تكوين SSO على Cisco Unified Communications Manager (CUCM) واستكشاف أخطائه وإصلاحها

المحتويات

المقدمة

يصف هذا وثيقة ال SSO سمة في CUCM، تشكيل، طرف أن يتحرى، مثال سجل تحليل، وموارد ل معلومة إضافية.

المتطلبات الأساسية

المتطلبات

توصي Cisco بمعرفة عدد قليل من مصطلحات تسجيل الدخول الأحادي (SSO):

- لغة تمييز تأكيد الأمان (SAML) - معيار مفتوح لتبادل بيانات المصادقة والتفويض بين الأطراف
- مزود الخدمة (SP) - SP هي الكيان الذي يستضيف الخدمة. في هذا المستند، يعد Cisco Unified Communications Manager (CUCM) هو مزود الخدمة
- موفر الهوية (IdP) - IdP هو الكيان الذي يقوم بمصادقة بيانات اعتماد العميل. تكون المصادقة شفافة تمامًا لـ SP حتى يمكن أن تكون بيانات الاعتماد بطاقة ذكية، اسم مستخدم/كلمة مرور، وهكذا. بمجرد أن يقوم IdP بمصادقة بيانات اعتماد العميل، فإنه يقوم بإنشاء تأكيد وإرساله إلى العميل وإعادة توجيه العميل مرة أخرى إلى SP
- التأكيدات - هي قطعة معلومات حساسة للوقت يتم إنشاؤها من قبل IdP بعد مصادقة ناجحة لمستخدم. والغرض من التأكيد هو توفير معلومات حول المستخدم الذي تمت مصادقته إلى SP
- الروابط - يحدد طريقة النقل المستخدمة لتقديم رسائل بروتوكول SAML بين الكيانات. تستخدم HTTP منتجات الاتصالات الموحدة من Cisco
- ملفات التعريف - القيود المحددة مسبقا ومجموعات من محتوى رسائل SAML (التأكيدات والبروتوكول والارتباطات) التي تعمل للحصول على حالة إستخدام أعمال معينة. يركز هذا التدريب على ملف تعريف تسجيل الدخول الأحادي لمستعرض الويب حيث أن هذه هي الطريقة المستخدمة من قبل CUCM
- البيانات الوصفية - مجموعة من معلومات التكوين التي يتم تبادلها بين الأطراف. يحتوي على معلومات مثل روابط SAML المدعومة والأدوار التشغيلية مثل IdP أو SP وسمات المعرف المدعومة ومعلومات المعرف ومعلومات الشهادة المستخدمة لتوقيع الطلب أو الاستجابة وتشفيرها.

المكونات المستخدمة

- Cisco Unified Communications Manager (CUCM) 12.5.1.14900-63
- نظام التشغيل Microsoft Windows Server 2016
- Active Directory Federation Services (AD FS)، الإصدار 4.0

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

الغرض من SSO أن يسمح للمستخدمين والمسئولين بالوصول إلى تطبيقات تعاون Cisco متعددة دون الحاجة إلى مصادقة منفصلة لكل واحد. يؤدي تمكين SSO إلى العديد من المميزات:

- وهو يحسن الإنتاجية لأن المستخدمين لا يحتاجون إلى إعادة إدخال بيانات الاعتماد لنفس الهوية على منتجات مختلفة.
- يقوم بنقل المصادقة من النظام الذي يستضيف التطبيقات إلى نظام تابع لجهة أخرى. يمكن إنشاء دائرة من الثقة بين معرف وموزع الخدمة مما يسمح للمعرف

بمصادقة المستخدمين نيابة عن SP.

- يوفر تشفير لحماية معلومات المصادقة التي يتم تمريرها بين IdP ومزود الخدمة والمستخدم.كما يخفي SSOs رسائل المصادقة التي يتم تمريرها بين IdP ومزود الخدمة من أي جهة خارجية.
- كما يمكن لهذا البرنامج أن يقلل من التكاليف حيث يتم إجراء عدد أقل من مكالمات مكتب المساعدة لإعادة تعيين كلمات المرور.

