排除Cisco Unified Communications Manager中的SSO故障

目录

简介

本文档介绍如何在Cisco Unified Communications Manager(CUCM)中配置单点登录(SSO)。

先决条件

要求

思科建议您了解以下主题：

- CUCM
- Active Directory联合身份验证服务(ADFS)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- CUCM 11.5.1.13900-52(11.5.1SU2)
- ADFS 2.0。

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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

请参阅在CUCM中配置单点登录。

- https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-version-105/118770-configure-cucm-00.html
- https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/211302-Configure-Single-Sign-On-using-CUCM-and.html

思科统一通信应用11.5(1)版SAML SSO部署指南。

- https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/SAML_SSO_deployment_guide/11_5_1/CUCM_BK_S12EF288_00_saml-sso-deployment-guide--1151.html

SAML RFC 6596。

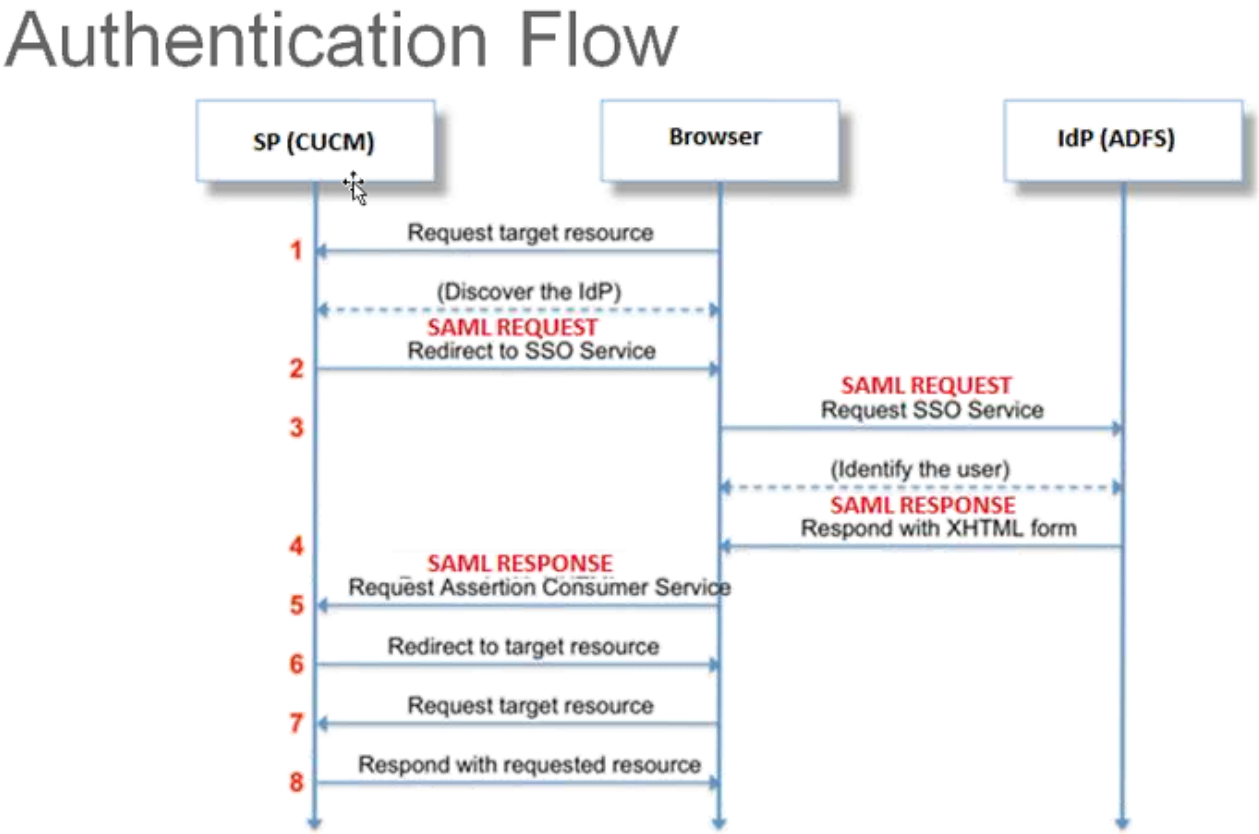
- https://tools.ietf.org/html/rfc6595

验证

当前没有可用于此配置的验证过程。

故障排除

SSO中的登录流



解码SAML响应

在Notepad++中使用插件

安装以下插件：

```
Notepad++ Plugin -> MIME Tools--SAML DECODE

Notepad++ Plugin -> XML Tools -> Pretty Print(XML only - with line breaks)
```

