安装并且配置口令标识供应商(IdP)思科身份服务的(ID)启用SSO

目录

简介

本文描述在OpenAM标识供应商(IdP)的配置启用单个符号(SSO)。

Cisco IDS部署模型

产品	部署
UCCX	共存
PCCE	有CUIC (Cisco Unified智能中心)和LD的(Live数据)共存
UCCE	有CUIC和LD的共存2k部署的。 4k和12k部署的独立。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco Unified Contact Center Express (UCCX)版本11.6或Cisco Unified Contact Center Enterprise版本11.6或被包的Contact Center企业(PCCE)版本11.6如可适用。

  Note:本文参考配置关于思科Identitify服务(ID)和标识供应商(IdP)。 本文参考UCCX屏幕画面和示例，然而配置是类似的关于思科Identitify服务(UCCX/UCCE/PCCE)和IdP。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络实际，请保证您了解所有命令潜在影响。

安装

口令是提供单一登录功能并且允许站点做出已保护联机资源单个访问的消息灵通的审定决定以保密性保留的方式的开放原始码的软体项目。它支持安全断言标记语言(SAML2)。ID不是SAML2客户端和预计支持与最小的口令或在ID上的变化。在11.6， ID合格与口令IdP一起使用。

> **Note**:本文参考口令版本3.3.0作为条件的部分与SSO的

系统要求

组件	详细信息
口令版本	v3.3.0
下载位置	http://shibboleth.net/downloads/identity-provider/
安装平台	Ubuntu 14.0.4 Java版本"1.8.0_121"
轻量级目录访问协议(LDAP)版本	活动目录2.0
口令网络服务器	Apache Tomcat/8.5.12

为口令的安装请参考wiki

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

配置

集成LDAP服务器

要集成有口令的一个LDAP服务器，字段在$shibboleth_home的**$shibboleth_home/conf/ldap.properties**需要更新(**默认**是/opt/shibboleth-idp)是指安装目录在口令的安装使用。

字段	预期值
idp.authn.LDAP.trustCertificates	装载信任锚点的资源从，通常一个本地文件以$ {idp.home} /credentials那里idp.home是作为在setenv.sh的JAVA_OPTS导出的环境变量
idp.authn.LDAP.trustStore	装载包含信任锚点的Java keystore的资源，通常在% {idp.home的}一个/credentials
idp.authn.LDAP.returnAttributes	需要返回LDAPAttributes的逗号被分离的列表。如果要返回所有属性，
idp.authn.LDAP.baseDN	LDAP搜索需要被执行的baseDN
idp.authn.LDAP.subtreeSearch	是否递归搜索
idp.authn.LDAP.userFilter	LDAP搜索过滤器
idp.authn.LDAP.bindDN	绑定的DN与，当搜索被执行
idp.authn.LDAP.bindDNCredential	绑定的密码与，当搜索被执行
idp.authn.LDAP.dnFormat	生成用户Dns的一个格式化字符串验证

idp.authn.LDAP.authenticator	控制验证如何的工作流出现LDAP
idp.authn.LDAP.ldapURL	LDAP目录的连接URI

欲了解更详细的信息，请参考：

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

示例配置文件

```
#

f
o
r
r
e
s
p
o
n
s
e
s
#
i
d
p
.
a
u
t
h
n
.
L
D
A
P
.
r
e
s
p
o
n
s
e
T
i
m
e
o
u
t

=

P
T
3
S
```

```
#
#
S
S
L

j
v
m
T
r
u
s
t

c
e
r
t
i
f
i
c
a
t
e
T
r
u
s
t

k
e
y
S
t
o
r
e
T
r
u
s
t
#
i
d
p
.
a
u
t
h
n
.
L
D
A
P
.
s
s
l
```

C
o
n
f
i
g

=

c
e
r
t
i
f
i
c
a
t
e
T
r
u
s
t
#
#

c
e
r
t
i
f
i
c
a
t
e
T
r
u
s
t

i
d
p
.
a
u
t
h
n
.
L
D
A
P
.
t
r
u
s
t

```
Certificates = %{idp.home}/credentials/ldapserver.crt
##
keyStor
```

eTrust

truststore

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

```
ntials/ldap-server.truststore
##

#idp.authn.LDAP.returnAttributes
```

=

userPrincipalName

sAMAccountName

idp.authn.LDAP.returnAttribute

s

=

*
#
#
D
N

#
#
#

D
N

a
n
o
n
S
e
a
r
c
h
A
u
t
h
e
n
t
i
c
a
t
o
r

b
i
n
d
S
e
a
r
c
h
A
u
t
h
e
n
t
i
c
a
t
o
r
#

for AD

Cn=users

DC=example

DC=org idp.authhn.LDAP.baseDN=

Cn=user

s

Dc=cisco

Dc=com
idp.authhn.LDAP.subtreeSearch

=*idp.authhn.LDAP.