دائرة الثقة

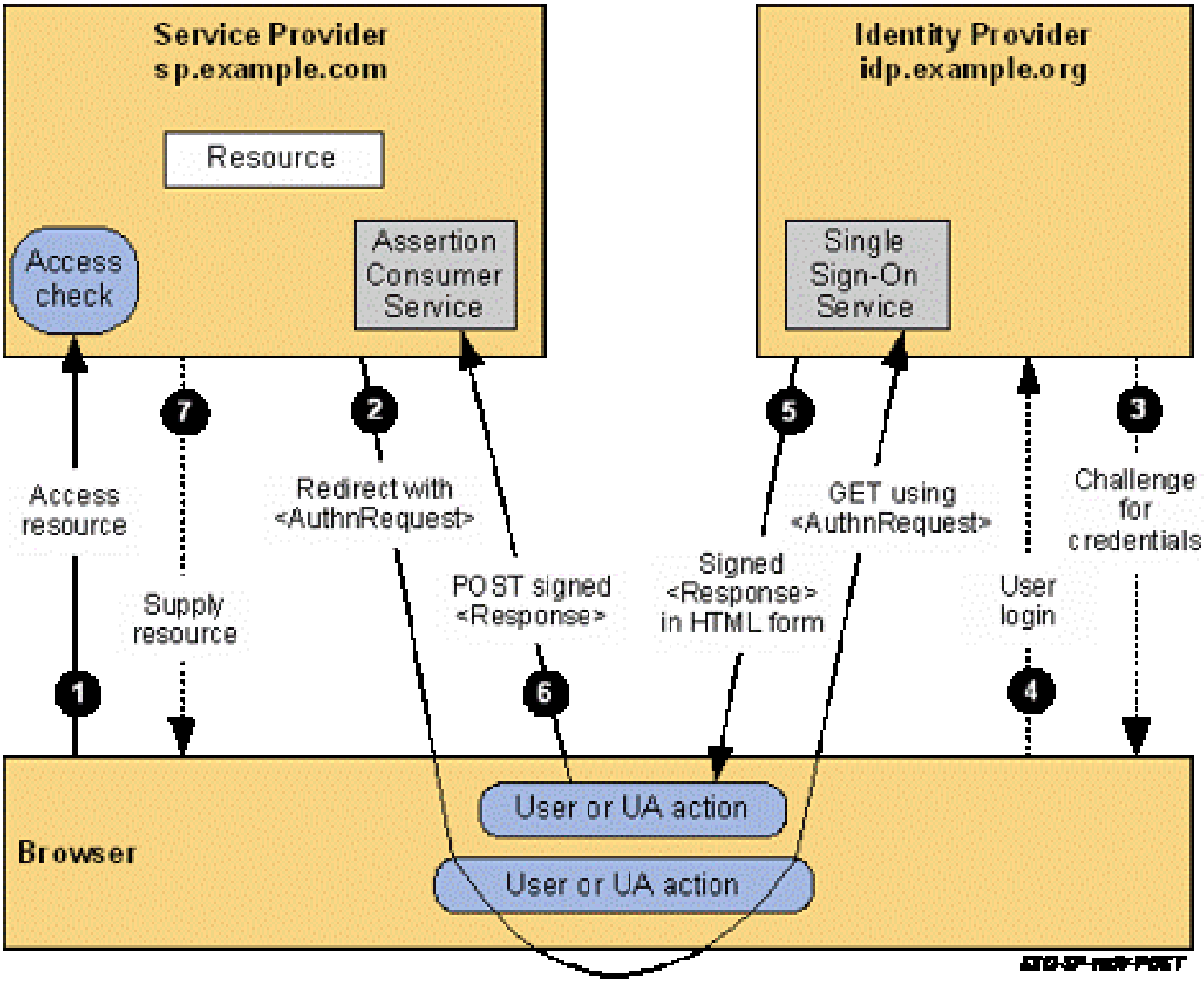
تلعب الشهادات دورا هاما جدا في SSO ويتم تبادلها بين SP و IDp عبر ملفات البيانات الأولية. يحتوي ملف بيانات تعريف SP على شهادة توقيع وتشفير مزود الخدمة بالإضافة إلى بعض المعلومات المهمة الأخرى مثل قيم فهرس Confirmation Consumption Service ومعلومات HTTP POST/REDIRECT. يحتوي ملف بيانات تعريف IdP على ترخيصه (ترخيصاته) بالإضافة إلى بعض المعلومات الأخرى حول إمكانيات IdP. يجب إستيراد بيانات تعريف SP إلى المعرف وإدراج بيانات تعريف IDp إلى SP لإنشاء دائرة ثقة. وبشكل أساسي، يقوم SP بتوقيع وتشفير أي طلب يقوم بتكوينه باستخدام الشهادة التي يثق بها IdP، ويوقع IdP ويشفر أي تأكيد (إستجابة) يقوم بتكوينه باستخدام شهادة (شهادات) يثق بها SP.

