Configuración y solución de problemas de SSO en Cisco Unified Communications Manager (CUCM)

Contenido

Introducción

Este documento describe la función SSO en CUCM, la configuración, las sugerencias para resolver problemas, el análisis de registro de ejemplo y los recursos para obtener información adicional.

Prerequisites

Requirements

Cisco recomienda conocer algunos términos de inicio de sesión único (SSO):

- Lenguaje de marcado de aserción de seguridad (SAML): un estándar abierto para intercambiar datos de autenticación y autorización entre partes
- Service Provider (SP): el SP es la entidad que aloja el servicio. En este documento, Cisco Unified Communications Manager (CUCM) es el proveedor de servicios
- Proveedor de identidad (IdP): el IdP es la entidad que autentica las credenciales del cliente. La autenticación es completamente transparente para el SP, por lo que las credenciales pueden ser una tarjeta inteligente, nombre de usuario/contraseña, etc. Una vez que el IdP autentica las credenciales del cliente, genera una aserción, la envía al cliente y redirige al cliente al SP
- Aserciones - Una pieza de información sensible al tiempo que el IdP genera después de la autenticación exitosa de un usuario. El propósito de la afirmación es proporcionar información sobre el usuario autenticado al SP
- Enlaces: define el método de transporte utilizado para entregar los mensajes del protocolo SAML entre entidades. Los productos de Comunicaciones Unificadas de Cisco utilizan HTTP
- Perfiles: restricciones predefinidas y combinaciones de contenido de mensajes SAML (aserciones, protocolos, enlaces) que funcionan para lograr un caso práctico empresarial específico. Esta formación se centra en el perfil de inicio de sesión único del navegador web, ya que es el método que utiliza CUCM
- Metadatos: conjunto de información de configuración que se intercambia entre las partes. Contiene información como enlaces SAML admitidos, funciones operativas como IdP o SP, atributos de identificador admitidos, información de identificador e información de certificado utilizada para firmar y cifrar la solicitud o respuesta.

Componentes Utilizados

- Cisco Unified Communications Manager (CUCM) 12.5.1.14900-63
- Microsoft Windows Server 2016
- Servicios de federación de Active Directory (AD FS) 4.0

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

El objetivo de SSO es permitir que los usuarios y los administradores accedan a varias aplicaciones de Cisco Collaboration sin necesidad de autenticaciones independientes en cada una de ellas. La habilitación de SSO conlleva varias ventajas:

- Mejora la productividad porque los usuarios no necesitan volver a introducir las credenciales para la misma identidad en productos diferentes.
- Transfiere la autenticación del sistema que aloja las aplicaciones a un sistema de terceros. Usted crea un círculo de confianza entre un IdP y un proveedor de servicios que permite que el IdP autentique a los usuarios en nombre del SP.
- Proporciona cifrado para proteger la información de autenticación pasada entre el IdP, el proveedor de servicios y el usuario.SSO también oculta los mensajes de autenticación pasados entre el IdP y el proveedor de servicios de cualquier tercero externo.
- Esto puede reducir los costes, ya que se realizan menos llamadas al soporte técnico para restablecer contraseñas.