在SSO日志中搜索包含编码响应的字符串“authentication.SAMLAuthenticator - SAML Response is : : ”。

使用此插件或联机SAML解码以获取XML响应。使用已安装的Pretty Print插件可以以可读格式调整响应。

在较新版本的CUCM SAML响应中，XML格式可通过搜索“SPASSUtils.getResponse:got response=<samlp:

响应xmlns:samlp="，然后使用Pretty Print插件进行打印。

使用Fiddler:

此实用程序可用于获取实时流量并对其进行解码。以下是相同指南；https://www.techrepublic.com/blog/software-engineer/using-fiddler-to-debug-http/。

SAML请求：

```
ID="s24c2d07a125028bfffa7757ea85ab39462ae7751f" Version="2.0" IssueInstant="2017-07-
15T11:48:26Z" Destination="https://win-91uhcn8tt3l.emeacucm.com/adfs/ls/" ForceAuthn="false"
IsPassive="false" AssertionConsumerServiceIndex="0">
<saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">cucmsso.emeacucm.com</saml:Issuer>
<samlp:NameIDPolicy xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
SPNameQualifier="cucmsso.emeacucm.com" AllowCreate="true"/>
</samlp:AuthnRequest>
```

SAML响应（未加密）：

```
<samlp:Response ID="_53c5877a-0fff-4420-a929-1e94ce33120a" Version="2.0" IssueInstant="2017-07-
01T16:50:59.105Z"
Destination="https://cucmsso.emeacucm.com:8443/ssosp/saml/SSO/alias/cucmsso.emeacucm.com"
Consent="urn:oasis:names:tc:SAML:2.0:consent:unspecified"
InResponseTo="s24c2d07a125028bfffa7757ea85ab39462ae7751f"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
<Issuer xmlns="urn:oasis:names:tc:SAML:2.0:assertion">http://win-
91uhcn8tt3l.emeacucm.com/adfs/services/trust</Issuer>
<samlp:Status>
<samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
</samlp:Status>
<Assertion ID="_0523022c-1e9e-473d-9914-6a93133ccfc7" IssueInstant="2017-07-01T16:50:59.104Z"
Version="2.0" xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
<Issuer>http://win-91uhcn8tt3l.emeacucm.com/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="#_0523022c-1e9e-473d-9914-6a93133ccfc7">
<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>9OvwrpJVeOQsDBNghwvkLIdnf3bc7aW82qmo7Zdm/Z4=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>VbWcKUwvwiNDhUg5AkdqSzQOmP0qs5OT2VT+u1LivWx7h9U8/plyhK3kJMUuxoG/HXPQJgVQaMOwN
q/Paz7Vg2uGNFigA2AFQsKgGo9hAA4etfucIQlMmkeVg+ocvGY+8IzaNVfaUXSU5laN6zriTArxXwxCK0+thgRgQ8/46vm91
Skq2Fa5Wt5uRPJ3F4eZPOEPdtKxOmUuHi3Q2pXTw4ywZ/y89xPfSixNQEmr10hpPAdyfPsIFGdNJJwWJV4WjNmfcAqClzaG8
pB74e5EawLmwrfV3/i8QfR1DyU5yCCpxj02rgE6Wi/Ew/X/l6qSCzOZEpl7D8LwAn74KijO+Q==</ds:SignatureValue>