ملاحظة: في حالة تغيير بعض المعلومات الموجودة على SP، مثل اسم المضيف/اسم المجال المؤهل بالكامل (FQDN) أو شهادة التوقيع/التشفير (Tomcat أو ITLRecovery)، يمكن كسر دائرة الثقة. قم بتنزيل ملف بيانات تعريف جديد من SP واستيراده إلى IdP. إذا تغيرت معلومات معينة عن IDp، قم بتنزيل ملف بيانات تعريف جديد من IDp وأعد تشغيل إختبار SSO بحيث يمكنك تحديث المعلومات على SP. إذا لم تكن متأكدا ما إذا كان تغييرك يتطلب تحديث بيانات أولية على الجهاز المقابل، فمن الأفضل تحديث الملف. لا يوجد جانب سلبي لتحديث بيانات التعريف على أي من الجانبين، وهذه خطوة صالحة لاستكشاف أخطاء SSO وإصلاحها، خاصة إذا كان هناك تغيير في التكوين.

التكوين

الرسم التخطيطي للشبكة

يتم عرض تدفق سجل دخول SSO القياسي في الصورة:

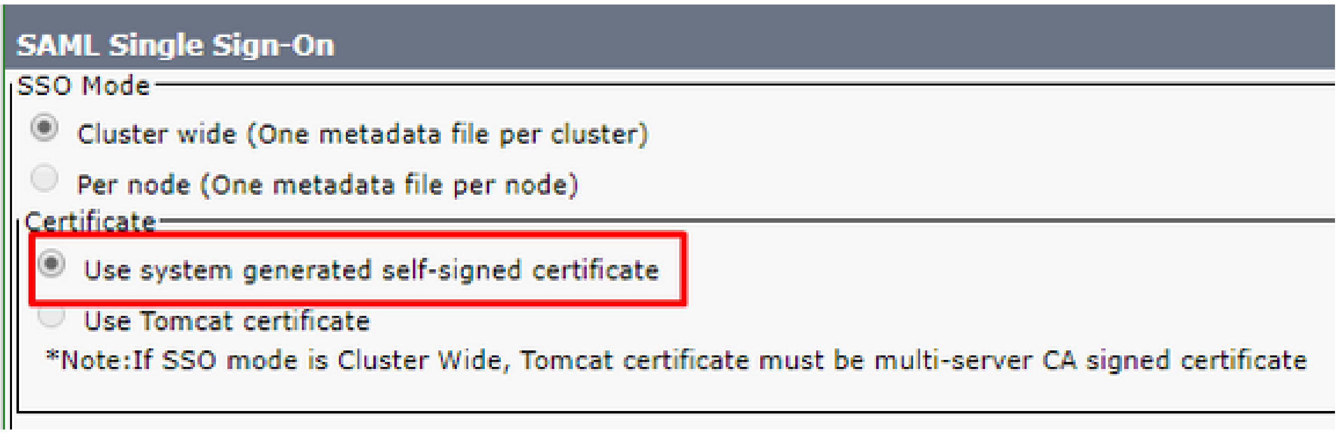


ملاحظة: العملية في الصورة ليست بالترتيب من اليسار إلى اليمين. تذكر أن SP هو CUCM و IDp هو تطبيق الطرف الثالث.