Círculo de confianza

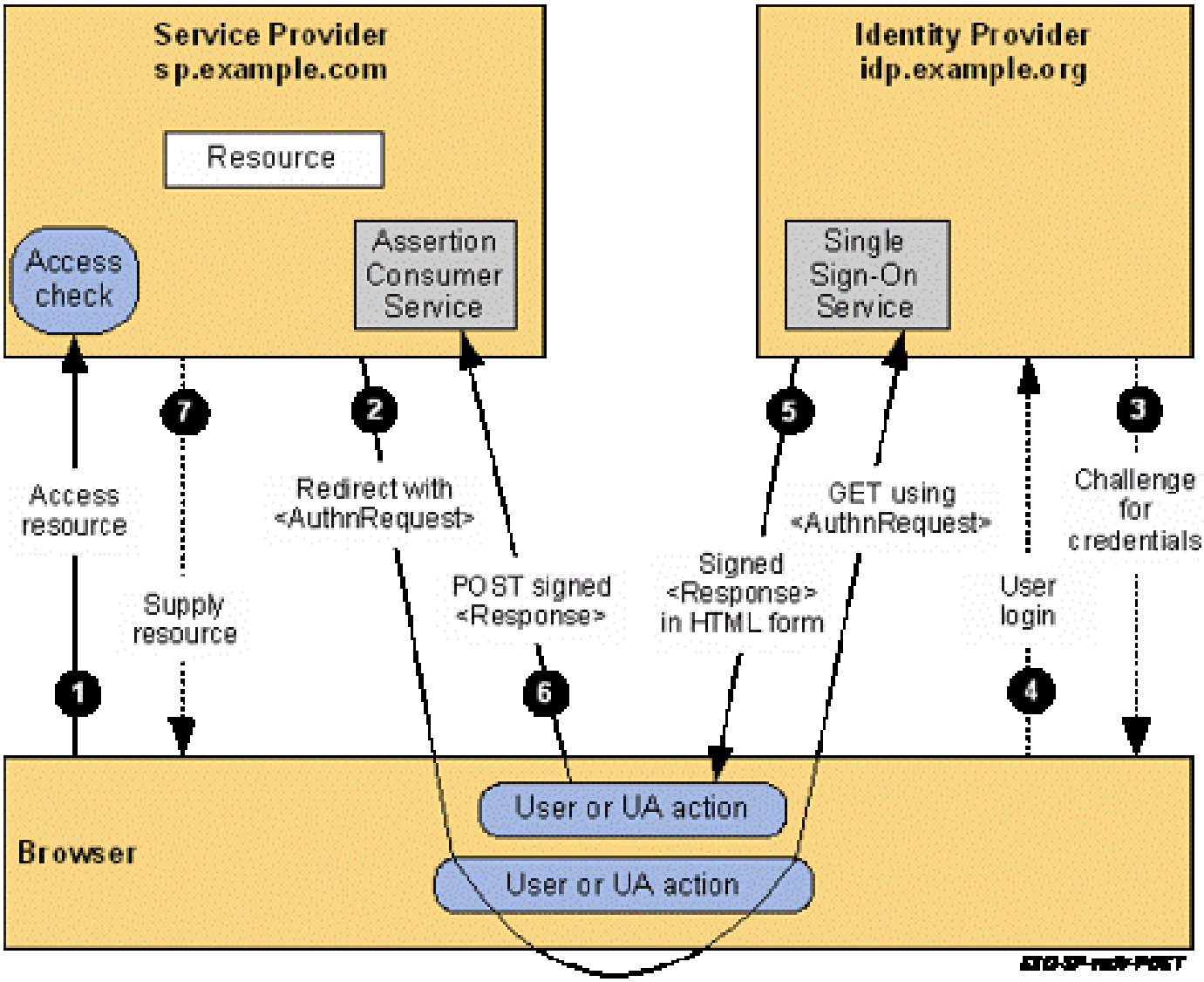
Los certificados desempeñan un papel muy importante en SSO y se intercambian entre el SP y el IdP a través de archivos de metadatos. El archivo de metadatos SP contiene el certificado de firma y cifrado del proveedor de servicios junto con otra información importante, como los valores de índice de consumo de servicios de aserción y la información HTTP POST/REDIRECT. El archivo de metadatos IdP contiene sus certificados junto con otra información sobre las capacidades IdP. Debe importar los metadatos SP en el IdP e importar los metadatos IdP en el SP para crear un círculo de confianza. Esencialmente, el SP firma y cifra cualquier solicitud que genera con el certificado en el que confía el IdP, y el IdP firma y cifra cualquier afirmación (respuesta) que genera con los certificados en los que confía el SP.

Nota: si cambia determinada información del SP, como el nombre de host/nombre de dominio completo calificado (FQDN) o el certificado de firma/cifrado (Tomcat o ITLRecrecovery), se puede romper el círculo de confianza. Descargue un nuevo archivo de metadatos del SP e impórtelo al IdP. Si cambia cierta información en el IdP, descargue un nuevo archivo de metadatos del IdP y vuelva a ejecutar la prueba de SSO para poder actualizar la información en el SP. Si no está seguro de si el cambio requiere una actualización de metadatos en el dispositivo opuesto, es mejor actualizar el archivo. No hay ningún inconveniente para una actualización de metadatos en ninguno de los lados y este es un paso válido para resolver problemas de SSO, especialmente si ha habido un cambio de configuración.

Configurar

Diagrama de la red

El flujo para un inicio de sesión SSO estándar se muestra en la imagen:

