 <AttributeEncoder xsi:type="SAML2String" name="uid" friendlyName="uid" />
</AttributeDefinition>

    <DataConnector id="LDAP" xsi:type="LDAPDirectory"
     ldapURL="ldap://adfsserver.cisco.com"
     baseDN="CN=users,DC=cisco,DC=com"
     principal="administrator@cisco.com"
     principalCredential="<cred>">
        <FilterTemplate>
            <![CDATA[
                %{idp.attribute.resolver.LDAP.searchFilter}
            ]]>
        </FilterTemplate>
      <ReturnAttributes>sAMAccountName userPrincipalName</ReturnAttributes>
      <LDAPProperty name="java.naming.referral" value="follow"/>
    </DataConnector>
```

Incorpore as mudanças em **"$shibboleth_home/conf/attribute-filter.xml"**

```
<PolicyRequirementRule xsi:type="ANY" />


        <AttributeRule attributeID="ciscoUID">
            <PermitValueRule xsi:type="ANY" />
        </AttributeRule>

        <AttributeRule attributeID="ciscoUPN">
            <PermitValueRule xsi:type="ANY" />
        </AttributeRule>
```

Mude o **toinclude "$shibboleth_home/conf/saml-nameid.xml"**

```
<bean parent="shibboleth.SAML2AttributeSourcedGenerator"
        p:format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
        p:attributeSourceIds="#{ {'ciscoUPN'} }" />
<bean parent="shibboleth.SAML2AttributeSourcedGenerator"
        p:format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
        p:attributeSourceIds="#{ {'ciscoUID'} }" />
```

Metadata de IdP

Os metadata de IdP estão disponíveis no dobrador "**$shibboleth_home/metadata**". O arquivo idp-metadata.xml pode ser transferido arquivos pela rede aos IdS através da interface de programação de aplicativo (o API)

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

onde o **idsport** não está uma entidade configurável e o valor são **"8553"**

> **aviso:** Os metadata do Shibboleth **podem** conter 2 Certificados de assinatura, o certificado de assinatura geral e o backchannel. Navegue ao arquivo **idp-backchannel.crt em** "$shibboleth_home/credentials**"** para identificar o certificado do backchannel. **Se o** certificado do canal traseiro está disponível nos metadata, você deve remover o certificado do canal traseiro do xml dos metadata antes da transferência de arquivo pela rede aos IdS. Isto é porque a biblioteca do fedlet 12.0 que os IdS usam apoios somente um certifcate nos metadata. Se mais de um certificado de assinatura está disponível, o fedlet usa o primeiro certificado disponível.

Configurar fornecedores dos metadata

Nós precisamos de configurar os fornecedores dos metadata com a entrada em **$shibboleth_home/metadata-providers.xml.**

```
<bean parent="shibboleth.SAML2AttributeSourcedGenerator"
        p:format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
        p:attributeSourceIds="#{ {'ciscoUPN'} }" />
<bean parent="shibboleth.SAML2AttributeSourcedGenerator"
        p:format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
        p:attributeSourceIds="#{ {'ciscoUID'} }" />
```

onde o atributo **" identificação "** pode ser todo o nome exclusivo.

Esta entrada indica que um fornecedor dos metadata está registrado com a identificação dada e os metadata estão disponíveis no arquivo especificado /opt/shibboleth-idp/SP/sp.xml.

Os metadata do provedor de serviços (SP) dos IdS devem ser copiados ao metadataFile especificados na entrada.

> **Note**: Os metadata SP dos IdS podem ser recuperados através do **GET https://<idshost>:<idsport>/ids/v1/config/spmetadata,** onde o **idsport** não é uma entidade configurável e o valor é **"8553".**

Configuração mais adicional para o SSO

Este documento descreve a configuração do aspecto de IdP para que o SSO integre com o serviço da identidade de Cisco. Para uns detalhes mais adicionais, refira os manuais de configuração dos produtos individuais:

- UCCX
- UCCE
- PCCE