التكوين

ومن منظور الاتحاد الأفريقي لحفظ الطبيعة، لا يوجد سوى القليل جدا لتكوينه فيما يتعلق بمنظمات المجتمع المدني. في CUCM 11.5 أو أعلى، يمكنك تحديد Cluster wide أو SSO لكل عقدة.

- في CUCM 11.5، يتطلب SSO على مستوى نظام المجموعة تثبيت شهادة TOMCAT متعددة الخوادم على كافة العقد نظرا لأنه يوجد ملف بيانات أولية واحد فقط لنظام المجموعة بالكامل (ويتم تخزين الشهادة في هذا الملف، لذا يجب أن تحتوي كل عقدة على نفس شهادة TOMCAT).
- في CUCM 12.0 وما فوق، لديك خيار إستخدام شهادة موقعة ذاتيا من النظام ل Cluster Wide SSO. يستخدم هذا الخيار شهادة ITLRovery بدلا من شهادة TOMCAT:



- SSO لكل عقدة هو الإعداد الافتراضي قبل CUCM 11.5. في التكوين الخاص بكل عقدة، تحتوي كل عقدة على ملف بيانات تعريف خاص بها يلزم إستيراده إلى المعرف نظرا لأنه من المحتمل أن تقوم أي من هذه العقد بإعادة توجيه مستخدم للمصادقة.
- كما يمكنك تمكين SSO ل RTMT في CUCM 11.5. يتم تمكين هذا الأمر بشكل افتراضي، وهو موجود في إدارة Cisco Unified CM > معلمات المؤسسة > إستخدام SSO ل RTMT.

ملاحظة: الملاحظة التي تشير إلى أنه إذا كان وضع SSO عبارة عن نظام المجموعة، يجب أن تكون شهادة Tomcat موقعة من CA متعدد الخوادم خاطئة على 12.0 و 12.5 وقد تم فتح عيب لتصحيحها (معرف تصحيح الأخطاء من Cisco CSCvr49382).

وبصرف النظر عن هذه الخيارات، فإن بقية تكوين SSO موجود على معرف العملية. يمكن أن تختلف خطوات التكوين بشكل كبير بناء على معرف IdP الذي تختاره. تحتوي هذه المستندات على خطوات لتكوين بعض المعرفات الأكثر شيوعا:

- دليل تكوين Microsoft AD FS
- دليل تكوين OKTA
- دليل تكوين PingFederate
- دليل تكوين Microsoft Azure

استكشاف الأخطاء وإصلاحها

البيانات المطلوب تجميعها

لاستكشاف أخطاء مشكلة SSO وإصلاحها، قم بتعيين تعقب SSO على تصحيح الأخطاء. لا يمكن تعيين مستوى سجل SSO على تصحيح الأخطاء عبر واجهة المستخدم الرسومية (GUI). لتعيين مستوى سجل SSO إلى تصحيح الأخطاء، قم بتشغيل هذا الأمر في CLI: set samltrace level debug

ملاحظة: هذا الأمر ليس Cluster wide، لذلك يجب تشغيله على كل عقدة يمكن أن تكون متعلقة بمحاولة تسجيل دخول SSO.

ما إن ثبتت السجل مستوى إلى يضبط، أنتج الإصدار وجمعت هذا معطيات من CUCM:

- سجلات SSO من Cisco
- سجلات Tomcat من Cisco

توجد معظم مشاكل SSO إستثناءات وأخطاء في سجلات SSO ولكن في بعض الظروف، قد يكون سجلات Tomcat مفيدة أيضا.