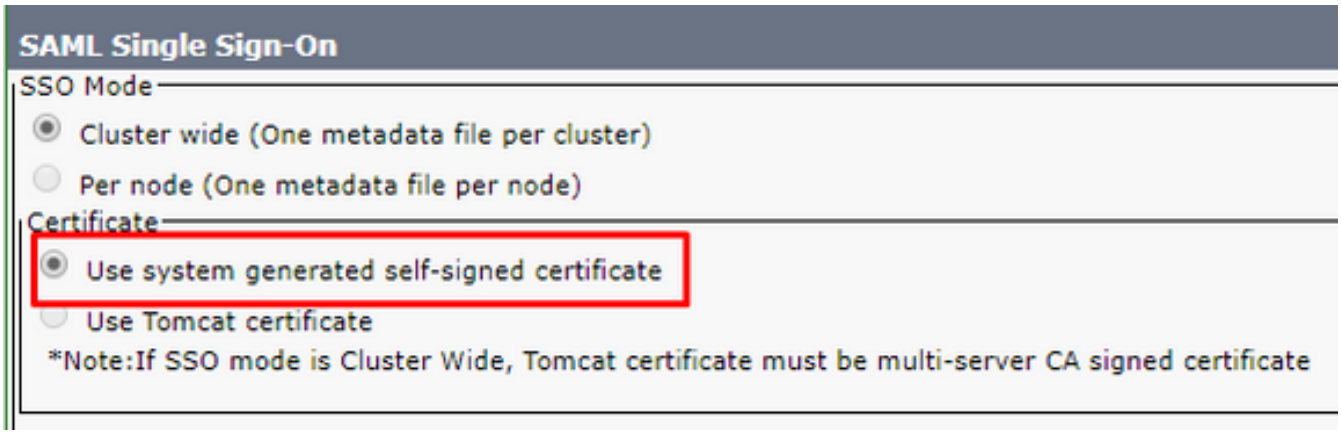


Nota: El proceso de la imagen no está en orden de izquierda a derecha. Recuerde que el SP es CUCM y el IdP es la aplicación de terceros.

Configuración

Desde la perspectiva de CUCM, hay muy poco que configurar con respecto a SSO. En CUCM 11.5 y versiones posteriores, puede seleccionar SSO por nodo o de ancho de clúster.

- En CUCM 11.5, SSO en todo el clúster requiere que se instale un certificado tomcat multiservidor en todos los nodos, ya que solo hay un archivo de metadatos para todo el clúster (y el certificado se almacena en ese archivo, por lo que cada nodo debe tener el mismo certificado tomcat).
- En CUCM 12.0 y versiones posteriores, tiene la opción de Utilizar certificado autofirmado generado por el sistema para SSO en todo el clúster. Esta opción utiliza el certificado ITLRecrecovery en lugar de tomcat:



- SSO por nodo es el valor predeterminado anterior a CUCM 11.5. En una configuración por nodo, cada nodo tiene su propio archivo de metadatos que debe importarse al IdP, ya que cualquiera de esos nodos puede redirigir potencialmente a un usuario para la autenticación.
- También puede habilitar SSO para RTMT en CUCM 11.5. Esta opción está activada de forma predeterminada y se encuentra en Administración de Cisco Unified CM > Parámetros de empresa > Usar SSO para RTMT.

Nota: La nota que indica Si el modo SSO es para todo el clúster, el certificado Tomcat debe ser un certificado firmado por CA de varios servidores es erróneo en 12.0 y 12.5 y se ha abierto un defecto para corregirlo (Id. de error de Cisco CSCvr49382).

Aparte de estas opciones, el resto de la configuración para SSO está en el IdP. Los pasos de configuración pueden diferir drásticamente en función del IdP que elija. Estos documentos contienen pasos para configurar algunos de los IdPs más comunes:

- Guía de configuración de Microsoft AD FS
- Guía de configuración de Okta
- Guía de configuración de PingFederate
- Guía de configuración de Microsoft Azure

Troubleshoot

Datos que recopilar

Para resolver un problema de SSO, establezca los seguimientos de SSO en debug. El nivel de registro de SSO no se puede establecer en debug mediante GUI. Para configurar el nivel de registro de SSO en debug, ejecute este comando en la CLI: set samltrace level debug

---

Nota: Este comando no se aplica a todo el clúster, por lo que debe ejecutarse en cada nodo que pueda estar implicado en un intento de inicio de sesión de SSO.

Una vez que el nivel de registro se haya configurado para depurar, reproduzca el problema y recopile estos datos de CUCM:

- Registros de Cisco SSO
- Registros de Cisco Tomcat

La mayoría de los problemas de SSO generan excepciones o errores en los registros de SSO, pero en algunas circunstancias, los registros de Tomcat también pueden ser útiles.

Análisis de ejemplo

Información del dispositivo del laboratorio TAC

CUCM (proveedor de servicios):

- Versión: 12.5.1.14900-11
- FQDN: 1cucm1251.sckiewer.lab

Windows Server 2016 (proveedor de identidad):