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>MIIC5DCCAcygAwIBAgIQZLLskb6vppxCiYP8xOahQDANBgkqhkiG9w0BAQsFADAuMSwwKgYDVQQD
EyNBREZTIFNpZ25pbmcgLSBXSU4ySzEyLnJrb3R1bGFrLmxhYjAeFw0xNTA2MjIxOTE2NDRaFw0xNjA2MjExOTE2NDRaMC4x
LDAqBgNVBAMTI0FERlMgU2lnbmluZyAtIFdJTjJLMTIucmtvdHVsYWsubGFiMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEApEe09jnZXEcEC7s1VJ7fMXAHPXj7jgOOcs9/Lzxrx4c68tePGItrEYnzW9vLe0Dj8OJET/Rd6LsKvuMQHfcGYqA+
XugZyHBrpc18wlhSmMfvfa0jN0Qc0lf+a3j72xfI9+hLtsqSPSnMp9qby3qSiQutP3/ZyXRN/TnzYDEmzur2MA+GP7vdeVOF
XlpENrRfaINzc8INqGRJ+1jZrm+vLFvX7YwIL6aOpmjaxcPoxDcjgEGMYO/TaoP3eXutX4FuJV5R9oAvbqD2F+73XrvP4e/w
Hi5aNrHrgiCnuBJTIxHwRGSoichdpZlvSB15v8DFaQSVAiEMPj1vP/4rMkacNQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQA5
uJZI0K1Xa40H3s5MAo1SG00bnn6+sG14eGIBe7BugZMw/FTgKd3VRsmlVuUWCabO9EgyfgdI1nYZCciyFhts4W9Y4BgTH0j4
+VnEWiQg7dMqp2M5lykZWPS6vV2uD010sX5V0avyYi3Qr88vISCtniIZpl24c3TqTn/5j+H7LLRVI/ZU38Oa17wuSNPyed6/
N4BfWhhCRZAdJgijapRG+JIBeoA1vNqN7bgFQMe3wJzSlLkTIoERWYgJGBciMPS3H9nkQlP2tGvmn0uwacWPglWR/LJG3VYo
isFm/oliNUF1DONK7QYiDzIE+Ym+vzYgIDS7MT+ZQ3XwHg0Jxtr8</ds:X509Certificate>
</ds:X509Data>
</KeyInfo>
</ds:Signature>
<Subject>
<NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient" NameQualifier="http:///win-
91uhcn8tt3l.emeacucm.com/com/adfs/services/trust"
SPNameQualifier="cucmsso.emeacucm.com">CHANDMIS\chandmis</NameID>
<SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
<SubjectConfirmationData InResponseTo="s24c2d07a125028bfffa7757ea85ab39462ae7751f"
NotOnOrAfter="2017-07-01T16:55:59.105Z"
Recipient="https://cucmsso.emeacucm.com:8443/ssosp/saml/SSO/alias/cucmsso.emeacucm.com" />
</SubjectConfirmation>
</Subject>
<Conditions NotBefore="2017-07-01T16:50:59.102Z" NotOnOrAfter="2017-07-01T17:50:59.102Z">
<AudienceRestriction>
<Audience>ccucmsso.emeacucm.com</Audience>
</AudienceRestriction>
</Conditions>
<AttributeStatement>
<Attribute Name="uid">
<AttributeValue>chandmis</AttributeValue>
</Attribute>
</AttributeStatement>
<AuthnStatement AuthnInstant="2017-07-01T16:50:59.052Z" SessionIndex="_0523022c-1e9e-473d-9914-
6a93133ccfc7">
<AuthnContext>
<AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</AuthnCo
ntextClassRef>
</AuthnContext>
</AuthnStatement>
</Assertion>

</samlp：响应>