u
s
e
r
F
i
l
t
e
r

=

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

{

}
)
*****
#

#

f
o
r
A
D

i
d
p
.
a
u
t
h
n
.
L
D
A
P
.
b
i
n
d
D

N=adminuser@domain.com
idp.authn.LDAP.bindDN = administrator@cisc

o
.
c
o
m
i
d
p
.
a
u
t
h
n
.
L
D
A
P
.
b
i
n
d
D
N
C
r
e
d
e
n
t
i
a
l

=

C
i
s
c
o
@
1
2
3
#

D
N

d
i
r
e
c
t
A
u
t
h
e
n

ticator

adAuthenticator

for AD

idp.authn.LDAP.dnFormat=%s@domain

.com#idp.authn.LDAP.dnFormat = %s@adfsserver.cisco.com#LDAP resso

l
v
e
r
.
x
m
l
#

t
h
i
s
l
i
k
e
l
y

V
2

i
d
p
.
a
t
t
r
i
b
u
t
e
.
r
e
s
o
l
v
e
r
.
L
D
A
P
.
l
d
a
p
U
R
L
=

%
{

idp.authn.LDAP.ldapURL}
idp.attribute.resolver.LDAP.connectTimeou

t=%{idp.authn.LDAP.connectTimeout:PT3S}
idp.attribute.resolver.LD

AP.responseTimeout=${idp.authn.LDAP.responseTimeout:PT3S}
idp.att

```
r
i
b
u
t
e
.
r
e
s
o
l
v
e
r
.
L
D
A
P
.
b
a
s
e
D
N

=

%
{
i
d
p
.
a
u
t
h
n
.
L
D
A
P
.
b
a
s
e
D
N

}
i
d
p
.
a
t
t
r
```

ibute.resolver.LDAP.bindDN = %{idp.authn.LDAP.bindDN}
idp.attri

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
e
d
e

```
ntial

}
idp.attributeresolver.LDAP.useStartTLS=%{idp.authn.LDAP
```

.
u
s
e
S
t
a
r
t
T
L
S

}
i
d
p
.
a
t
t
r
i
b
u
t
e
.
r
e
s
o
l
v
e
r
.
L
D
A
P
.
t
r
u
s
t
C
e
r
t
i
f
i
c
a
t
e
s
=
%
{
i

dp.authn.LDAP.trustCertificates

}
idp.attribute.resolver.LDAP.se

```
archFilter=(sAMAccountName=$resolutionContext.principal)
```

允许从所有客户端的请求

要保证从所有客户端的请求到达，变化要求在“$shibboleth_home/conf/access-control.xml上”

<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>

添加**'0.0.0.0/0'**到允许范围。这允许从所有ip范围的请求。

配置口令集成ID

在ID的安全散列算法(SHA1)和加密配置

要配置ID默认为SHA1，请打开**“$shibboleth_home/conf/idp.properties”和**集：

idp.signing.config = shibboleth.SigningConfiguration.SHA1

此配置可能也更改：

idp.encryption.optional =真

如果设置它对真，疏忽找出加密密钥使用，当启用，不会导致请求失败。即，这帮助执行加密“机会主义”加密若情况许可(一兼容的密钥在对等体的元数据被找到加密与)，但是否则跳过加密。

配置uid和user_principal对SAML答复

AttributeDefinition在**“$shibboleth_home/conf/attribute-resolver.xml”**被添加映射sAMAccountName和userPrincipalName到到uid和user_principal在SAML答复。

另外，请添加与标记<DataConnector>的ldap连接器设置。

> **Note**: ReturnAttributes需要指定与值“**sAMAccountName userPrincipalName**”。

> **Note**: 如果有与激活目录(AD)的集成LDAPProperty是必须，万一。

```
<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>
```

合并在"$shibboleth_home/conf/attribute-filter.xml上的"变化

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


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

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

更改 "$shibboleth_home/conf/saml-nameid.xml" toinclude

```
<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'} }" />
```

IdP元数据

IdP元数据是可用的在文件夹"$shibboleth_home/metadata"。idp-metadata.xml文件可以上传到ID通过Application Programming Interface (API)

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

那里idsport不一个可配置实体和值是"8553"

> 警告：口令元数据能包含2签署的证书、一般签署的证书和backchannel。导航到在"$shibboleth_home/credentials的"文件idp-backchannel.crt识别backchannel证书。 如果反向信道证书是可用的在元数据，您应该从元数据xml删除反向信道证书在加载前到ID。这是因为fedlet 12.0库ID在元数据使用支持仅一certifcate。如果超过一签署的证书是可用的， fedlet使用第一可用的证书。

配置元数据供应商

我们需要配置与条目的元数据供应商在$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'} }" />
```

那里" id "属性可以是所有唯一的名称。

此条目表明元数据供应商注册与给的id，并且元数据是可用的在指定的文件/opt/shibboleth-idp/SP/sp.xml。

必须复制ID服务提供商(SP)元数据到在条目指定的metadataFile。

> **Note**: ID SP元数据可以通过**GET https://<idshost>:<idsport>/ids/v1/config/spmetadata**获取，**idsport**不是一个可配置实体，并且值是**"8553"。**

SSO的进一步配置

本文描述从IdP方面的配置SSO的能集成思科身份服务。关于更详细的资料，参考单个产品配置指南：

- UCCX
- UCCE
- PCCE