- Active Directory Federation Services 3.0
- FQDN: WinServer2016.sckiewer.lab

Revisión de registros para CUCM

```
tomcat/logs/ssosp/log4j/

%%%%% A user has attempted to access Cisco Unified CM Administration
2021-04-30 09:00:53,156 DEBUG [http-bio-443-exec-83] filter.SSOAuthAgentFilter - servlet path :/showHom
2021-04-30 09:00:53,157 DEBUG [http-bio-443-exec-83] filter.SSOAuthAgentFilter - recovery URL :/showRec

%%%%% You can see the SP and IdP EntityIDs here
2021-04-30 09:00:53,194 DEBUG [http-bio-443-exec-83] fappend.SamlLogger - SPSSOFederate: spEntityID is
2021-04-30 09:00:53,194 DEBUG [http-bio-443-exec-83] fappend.SamlLogger - SPSSOFederate: idpEntityID :

%%%%% The client is redirected to the SSO URL listed here
2021-04-30 09:00:53,196 DEBUG [http-bio-443-exec-83] fappend.SamlLogger - SPSSOFederate: SingleSignOnSe

%%%%% CUCM prints the AssertionConsumerService URL and you can see that CUCM uses an HTTP-POST
2021-04-30 09:00:53,196 DEBUG [http-bio-443-exec-83] fappend.SamlLogger - SPSSOFederate: AssertionConsu
2021-04-30 09:00:53,196 DEBUG [http-bio-443-exec-83] fappend.SamlLogger - SPSSOFederate: AssertionConsu
2021-04-30 09:00:53,196 DEBUG [http-bio-443-exec-83] fappend.SamlLogger - SPSSOFederate: AssertionConsu

%%%%% Here CUCM prints the AuthnRequest to the client. The client is redirected to the IdP with a 302 a
2021-04-30 09:00:53,199 DEBUG [http-bio-443-exec-83] fappend.SamlLogger - SPSSOFederate: AuthnRequest:<
ID="s29fd87c888ef6a4bc8c48d7e7087a8aeb997dd76f" Version="2.0" IssueInstant="2021-04-30T13:00:53Z" Desti
<saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">1cucm1251.sckiewer.lab</saml:Issuer>
<samlp:NameIDPolicy xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" Format="urn:oasis:names:tc:SAML:
</samlp:AuthnRequest>

%%%%% You can see that CUCM has received an encoded SAML response that is base64 encoded
2021-04-30 09:01:03,986 DEBUG [http-bio-8443-exec-85] authentication.SAMLAuthenticator - SAML Response

%%%%% Here is the encrypted SAML response from the client. You can see that the InResponseTo value matc
2021-04-30 09:01:04,005 DEBUG [http-bio-8443-exec-85] fappend.SamlLogger - SPACSUtils.getResponse: got
<samlp:StatusCode xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
Value="urn:oasis:names:tc:SAML:2.0:status:Success">
```

```
</samlp:StatusCode>
</samlp:Status><EncryptedAssertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion"><xenc:EncryptedData xm

%%%%% Here you can see that the IdP uses a supported binding type
2021-04-30 09:01:04,010 DEBUG [http-bio-8443-exec-85] fappend.SamlLogger - SAML2Utils.verifyResponse:bi

%%%%% The decrypted assertion is printed here. You see that a lot of important information covered late
2021-04-30 09:01:04,090 DEBUG [http-bio-8443-exec-85] authentication.SAMLAuthenticator - <Assertion xml

%%%%% CUCM looks at its current time and makes sure that it is within the validity timeframe of the ass
2021-04-30 09:01:04,090 DEBUG [http-bio-8443-exec-85] authentication.SAMLAuthenticator - Time Valid?:tr
2021-04-30 09:01:04,090 DEBUG [http-bio-8443-exec-85] authentication.SAMLAuthenticator - SAML Authentic
2021-04-30 09:01:04,090 DEBUG [http-bio-8443-exec-85] authentication.SAMLAuthenticator - Attributes: {u

%%%%% CUCM prints the username here
2021-04-30 09:01:04,090 DEBUG [http-bio-8443-exec-85] authentication.SAMLAuthenticator - userid is ::ad
2021-04-30 09:01:04,090 DEBUG [http-bio-8443-exec-85] authentication.SAMLAuthenticator - Realy state is
2021-04-30 09:01:04,091 DEBUG [http-bio-8443-exec-85] authentication.SAMLAuthenticator - http request c

%%%%% The client is redirected to the resource it initially tried to access
2021-04-30 09:01:04,283 INFO [http-bio-8443-exec-85] servlet.RelayToOriginalAppServlet - relayUrl ::/cc
2021-04-30 09:01:04,284 INFO [http-bio-8443-exec-85] servlet.RelayToOriginalAppServlet - redirecting to
```

Análisis más detallado de la solicitud y afirmación SAML

Solicitud SAML

Análisis e información sobre la solicitud SAML:

```
AuthnRequest:<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"

%%%%% The ID from the request is returned in the assertion generated by the IdP.  This allows CUCM to c
%%%%% This log snippet was taken from CUCM 12.5, so you use the AssertionConsumerServiceIndex rather th
ID="s29fd87c888ef6a4bc8c48d7e7087a8aeb997dd76f" Version="2.0" IssueInstant="2021-04-30T13:00:53Z" Desti
<saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">1cucm1251.sckiewer.lab</saml:Issuer>

%%%%% The NameID Format must be transient.
%%%%% The SP Name Qualifier allows us to see which node generated the request.
<samlp:NameIDPolicy xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" Format="urn:oasis:names:tc:SAML:
</samlp:AuthnRequest>
```