تحليل المثال

معلومات الجهاز من مختبر TAC

CUCM (وزود الخدمة):

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

Windows Server 2016 (موفر الهوية):

- خدمات إتحاد Active Directory 3.0
- FQDN: WinServer2016.sckiewer.lab

مراجعة السجل ل 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
```

نظرة أكثر قربا على طلب SAML وتأكيده

طلب SAML

تحليل ومعلومات حول طلب 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>
```

تأكيد

تحليل ومعلومات حول إستجابة 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

أوامر CLI المساعدة

- Utils sso disable - يسمح هذا بتعطيل SSO إذا لم يكن يعمل
- تظهر حالة SSO الحالية - توضح هذه الحالة الحالية لـ SSO على العقدة
- يتم تمكين SSO recovery-url - يسمح لك هذا بتعطيل URL الاسترداد
- SSO recovery-url disable - يسمح هذا بأن يمكن الإستعادة URL
- show samltrace level - يعرض هذا مستوى السجل الحالي لسجلات SSO
- تعيين مستوى Samltrace - يتيح لك هذا تعيين مستوى السجل لسجلات SSO. هذا يحتاج أن يكون ثبتت إلى صحح in order to نحن بفعالية تحريت إصدار.

التغيير من ConfirmationConsumerServiceURL إلى ConfirmationConsumerServiceIndex

عند إضافة SSO على مستوى المجموعة في CUCM 11.5، لم تعد CUCM تكتب عنوان URL ConfirmationConsumerService (ACS) في طلب SAML. بدلا من ذلك، يكتب CUCM ConfirmationConsumerServiceIndex. رأيت هذا قصاصة من طلب SAML:

CUCM pre 11.5.1:

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

CUCM 11.5.1 وما فوق:

```
AssertionConsumerServiceIndex="0"
```

في 11.5 أو على، تتوقع CUCM أن يستخدم IDp رقم ACS # من الطلب in order to بحث عن عنوان URL ل ACS من ملف بيانات التعريف الذي تم تحميله أثناء عملية التكوين. تعرض هذه القصاصة لبيانات تعريف CUCM عنوان URL الخاص بمادة النشر (الخاص بالناشر) المرتبط بالفهرس 0:

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

ال يوجد حل بديل لتغيير هذا السلوك ويجب أن يستخدم IdP قيم فهرس ACS بدلا من عنوان URL ل ACS. يمكن العثور على مزيد من المعلومات هنا، معرف تصحيح الأخطاء من Cisco CSCvc56596.

المشكلات الشائعة

يتعذر الوصول إلى إدارة نظام التشغيل أو إستعادة البيانات بعد الكوارث

في CUCM 12.x، تستخدم تطبيقات الويب الخاصة بنظام الإدارة الموحدة لنظام التشغيل

واسترداد البيانات بعد الكوارث من Cisco SSO. إذا فشلت محاولات تسجيل الدخول إلى هذه التطبيقات بخطأ 403 بعد تمكين SSO، فمن المحتمل أن يكون ذلك بسبب عدم قدرة النظام الأساسي ل CUCM على العثور على معرف المستخدم. يحدث هذا لأن هذه التطبيقات لا تشير إلى جدول المستخدم النهائي المستخدم من قبل إدارة CM، والقابلية للخدمة، وإعداد التقارير. ولهذا السبب، لا يوجد معرف المستخدم الذي تمت مصادقة معرف IdP عليه على جانب النظام الأساسي ل CUCM، وبالتالي ترجع CUCM محظور رقم 403. يوضح [هذا المستند](#) كيفية إضافة المستخدمين المناسبين إلى النظام بحيث تستخدم تطبيقات النظام الأساسي SSO بنجاح.

فشل NTP

يعتبر SSO حساس للوقت لأن IDp يقوم بإلحاق "إطار زمني للصلاحية" للتأكيدات. in order to تحقق ما إذا الوقت إصدار في حالتك، أنت يستطيع بحث هذا قسم في ال SSO سجل:

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

إذا وجدت الوقت صالحا؟:خطأ في سجلات SSO الخاصة بك، تحقق من قسم "الشروط" في التأكيد لتحديد الإطار الزمني الذي يجب اعتبار التأكيد صالحا:

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

يمكنك أن ترى في المثال الخاص أن هذا التأكيد صالح فقط من 13:01:03:8917 إلى 14:01:03:8917 على 4/30/2021. في سيناريو الفشل، راجع الوقت الذي تلقى CUCM هذا التأكيد وتحقق من أنه يقع ضمن فترة الصلاحية من التأكيد. إذا كان وقت معالجة CUCM للتأكيد خارج فترة الصلاحية، فهذا هو سبب مشكلتك. تأكد من مزامنة CUCM و IdP مع نفس خادم NTP لأن SSO حساس جدا للوقت.