```
Version="2.0"  :- The version of SAML being used.

InResponseTo="s24c2d07a125028bfffa7757ea85ab39462ae7751f" :- The id for SAML Request to which
this reponse corresponds to

samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success :- Status Code of SAML
reponse. In this case it is Success.

<Issuer>http://win-91uhcn8tt3l.emeacucm.com/adfs/services/trust</Issuer> :- IdP FQDN

SPNameQualifier="cucmsso.emeacucm.com" :- Service Provider(CUCM) FQDN

Conditions NotBefore="2017-07-01T16:50:59.102Z" NotOnOrAfter="2017-07-01T17:50:59.102Z :- Time
range for which the session will be valid.

<AttributeValue>chandmis</AttributeValue> :- UserID entered during the login
```

如果SAML响应已加密，则您将无法看到完整信息，必须禁用Intrusion Detection & Prevention(IDP)上的加密才能查看完整响应。用于加密的证书详细信息位于SAML响应的“ds:X509IssuerSerial”下。

日志和CLI命令

CLI命令：

utils sso disable

此命令禁用两个基于（OpenAM SSO或SAML SSO）的身份验证。此命令列出为其启用SSO的Web应用。出现提示时，输入**Yes**以禁用指定应用的SSO。如果在集群中，则必须在两个节点上运行此命令。SSO也可以从图形用户界面(GUI)中禁用，并在Cisco Unity Connection Administration中的特定SSO下选择**Disable**按钮。

命令语法
utils sso disable

utils sso status

此命令显示SAML SSO的状态和配置参数。它有助于逐个验证每个节点上的SSO状态（启用或禁用）。

命令语法
utils sso status

utils sso enable

此命令返回一条信息性文本消息，提示管理员仅能从GUI启用SSO功能。无法使用此命令启用基于OpenAM的SSO和基于SAML的SSO。

命令语法

utils sso enable

utils sso recovery-url enable

此命令启用恢复URL SSO模式。它还验证此URL是否成功运行。如果在集群中，则必须在两个节点上运行此命令。

命令语法
utils sso recovery-url enable

utils sso recovery-url disable

此命令在该节点上禁用恢复URL SSO模式。如果在集群中，则必须在两个节点上运行此命令。

命令语法
utils sso recovery-url disable

set samltrace level <trace-level>

此命令启用特定跟踪和跟踪级别，这些跟踪和跟踪级别可以找到任何错误、调试、信息、警告或致命错误。如果在集群中，则必须在两个节点上运行此命令。

命令语法
set samltrace level <trace-level>

show samltrace level

此命令显示SAML SSO的日志级别集。如果在集群中，则必须在两个节点上运行此命令。

命令语法
show samltrace level

跟踪以查看故障排除时间：

默认情况下，SSO日志未设置为详细级别。

首先运行命令set **samltrace level debug**，以设置要调试的日志级别，重现问题并收集这组日志。

从RTMT:

Cisco Tomcat

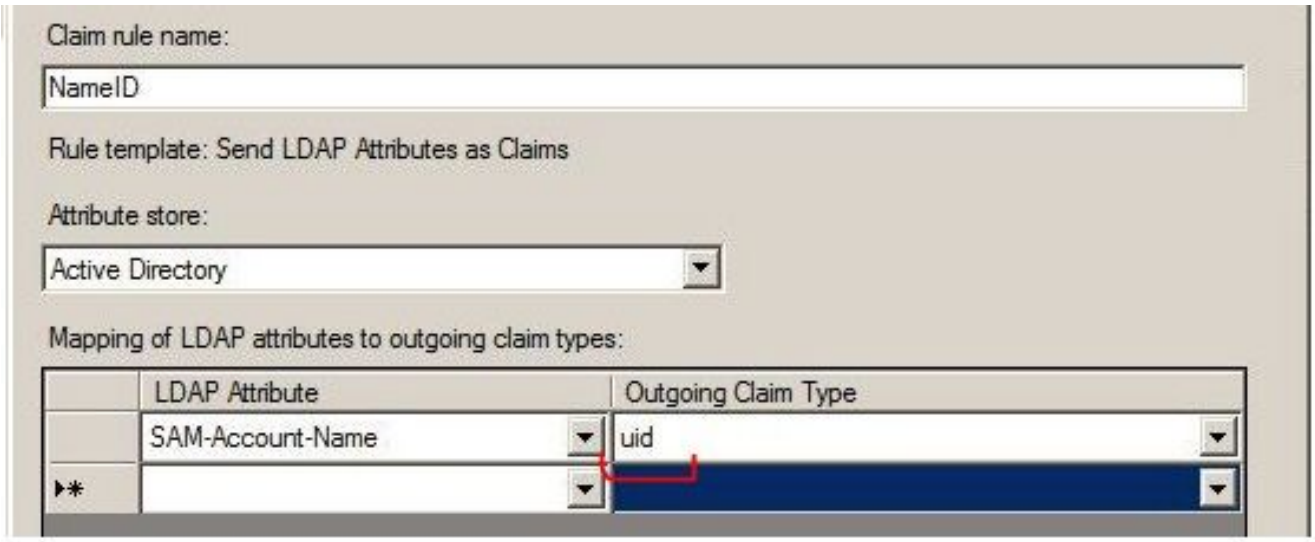
Cisco Tomcat安全

思科SSO

常见问题

唯一标识符(UID)的值不正确：

它应该是UID，如果不是，CUCM无法理解。



领款申请规则不正确或NameID策略错误：

在此场景中，很可能没有提示用户名和密码。

SAML响应中将不存在任何有效断言，状态代码将如下：

```
<samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:InvalidNameIDPolicy"/>
```

验证在IDP端正确定义了索赔规则。

领款申请规则中定义的大小写/名称差异：

声明规则中的CUCM FQDN应与实际服务器上指定的CUCM FQDN完全匹配。

通过在CUCM的CLI上运行**show network cluster/show network etho details**命令，可以将IDP的元数据xml文件中的条目与CUCM上的条目进行比较。

错误时间：

CUCM和IDP之间的NTP的差异大于《部署指南》中允许的3秒。

断言签名者不受信任：

在IDP和CUCM（服务提供商）之间交换元数据时。

交换证书，如果证书已撤销，则应再次交换元数据。

DNS配置错误/无配置

DNS是SSO工作的主要要求。运行**show network etho detail**,**在CLI上使用diagnose test**以验证

DNS/Domain是否配置正确。

已知缺陷

CSCuj66703

ADFS签名证书续约，并将两个签名证书添加到IDP响应返回CUCM(SP)，因此您会遇到缺陷。您必须删除不需要的签名证书

CSCvf63462

从CCM Admin导航至SAML SSO页面时，系统会提示“The following servers failed during attempt to get SSO Status”，后跟节点名称。

CSCvf96778

在CCMAdmin//System/Sever中将CUCM服务器定义为IP地址时，基于CTI的SSO失败。