Afirmación

Análisis e información sobre la respuesta SAML:

<#root>

```
<Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion" ID="_23d2b89f-7e75-4dc8-b154-def8767a391c" Iss

%%%%% You can see that the issuer of the assertion was my Windows server
```

```
<Issuer>http://WinServer2016.sckiewer.lab/adfs/services/trust</Issuer>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
<ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
<ds:Reference URI="#_23d2b89f-7e75-4dc8-b154-def8767a391c">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
<ds:DigestValue>aYnlNK8NiHWHshYMggpeDsta2GyUKQI5MmRmx+gI374=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>rvkc6QWoTCLDly8/MoRCzGcu0FJr6PSu5BTQt3qp5ua7J/AQbbzWn7gWK6TzI+xcH2478M2Smm5mIVVINXnG
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>MIIC8DCCAdigAwIBAgIQQ2RhydxzTY1GQQ88eF3LWjANBgkqhkiG9w0BAQsFADA0MTIwMAYDVQQDEylBREZ
</ds:X509Data>
</KeyInfo>
</ds:Signature>
<Subject>

%%%%% The NameID Format is transient which is what CUCM expects
<NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient" NameQualifier="http://WinServer201
<SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">

%%%%% You have an InResponseTo value that matches our SAML request, so you can correlate a given assert
<SubjectConfirmationData InResponseTo="s29fd87c888ef6a4bc8c48d7e7087a8aeb997dd76f" NotOnOrAfter="2021-0
</SubjectConfirmation>
</Subject>


%%%%% You can see here that this assertion is only to be considered valid from 13:01:03:891-14:01:03:89


<Conditions NotBefore="2021-04-30T13:01:03.891Z" NotOnOrAfter="2021-04-30T14:01:03.891Z">
<AudienceRestriction>
<Audience>1cucm1251.sckiewer.lab</Audience>
</AudienceRestriction>
</Conditions>


%%%%% AttributeStatement is a required section that provides the ID of the user (admin in this case) an
<AttributeStatement>
<Attribute Name="uid">
<AttributeValue>admin</AttributeValue>
</Attribute>
</AttributeStatement>
<AuthnStatement AuthnInstant="2021-04-30T13:01:03.844Z" SessionIndex="_23d2b89f-7e75-4dc8-b154-def8767a
<AuthnContext>
<AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</AuthnContextCl
</AuthnContext>
</AuthnStatement>
</Assertion> XML Representation
```

Comandos útiles de CLI

- utils sso disable - Esto le permite inhabilitar SSO si no es funcional
- utils sso status - Muestra el estado actual de SSO en el nodo
- utils sso recovery-url enable - Esto le permite inhabilitar la URL de recuperación
- utils sso recovery-url disable - Esto le permite habilitar la URL de recuperación
- show samltrace level - Muestra el nivel de registro actual para los registros de SSO
- set samltrace level - Esto le permite establecer el nivel de registro para los registros SSO. Esto debe configurarse en DEBUG para que podamos resolver eficazmente los problemas.

Cambio de AssertionConsumerServiceURL a AssertionConsumerServiceIndex

Cuando se agregó SSO en todo el clúster en CUCM 11.5, CUCM ya no escribe la URL de AssertionConsumerService (ACS) en la solicitud SAML. En su lugar, CUCM escribe el AssertionConsumerServiceIndex. Vea estos fragmentos de una solicitud SAML:

CUCM anterior a 11.5.1:

```
AssertionConsumerServiceURL="https://1cucm1101.sckiewer.lab:443/ssosp/saml/SSO/alias/1cucm1101.sckiewer
```

CUCM 11.5.1 y superiores:

```
AssertionConsumerServiceIndex="0"
```

En la versión 11.5 y posteriores, CUCM espera que el IdP utilice el número de índice ACS de la solicitud para buscar la URL ACS del archivo de metadatos que se cargó durante el proceso de configuración. Este fragmento de metadatos de CUCM muestra la URL POST (del publicador) asociada con el índice 0:

```
<md:AssertionConsumerService index="0" Location="https://cucm14.sckiewer.lab:8443/ssosp/saml/SSO/alias/
```

No existe una solución alternativa para cambiar este comportamiento y el IdP debe utilizar los valores del Índice ACS en lugar de la URL ACS. Puede encontrar más información aquí, Id. de error de Cisco CSCvc56596.

Problemas comunes

No se puede acceder a la administración del sistema operativo o a la recuperación ante desastres

En CUCM 12.x, las aplicaciones web de Cisco Unified OS Administration y Disaster Recovery

System utilizan SSO. Si los intentos de inicio de sesión de estas aplicaciones fallan con un error 403 después de habilitar SSO, probablemente se deba a que la plataforma CUCM no puede encontrar el ID de usuario. Esto se debe a que estas aplicaciones no hacen referencia a la tabla de usuario final utilizada por Administración de CM, Serviciabilidad e Informes. Debido a esto, el ID de usuario que el IdP ha autenticado no existe en el lado de la plataforma de CUCM, por lo que CUCM devuelve un 403 Forbidden. Este documento detalla cómo agregar los usuarios adecuados al sistema para que las aplicaciones de la plataforma utilicen SSO con éxito.

