排除故障在Cisco Unified Communications Manager的SSO

目录

简介

本文描述如何配置单一登录(SSO)在Cisco Unified Communications Manager (CUCM)。

先决条件

要求

思科建议您有主题的知识：

- CUCM
- 活动目录联邦服务(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

参考单个符号的配置在CUCM。

- 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

SAML Cisco Unified通信应用的SSO部署指南，版本11.5(1)。

- 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。

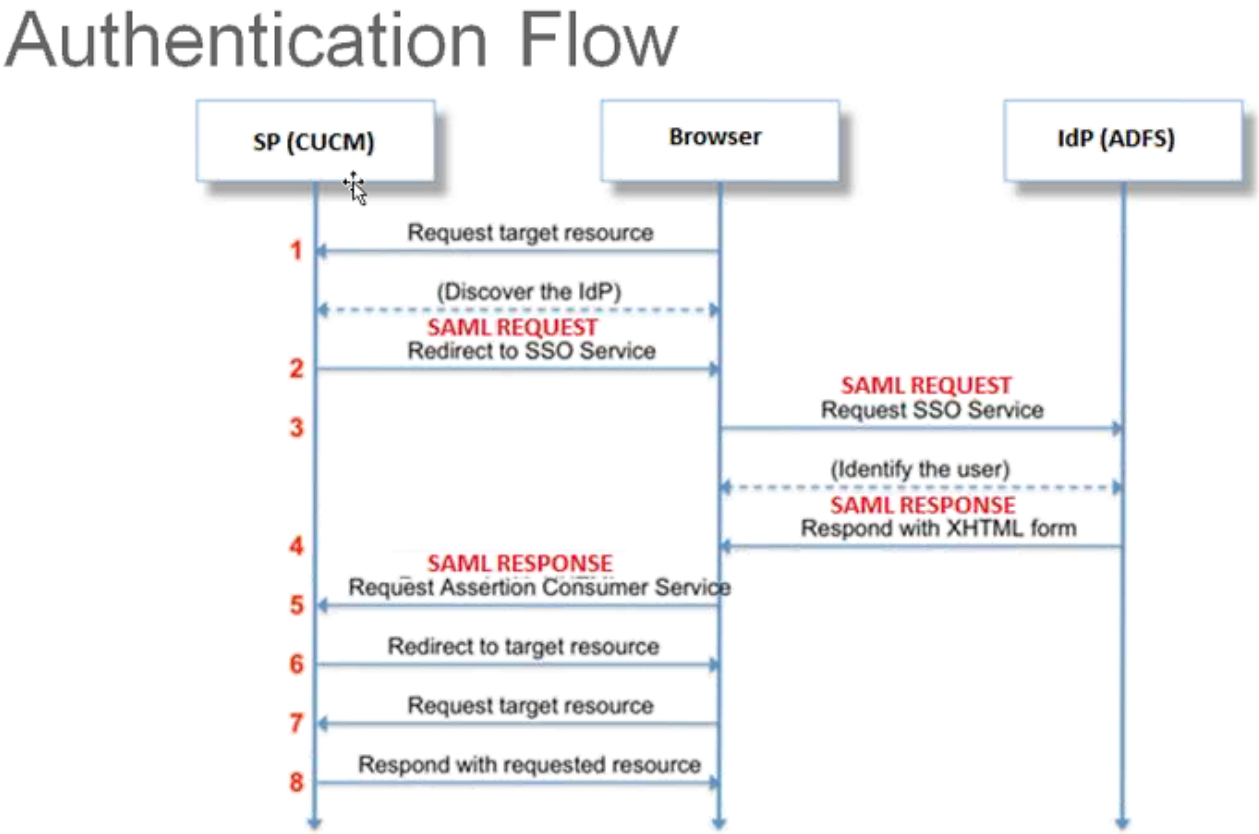
- https://tools.ietf.org/html/rfc6595

验证

当前没有可用于此配置的验证过程。

故障排除

登陆在SSO的流



解码SAML答复

使用在Notepad++的插件

安装这些插件：

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

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

在SSO日志请搜索字符串“authentication.SAMLAuthenticator - SAML答复是： ：”包含编码的答复。

请使用此插件或联机SAML解码为了得到XML答复。答复在与插件使用安装的完美印出的一种可读的格式可以调节。

在CUCM SAML答复中新版本在可以通过搜索“SPACSUtils.getResponse找到的XML格式：获得的response=<samlp ：

答复xmlns ：samlp= “然后打印与插件的使用完美印出。

使用提琴手：

此工具可以用于获得实时数据流和解码它。这是同样的指南
; 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答复(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 : Response>

```
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
```

万一SAML答复然后加密您不能发现完整信息并且必须禁用在入侵检测&预防(IDP)的加密发现完整答复。用于加密的证书详细信息是在“ds:X509IssuerSerial” SAML答复下。

日志和CLI命令

CLI命令：

使用情况sso禁用

此命令禁用两(OpenAM SSO或SAML SSO)基于验证。此命令一览表SSO启用的Web应用程序。输入**是，**当提示为了禁用指定的应用程序的SSO。您必须运行此on命令两节点，如果在集群。SSO能从图形用户界面(GUI)也禁用和选择**禁用**按钮，在Cisco Unity Connection管理的特定SSO下。

命令语法
使用情况sso禁用

使用情况sso状态

此命令显示SAML SSO状态和配置参数。它帮助验证SSO状态，启用或禁用的，在每个节点单个。

命令语法
使用情况sso状态

使用情况sso enable (event)