عبارة سمة غير صالحة

ارجع إلى تحليل التأكيد [هنا](#) وانظر الملاحظة المتعلقة ببيان السمة. تتطلب منتجات الاتصالات الموحدة من Cisco بيان سمة ليتم توفيره بواسطة IDp، ولكن في بعض الأحيان لا يقوم IdP بإرسال واحد. بالنسبة للمرجع، هذه عبارة صالحة عن AttributeStatement:

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

إذا رأيت تأكيدا من IdP، ولكن يتم حذف عبارة السمة، فاعمل مع مورد برنامج IdP الخاص بك وفي idP لا على بناء حالصإلا فلتخي .ةرابعلا هذه رفوت ثيحب ةمزاللا تارييغتلا ءارجإل في بعض السيناريوهات، يمكن إرسال المزيد من المعلومات في هذه العبارة أكثر مما تراه في AttributeValue وقباطي المستخدم فرعملا ىلإ نيعم ةمس مسا كانه مادام .ةصاقلا الباب الامتيازات الصحيحة في قاعدة بيانات CUCM، يكون تسجيل الدخول ناجحا.

شهادة توقيع - AD FS

هذه المشكلة خاصة ب Microsoft AD FS. عندما تكون شهادة التوقيع على AD FS قريبة من انتهاء الصلاحية، يقوم مدير Windows بإنشاء شهادة توقيع جديدة، لكن أترك الشهادة القديمة في مكانها حتى تنتهي صلاحيتها. عندما يحدث ذلك، فإن بيانات AD FS الأولية تحتوي على شهادتي توقيع. رسالة الخطأ التي يمكنك رؤيتها عند محاولة تشغيل إختبار SSO أثناء هذا الإطار الزمني هي، خطأ أثناء معالجة إستجابة SAML.

ملاحظة:خطأ أثناء معالجة إستجابة SAML يمكن أيضا تقديمه لمشكلات أخرى لذلك لا يفترض أن هذه مشكلتك إذا رأيت هذا الخطأ. تأكد من التحقق من سجلات SSO للتحقق.

إذا رأيت هذا الخطأ، فراجع سجلات SSO وابحث عن هذا:

```
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
```

يشير هذا الخطأ إلى أن بيانات تعريف IdP التي تم إستيرادها إلى CUCM تحتوي على شهادة توقيع لا تتطابق مع IdP المستخدم في توقيع SAML هذا. يحدث هذا الخطأ على الأرجح لأن AD FS يحتوي على شهادتي توقيع. عندما تكون الشهادة الأصلية قريبة من انتهاء الصلاحية، يجب أن يقوم AD FS تلقائيا بإنشاء شهادة توقيع جديدة. يجب أن تنتبه إلى موقع بيانات أولية جديد من AD FS، تأكد من أنه يحتوي على شهادة توقيع وتشفير واحدة فقط وقم باستيرادها إلى CUCM. تحتوي المعرفات الأخرى أيضا على شهادات توقيع تحتاج إلى تحديث بحيث يمكن أن يكون موقع مخصص لما لم يستورد ملف البيانات الأولية الجديد الذي يحتوي على الشهادة الجديدة إلى CUCM.