Falla de NTP

SSO es sensible al tiempo porque el IdP asocia un 'período de validez' a las aserciones. Para verificar si la hora es el problema en su caso, puede buscar esta sección en los registros de SSO:

```
2021-04-30 09:01:04,090 DEBUG [http-bio-8443-exec-85] authentication.SAMLAuthenticator - Time Valid?:tr
2021-04-30 09:01:04,090 DEBUG [http-bio-8443-exec-85] authentication.SAMLAuthenticator - SAML Authentic
```

Si encuentra Time Valid?:false en sus registros de SSO, investigue la sección Condiciones de la afirmación para identificar el marco de tiempo que la afirmación debe considerarse válida:

```
<Conditions NotBefore="2021-04-30T13:01:03.891Z" NotOnOrAfter="2021-04-30T14:01:03.891Z">
<AudienceRestriction>
<Audience>1cucm1251.sckiewer.lab</Audience>
</AudienceRestriction>
</Conditions>
```

Puede ver en el fragmento de ejemplo que esta afirmación sólo es válida de 13:01:03:8917 a 14:01:03:8917 el 30/4/2021. En un escenario de error, consulte el momento en que CUCM recibió esta afirmación y verifique que se encuentra dentro del período de validez de la afirmación. Si el tiempo que CUCM procesó la afirmación está fuera del período de validez, esta es la causa del problema. Asegúrese de que CUCM y el IdP se sincronicen con el mismo servidor NTP, ya que SSO es muy sensible al tiempo.

Instrucción de atributo no válida

Refiérase al análisis de la afirmación aquí y vea la nota sobre la sentencia de atributo. Los productos de Cisco Unified Communications requieren que el IdP proporcione una declaración de atributo, pero a veces el IdP no envía una. A modo de referencia, se trata de una AttributeStatement válida:

```
<AttributeStatement>
<Attribute Name="uid">
<AttributeValue>admin</AttributeValue>
</Attribute>
```

```
</AttributeStatement>
```

Si ve una aserción del IdP, pero se omite la sentencia de atributo, trabaje con el proveedor de su software de IdP para realizar los cambios necesarios de modo que proporcione esta declaración. La corrección difiere según el IdP y, en algunos escenarios, se puede enviar más información en esta instrucción que la que se ve en el fragmento de código. Siempre que haya un Nombre de atributo establecido en uid y un Valor de atributo que coincida con un usuario con los privilegios correctos en la base de datos de CUCM, el inicio de sesión se realizará correctamente.

Dos certificados de firma: AD FS

Este problema es específico de Microsoft AD FS. Cuando el certificado de firma en AD FS está a punto de caducar, Windows Server genera automáticamente un nuevo certificado, pero deja el certificado antiguo en su lugar hasta que caduque. Cuando esto ocurre, los metadatos de AD FS contienen dos certificados de firma. El mensaje de error que puede ver cuando intenta ejecutar la prueba SSO durante este período de tiempo es Error al procesar la respuesta SAML.

Nota:Error al procesar la respuesta SAML también se puede presentar para otros problemas, así que no asuma que este es su problema si ve este error. Asegúrese de verificar los registros de SSO para verificarlos.

Si ve este error, revise los registros de SSO y busque lo siguiente:

```
2018-12-26 13:49:59,581 ERROR [http-bio-443-exec-45] authentication.SAMLAuthenticator - Error while pro
com.sun.identity.saml2.common.SAML2Exception: The signing certificate does not match what's defined in
```

Este error indica que los metadatos IdP importados en CUCM contienen un certificado de firma que no coincide con lo que el IdP utilizado en este intercambio SAML. Este error suele producirse porque AD FS tiene dos certificados de firma. Cuando el certificado original está a punto de expirar, AD FS genera automáticamente un nuevo certificado. Debe descargar un nuevo archivo de metadatos de AD FS, comprobar que solo tiene un certificado de firma y cifrado e importarlo a CUCM. Otros IdPs también tienen certificados de firma que deben actualizarse para que sea posible que alguien lo haya actualizado manualmente, pero simplemente no haya importado el nuevo archivo de metadatos que contiene el nuevo certificado a CUCM.

