Instale y configure el proveedor de la identidad del santo y seña (IdP) para el servicio de la identidad de Cisco (IdS) para habilitar el SSO

Contenido

Introducción

Este documento describe la configuración en el proveedor de la identidad de OpenAM (IdP) para habilitar la sola muestra encendido (SSO).

Modelos de despliegue del Cisco IDS

Producto	Despliegue
UCCX	Coresidente
PCCE	Coresidente con CUIC (centro unificado Cisco de la inteligencia) y LD (datos vivos)
UCCE	Coresidente con CUIC y el LD para las implementaciones 2k. Independiente para las implementaciones 4k y 12k.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Versión 11.6 del Cisco Unified Contact Center Express (UCCX) o versión 11.6 del Cisco Unified Contact Center Enterprise o versión embalada 11.6 de la empresa del Centro de

contacto (PCCE) como aplicables.

> **Note**: Este documento se refiere a la configuración en cuanto al servicio de Cisco Identitify (IdS) y al proveedor de la identidad (IdP). El documento se refiere a UCCX al screenshots y a los ejemplos, no obstante la configuración es similar en cuanto al servicio de Cisco Identitify (UCCX/UCCE/PCCE) y al IdP.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si su red está viva, asegúrese de que usted entienda el impacto potencial del comando any.

Instalar

El santo y seña es un proyecto de fuente abierta que proporciona solo Muestra-en las capacidades y permite que los sitios tomen las decisiones informadas de autorización para el acceso individual de los recursos en línea protegidos de una manera aislamiento-que preserva. Soporta el lenguaje de marcado de la aserción de la Seguridad (SAML2). Los IdS son un cliente SAML2 y esperado soportar el santo y seña con mínimo o ningunos cambios en los IdS. En 11.6, los IdS se califican para trabajar con el santo y seña IdP.

> **Note**: Este documento se refiere a la versión 3.3.0 del santo y seña como parte de la calificación con el SSO

Requisitos del sistema

Componente	Detalles
Versión del santo y seña	v3.3.0
Ubicación de la descarga	http://shibboleth.net/downloads/identity-provide
Instale la plataforma	Ubuntu 14.0.4 versión de Java el "1.8.0_121"
Versión del Lightweight Directory Access Protocol (LDAP)	Active Directory 2.0
Web server del santo y seña	Apache Tomcat/8.5.12

Refiera por favor el wiki para la instalación del santo y seña

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

Configurar

Integre con un servidor LDAP

Para integrar a un servidor LDAP con el santo y seña, los campos necesitan ser puestos al día

en **$shibboleth_home/conf/ldap.properties donde** $shibboleth_home **(el valor por defecto** es /opt/shibboleth-idp) refiere al directorio del instalar que se utiliza en la instalación del santo y seña.

Campo	Valor esperado	Descripción
idp.authn.LDAP.trustCertificates	Un recurso para cargar las anclas de la confianza de, generalmente un archivo local en $ {idp.home} /credentials donde está una variable de entorno idp.home exportada como JAVA_OPTS en setenv.sh	% {idp.home} /credentials/ldap-server.crt
idp.authn.LDAP.trustStore	Un recurso para cargar un keystore de las Javas que contiene las anclas de la confianza, generalmente un archivo local en % {idp.home} /credentials	% {idp.home} /credentials/ldap-server.truststore
idp.authn.LDAP.returnAttributes	La lista separada coma de LDAPAttributes que necesita ser vuelto. Si usted quiere volver todos los atributos, agregue "*".	*
idp.authn.LDAP.baseDN	El baseDN en el cual la búsqueda LDAP necesita ser realizada	CN=users, dc=cisco, dc=com
idp.authn.LDAP.subtreeSearch	Si buscar recurrentemente	verdad
idp.authn.LDAP.userFilter	Filtro de la búsqueda LDAP	(sAMAccountName= {usuario}) *
idp.authn.LDAP.bindDN	DN a atar con cuando se realiza la búsqueda	administrator@cisco.com
idp.authn.LDAP.bindDNCredential	Contraseña a atar con cuando se realiza la búsqueda	
idp.authn.LDAP.dnFormat	Una cadena del formato para generar al usuario DN para autenticar	% de s@adfsserver.cisco.com (% de s@domainname)
idp.authn.LDAP.authenticator	Controla el flujo de trabajo para cómo la autenticación ocurre contra el LDAP	bindSearchAuthenticator
idp.authn.LDAP.ldapURL	Conexión URI para el directorio LDAP	

Para más detalles, refiérase:

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

Ejemplo de archivo de configuración

```
# hora en los milisegundos de esperar los forresponses
#idp.authn.LDAP.responseTimeout = PT3S
Configuración de SSL del ##, jvmTrust, certificateTrust,
o keyStoreTrust
#idp.authn.LDAP.sslConfig = certificateTrust
## si usa el certificateTrust arriba, conjunto a la
trayectoria del certificado confiable
idp.authn.LDAP.trustCertificates = % {idp.home}
/credentials/ldap-server.crt
## si usa el keyStoreTrust arriba, conjunto a la
trayectoria del truststore
idp.authn.LDAP.trustStore = % {idp.home}
/credentials/ldap-server.truststore
Atributos de la vuelta del ## durante la autenticación
```

```
#idp.authn.LDAP.returnAttributes = userPrincipalName,
sAMAccountName
idp.authn.LDAP.returnAttributes = *
## de las propiedades de la resolución del ## DN
# resolución de la búsqueda DN, usada por el
anonSearchAuthenticator, bindSearchAuthenticator
# forAD: Cn=Users, DC=example, DC=org
idp.authn.LDAP.baseDN = CN=users, dc=cisco, dc=com
idp.authn.LDAP.subtreeSearch = verdad
*idp.authn.LDAP.userFilter = (sAMAccountName= {usuario})
*
# configuración de la búsqueda del lazo
# forAD: idp.authn.LDAP.bindDN= adminuser@domain.com
idp.authn.LDAP.bindDN = administrator@cisco.com
idp.authn.LDAP.bindDNCredential = Cisco@123
# resolución del formato DN, usada por el
directAuthenticator, adAuthenticator
# uso el idp.authn.LDAP.dnFormat=% s@domain.com del
forAD
#idp.authn.LDAP.dnFormat = % de s@adfsserver.cisco.com
# la configuración del atributo LDAP, considera
attribute-resolver.xml
# la nota, thislikely no se aplicará al uso de las
configuraciones del software de resolución de nombres de
la herencia V2
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: indefinido}
idp.attribute.resolver.LDAP.bindDN = %
{idp.authn.LDAP.bindDN: indefinido}
idp.attribute.resolver.LDAP.bindDNCredential = %
{idp.authn.LDAP.bindDNCredential: indefinido}
idp.attribute.resolver.LDAP.useStartTLS = %
{idp.authn.LDAP.useStartTLS: verdad}
idp.attribute.resolver.LDAP.trustCertificates = %
{idp.authn.LDAP.trustCertificates: indefinido}
idp.attribute.resolver.LDAP.searchFilter =
(sAMAccountName=$resolutionContext.principal)
```

Permita las peticiones de todos los clientes

Para asegurarse de que las peticiones de todos los clientes alcancen, los cambios se requieren en **"$shibboleth_home/conf/access-control.xml"**

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

Agregue **'0.0.0.0/0' a los** rangos permitidos. Esto permite las peticiones de cualquier rango del IP.

Santo y seña de la configuración a integrar con los IdS

Algoritmo de troceo seguro (SHA1) y configuración de encripción en los IdS

Para configurar los IdS para omitir el SHA1, **"$shibboleth_home/conf/idp.properties** abierto**" y el** conjunto:

idp.signing.config = shibboleth.SigningConfiguration.SHA1

Esta configuración puede también ser cambiada:

idp.encryption.optional = verdad

Si usted la fija para verdad, el error localizar una clave de encripción para utilizar, cuando está habilitado, no dará lugar al error de la petición. Esto ayuda a hacer el cifrado “oportunista”, es decir, para cifrar siempre que sea posible (una clave compatible se encuentra en los meta datos del par para cifrar con) pero para saltar el cifrado de otra manera.

Configure el uid y user_principal a la respuesta de SAML

El AttributeDefinition se agrega en **“$shibboleth_home/conf/attribute-resolver.xml”** para asociar el sAMAccountName y el userPrincipalName al al uid y user_principal en la respuesta de SAML.

Además, agregue las configuraciones del conector del ldap con el <DataConnector> de la etiqueta.

> **Note**: ReturnAttributes necesita ser especificado con el valor “**userPrincipalName del sAMAccountName**”.

> **Note**: LDAPProperty es obligatorio en caso de que si hay una integración con un Active Directory (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 los cambios en **“$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>
```

Cambie el **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'} }" />
```

Meta datos de IdP

Los meta datos de IdP están disponibles en la carpeta "**$shibboleth_home/metadata**". El archivo idp-metadata.xml se puede cargar a los IdS vía la interfaz de programación de aplicaciones (el API)

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

donde no está el **idsport una** entidad configurable y el valor es el **"8553"**

> **Advertencia:** Los meta datos del santo y seña **pueden** contener 2 Certificados de firma, el certificado de firma general y el backchannel. Navegue al archivo **idp-backchannel.crt en** "$shibboleth_home/credentials**"** para identificar el certificado del backchannel. **Si el** certificado del canal posterior está disponible en los meta datos, usted debe quitar el certificado del canal posterior del xml de los meta datos antes de la carga a los IdS. Esto es porque la biblioteca del fedlet 12.0 que los IdS utilizan los soportes solamente un certifcate en los meta datos. Si más de un certificado de firma está disponible, el fedlet utiliza el primer certificado disponible.

Proveedores de los meta datos de la configuración

Necesitamos configurar los proveedores de los meta datos con la entrada en **$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'} }" />
```

donde el atributo **" identificación "** puede ser cualquier nombre único.

Esta entrada indica que un proveedor de los meta datos está registrado con la identificación dada y los meta datos están disponibles en el archivo especificado /opt/shibboleth-idp/SP/sp.xml.

Los meta datos del proveedor de servicio (SP) de los IdS se deben copiar al metadataFile especificados en la entrada.

> **Note**: Los meta datos SP de los IdS se pueden extraer

vía **GET https://<idshost>:<idsport>/ids/v1/config/spmetadata,** donde no está una entidad el **idsport** configurable y el valor es el **"8553".**

Configuración adicional para el SSO

Este documento describe la configuración del aspecto de IdP para que el SSO integre con el servicio de la identidad de Cisco. Para otros detalles, refiera a las guías de configuración del producto individual:

- UCCX
- UCCE
- PCCE