إذا واجهت الأخطاء المذكورة:

- إن كنت تستعمل AD FS، أحلت cisco بق id CSCuj66703
- إذا لم تكن تستخدم AD FS، قم بتجميع ملف بيانات أولية جديد من IdP وقم باستيراده إلى CUCM

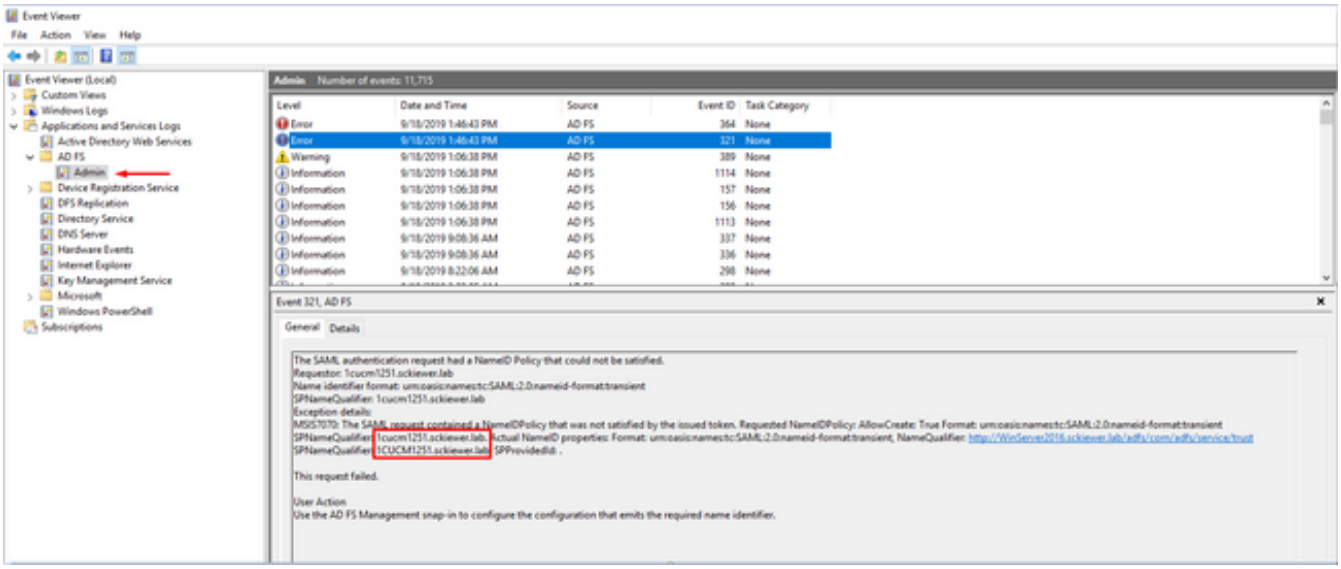
رمز حالة غير صالح في الاستجابة

هذا خطأ شائع في عمليات النشر باستخدام AD FS:

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

وفي جميع الحالات تقريبا، تكون هذه مشكلة تتعلق بقاعدة المطالبة على جانب إدارة الدعم الميداني. الصق القاعدة في Notepad أولا، وقم بإضافة EntityIDs الخاصة بك، ثم الصق القاعدة من Notepad في AD FS. في بعض السيناريوهات، يمكن أن يقوم النسخ/اللصق مباشرة من برنامج الإلكتروني أو المستعرض بحذف بعض علامات الترقيم ويتسبب في حدوث خطأ في بناء الجملة.