Si encuentra los errores mencionados:

- Si usa AD FS, consulte Id. de error de Cisco CSCuj66703
- Si NO utiliza AD FS, recopile un nuevo archivo de metadatos del IdP e impórtelo en CUCM

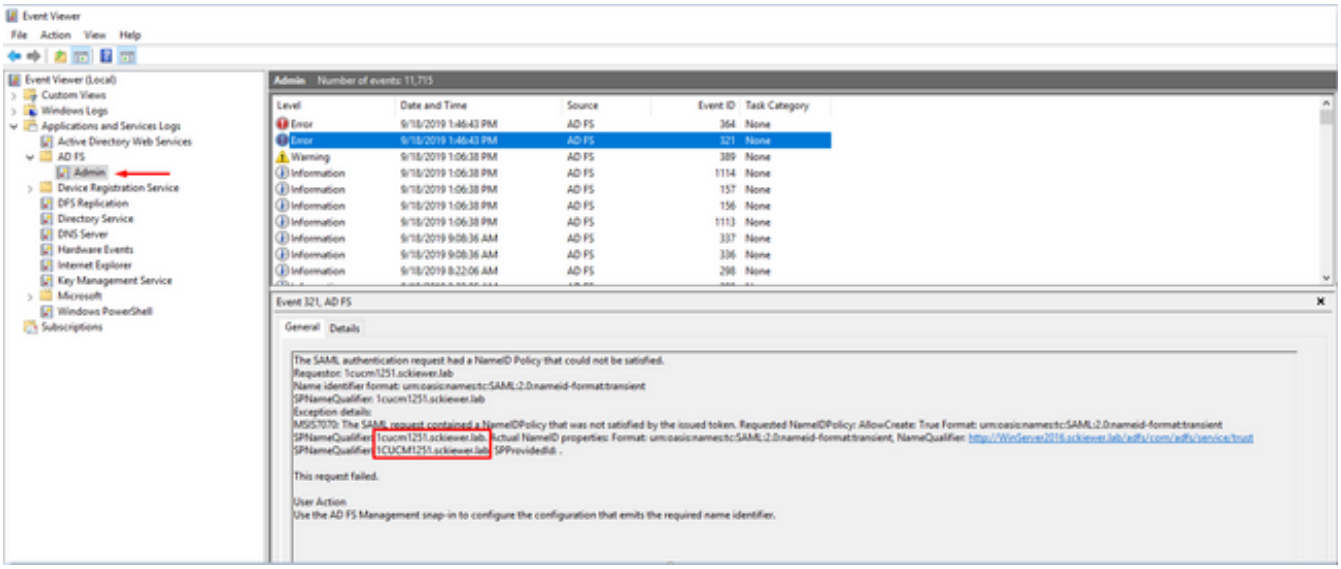
Código de estado no válido en respuesta

Este es un error común en implementaciones con AD FS:

```
Invalid Status code in Response. This may be caused by a configuration error in the IDP. Please check t
```

En casi todos los casos, se trata de un problema con la regla de reclamación del lado de AD FS. Pegue primero la regla en el bloc de notas, agregue los Id. de entidad y, a continuación, pegue la regla del bloc de notas en AD FS. En algunos escenarios, una copia/pegado directamente desde su correo electrónico o navegador puede omitir algunos de los signos de puntuación y causar un error de sintaxis.

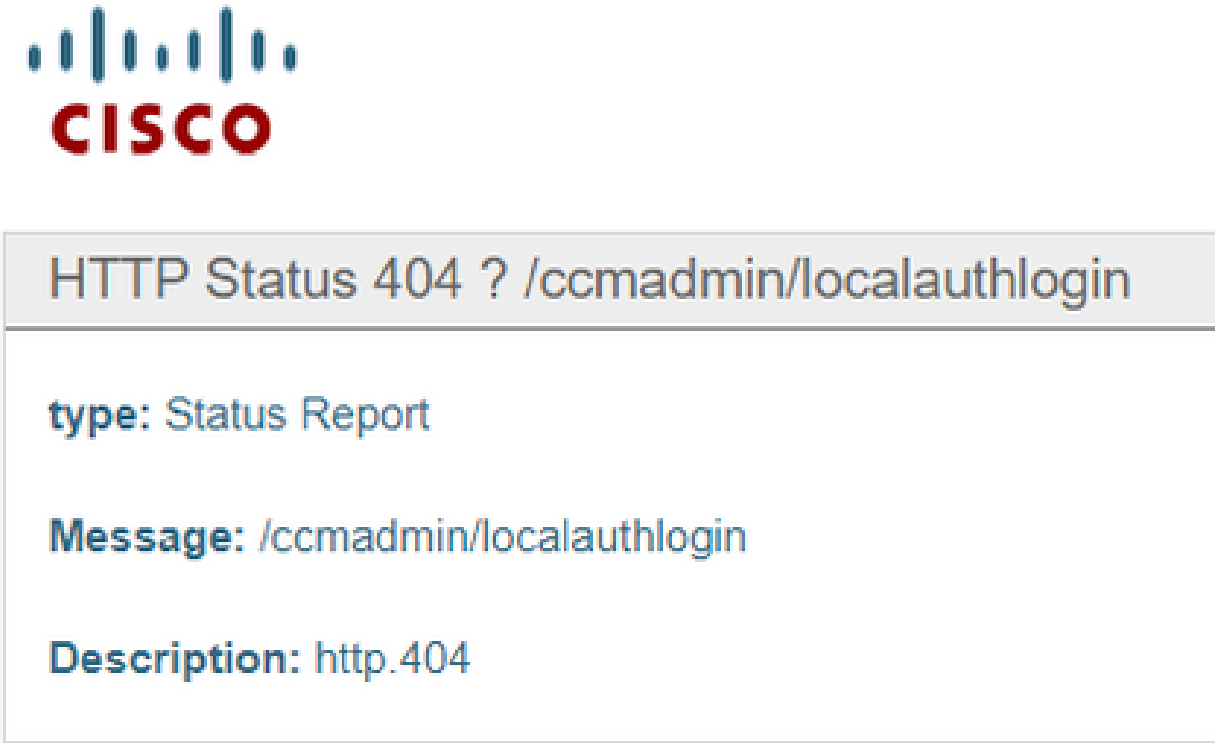
Otro problema común es que la regla de reclamación es que la capitalización del IdP o del FQDN del SP no coincide con el entityID en los archivos de metadatos. Compruebe los registros del Visor de sucesos en Windows Server para determinar si éste es su problema.