此命令返回提示的一个信息性文本消息管理员能启用SSO仅功能从GUI。OpenAM根据SSO，并且SAML基于SSO不可能用此命令启用。

命令语法
使用情况sso enable (event)

使用情况sso恢复URL enable (event)

此命令启动恢复URL SSO模式。它也验证此URL顺利地运作。您必须运行此on命令两节点，如果在集群。

命令语法
使用情况sso恢复URL enable (event)

使用情况sso恢复URL禁用

此命令禁用在该节点的恢复URL SSO模式。您必须运行此on命令两节点，如果在集群。

命令语法
使用情况sso恢复URL禁用

设置samltrace级别<trace-level>

此命令启用能找出所有错误、调试、信息，警告或者致命的特定跟踪和跟踪级别。您必须运行此on命令两节点，如果在集群。

命令语法
设置samltrace级别<trace-level>

显示级的samltrace

此命令显示为SAML SSO设置的日志级别。您必须运行此on命令两节点，如果在集群。

命令语法
显示级的samltrace

查找的跟踪在时排除故障：

默认情况下SSO日志没有设置为详细的级别。

首先运行set命令**samltrace级别调试**为了设置日志成水平调试，再生产问题，并且这些设置日志的收集。

从RTMT ：

Cisco Tomcat

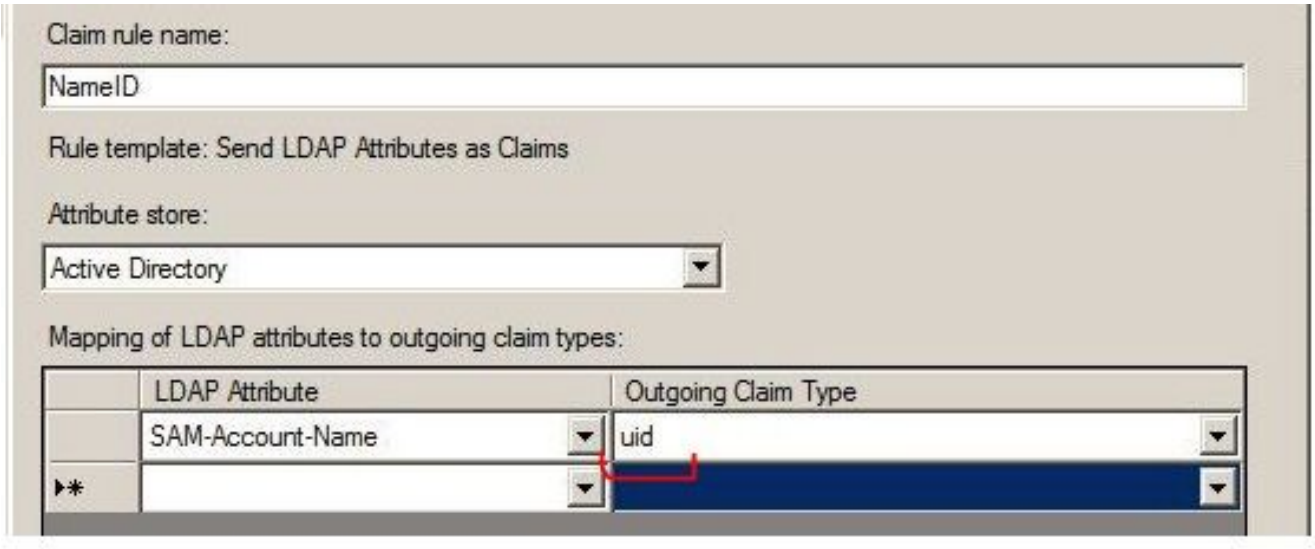
思科Tomcat安全

思科SSO

常见问题

唯一Indentifier的(UID)不正确的值：

它应该正确地是UID，并且，如果它不是实际情形， CUCM无法了解那。



不正确声明规则或错误的NameID策略：

很可能用户名和密码不是及时在此方案。

将没有在SAML答复的所有有效断言，并且状态码类似：

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

验证声明规则正确地定义在IDP侧。

差异，万一/在声明规则定义的名称：

在声明规则的CUCM FQDN应该完全地匹配与在实际服务器指定的那个。

您能通过运行**show network集群/show network etho详细信息**CUCM on命令CLI比较在IDP元数据xml文件的条目与那个的在CUCM。

不正确的时间：

在CUCM和IDP之间的NTP比允许的3秒有一差异极大在部署指南。

断言签署人没有委托：

在元数据的交换时在IDP和CUCM (服务提供商)之间的。

证书交换，并且，如果有执行的证书的任何撤销，应该再交换元数据。

DNS Misconfiguration/No配置

DNS是SSO的主要需求能工作。运行**show network etho详细信息**，**使用情况诊断**在CLI的**测验**为了验证DNS/Domain正确地配置。

已知缺陷

CSCuj66703

ADFS签署的证书更新并且添加两签署的certs到IDP答复回到CUCM (SP)因而造成您遇到缺陷。您必须删除没有要求的签署的证书

CSCvf63462

当您导航对从CCM Admin时的SAML SSO页您用“在尝试失败的以下服务器提示得到SSO状态期间”跟随由节点名。

CSCvf96778

CTI基于SSO发生故障，当定义CUCM服务器作为在CCMAdmin//System/Sever的IP地址。