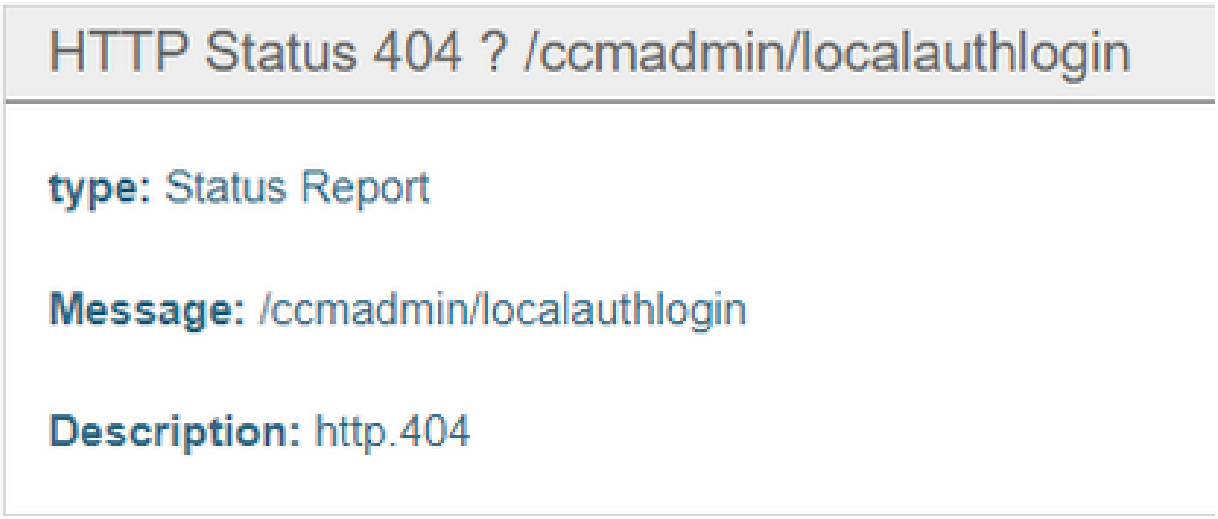
توجد مشكلة أخرى شائعة في قاعدة المطالبة وهي أن رسملة إما IdP أو SP FQDNs لا تطابق EntityID في ملفات بيانات التعريف. تحقق من سجلات "عارض الأحداث" الموجودة على "خادم Windows" لتحديد ما إذا كانت هذه مشكلتك أم لا.



يمكنك أن ترى في الصورة أن NameID المطلوب وه 1cucm1251.sciewer.lab بينما NameID الفعلي وه 1CUCM1251.sckiewer.lab. يجب أن يتطابق NameID المطلوب مع EntityID في ملف بيانات تعريف SP بينما يتم تعيين NameID الفعلي في قاعدة المطالبة. لإصلاح هذه المشكلة، أحتاج إلى تحديث قاعدة المطالبة باستخدام FQDN لحالة أقل ل SP.

عدم تطابق حالة SSO بين CLI و GUI

في بعض الحالات، يمكن أن تظهر حالة sso ووواجهة المستخدم الرسومية معلومات مختلفة فيما يتعلق بما إذا كان SSO ممكنا أو معطل. تعتبر أسهل طريقة لإصلاح هذه المشكلة هي تعطيل SSO وإعادة تمكينه. هناك عدد قليل جدا من الملفات والمراجع التي يتم تحديثها من خلال عملية التمكين، لذلك من غير الممكن محاولة تحديث جميع هذه الملفات يدويا. في معظم الحالات، يمكنك تسجيل الدخول إلى واجهة المستخدم الرسومية (GUI) وتعطيل وإعادة تمكين بدون أي مشاكل، ومع ذلك، من الممكن أن ترى هذا الخطأ عندما تحاول الوصول إلى الناشر عبر عنوان URL للاستعادة أو الارتباط الرئيسي:



أنت يستطيع فحصت ال gui أن يري إن يكون الإستعادة URL خيار وأنت يستطيع أيضا فحصت ال utils حالة إنتاج من ال 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
```

بعد ذلك، تحقق من جدول عقدة العملية. في هذا المثال، يمكنك أن ترى أن SSO معطل في قاعدة البيانات (راجع قيمة tkssomode ل 1cucm1251.sckiewer.lab في أقصى اليمين):

```
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
```

لإصلاح ذلك، قم بتعيين حقل tkssomode في جدول عقدة العملية مرة أخرى إلى 2 بحيث يمكنك تسجيل الدخول عبر عنوان URL للاستعادة:

```
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
```

عند هذه النقطة، اختبر عنوان URL الخاص بالاستعادة وتابع مع تعطيل > إعادة تمكين SSO الذي يؤدي إلى تشغيل CUCM لتحديث جميع المراجع في النظام.

معلومات ذات صلة

- دليل نشر SAML SSO لتطبيقات الاتصالات الموحدة من Cisco، الإصدار 12.5(1)
- نظرة عامة فنية على لغة تمييز تأكيد الأمان (SAML) V2.0
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).