Puede ver en la imagen que el NameID solicitado es 1cucm1251.sckiewer.lab mientras que el NameID real es 1CUCM1251.sckiewer.lab. El NameID solicitado debe coincidir con el entityID en el archivo de metadatos SP mientras que el Actual NameID está establecido en la regla de reclamación. Para solucionar este problema, necesito actualizar la regla de reclamación con un FQDN en minúsculas para el SP.

Discordancia de estado de SSO entre CLI y GUI

En algunos casos, el estado de SSO de las utilidades y la GUI pueden mostrar información diferente con respecto a si SSO está habilitado o inhabilitado. La forma más sencilla de solucionar este problema es deshabilitar y volver a habilitar SSO. Hay bastantes archivos y referencias que se actualizan a través del proceso de habilitación, por lo que no es factible intentar actualizar manualmente todos esos archivos. En la mayoría de los casos, puede iniciar sesión en la GUI y deshabilitar y volver a habilitar sin problemas, sin embargo, es posible ver este error cuando intenta acceder al editor a través de la URL de recuperación o el enlace principal:



Puede verificar la GUI para ver si la URL de recuperación es una opción y también puede verificar la salida del estado de utils sso desde la CLI:

```
admin:utils sso status
SSO Status: SAML SSO Enabled
IdP Metadata Imported Date = Fri Apr 09 09:09:00 EDT 2021
SP Metadata Exported Date = Fri Apr 02 15:00:42 EDT 2021
SSO Test Result Date = Fri Apr 09 09:10:39 EDT 2021
SAML SSO Test Status = passed
Recovery URL Status = enabled
Entity ID = http://WinServer2016.sckiewer.lab/adfs/services/trust
```

A continuación, compruebe la tabla de nodos de proceso. En este ejemplo, puede ver que SSO está desactivado en la base de datos (consulte el valor tkssomode para 1cucm1251.sckiewer.lab en el extremo derecho):

```
admin:run sql select pkid,name,tkssomode from processnode
pkid                                 name                  tkssomode
====================================     ==================     =========
00000000-1111-0000-0000-000000000000     EnterpriseWideData        0
04bff76f-ba8c-456e-8e8f-5708ce321c20     1cucm1251.sckiewer.lab    0
```

```
admin:run sql select * from typessomode
enum name       moniker
==== ========== ==================
0    Disable    SSO_MODE_DISABLE
```

```
1     Agent Flow SSO_MODE_AGENT_FLOW
2     SAML       SSO_MODE_SAML
```

Para solucionar esto, vuelva a establecer el campo tkssomode en la tabla de nodos de proceso en 2 para que pueda iniciar sesión a través de la URL de recuperación:

```
admin:run sql update processnode set tkssomode='2' where name ='1cucm1251.sckiewer.lab'
Rows: 1

admin:run sql select pkid,name,tkssomode from processnode
pkid                                  name                  tkssomode
====================================  ====================  =========
00000000-1111-0000-0000-000000000000  EnterpriseWideData       0
04bff76f-ba8c-456e-8e8f-5708ce321c20  1cucm1251.sckiewer.lab   2
```

En este momento, pruebe la URL de recuperación y continúe con Disable > Re-enable of SSO que activa CUCM para actualizar todas las referencias en el sistema.

Información Relacionada

- Guía de implementación de SAML SSO para aplicaciones de Cisco Unified Communications, versión 12.5(1)
- Descripción técnica de Security Assertion Markup Language (SAML) V2.0
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).