Cisco Unified Communications Manager中的SSO故障排除

目錄

簡介

本文說明如何在Cisco Unified Communications Manager(CUCM)中配置單一登入(SSO)。

必要條件

需求

思科建議您瞭解以下主題：

- CUCM
- Active Directory聯合身份驗證服務(ADFS)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

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

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

設定

請參閱CUCM中的單點登入配置。

- 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

思科統一通訊應用SAML 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。

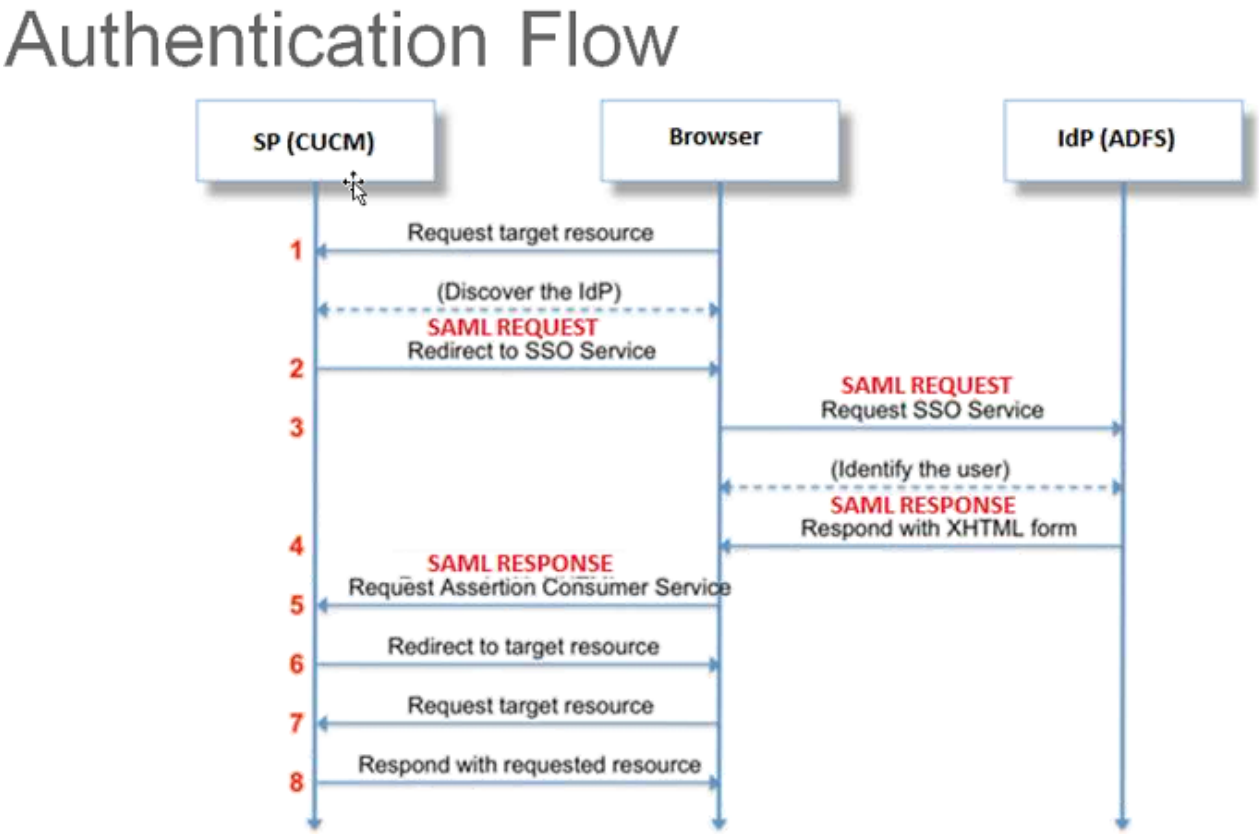
- https://tools.ietf.org/html/rfc6595

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

SSO中的登入流



解碼SAML響應

在記事本中使用外掛++

安裝以下外掛：

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

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

在SSO日誌中，搜尋包含編碼響應的字串「authentication.SAMLAuthenticator - SAML Response is：：」。

使用此外掛或聯機SAML解碼以獲取XML響應。使用安裝的Pretty Print外掛可以以一種可讀的格式調整響應。

在較新版本的CUCM SAML中，響應採用XML格式，可通過搜尋「SPACSUtils.getResponse:獲取響應=<samlp:

響應xmlns:samlp="然後使用Pretty Print外掛進行列印。

使用Fiddler:

該實用程式可用於獲取即時流量並將其解碼。以下是https://www.techrepublic.com/blog/software-engineer/using-fiddler-to-debug-http/的指南。

SAML請求：

```
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響應（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：響應>

```
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響應已加密，您將無法檢視完整資訊，必須禁用入侵檢測和防禦(IDP)上的加密才能檢視完整響應。用於加密的證書詳細資訊位於SAML響應的「ds:X509IssuerSerial」下。

日誌和CLI命令

CLI命令：

utils sso disable

此命令禁用基於兩者（OpenAM SSO或SAML SSO）的身份驗證。此命令列出啟用了SSO的Web應用程式。出現提示時輸入**Yes**，以便為指定的應用程式禁用SSO。如果在群集中，必須在兩個節點上運行此命令。也可以通過圖形使用者介面(GUI)禁用SSO，然後在Cisco Unity Connection管理中的特定SSO下選擇**Disable**按鈕。

指令語法
utils sso disable

utils sso狀態

此命令顯示SAML SSO的狀態和配置引數。它有助於分別驗證每個節點上的SSO狀態（已啟用或已禁用）。

指令語法
utils sso狀態

utils sso enable

此命令返回一條資訊性文本消息，提示管理員只能從GUI啟用SSO功能。無法使用此命令同時啟用基於OpenAM的SSO和基於SAML的SSO。

指令語法
utils sso enable

utils sso recovery-url enable

此命令啟用恢復URL SSO模式。也會驗證此URL是否成功工作。如果在群集中，必須在兩個節點上運行此命令。

指令語法
utils sso recovery-url enable

utils sso recovery-url disable

此命令禁用該節點上的恢復URL SSO模式。如果在群集中，必須在兩個節點上運行此命令。

命令語法
utils sso recovery-url disable

set samltrace level <trace-level>

此命令啟用可定位任何錯誤、調試、資訊、警告或致命的特定跟蹤和跟蹤級別。如果在群集中，必須在兩個節點上運行此命令。

命令語法
set samltrace level <trace-level>

show samltrace level

此命令顯示SAML SSO的日誌級別集。如果在群集中，必須在兩個節點上運行此命令。

命令語法
show samltrace level

跟蹤以檢視故障排除時間：

預設情況下，SSO日誌未設定為詳細級別。

首先運行命令**set samltrace level debug** 以將日誌級別設定為調試、重現問題並收集這些日誌。

在RTMT上：

Cisco Tomcat

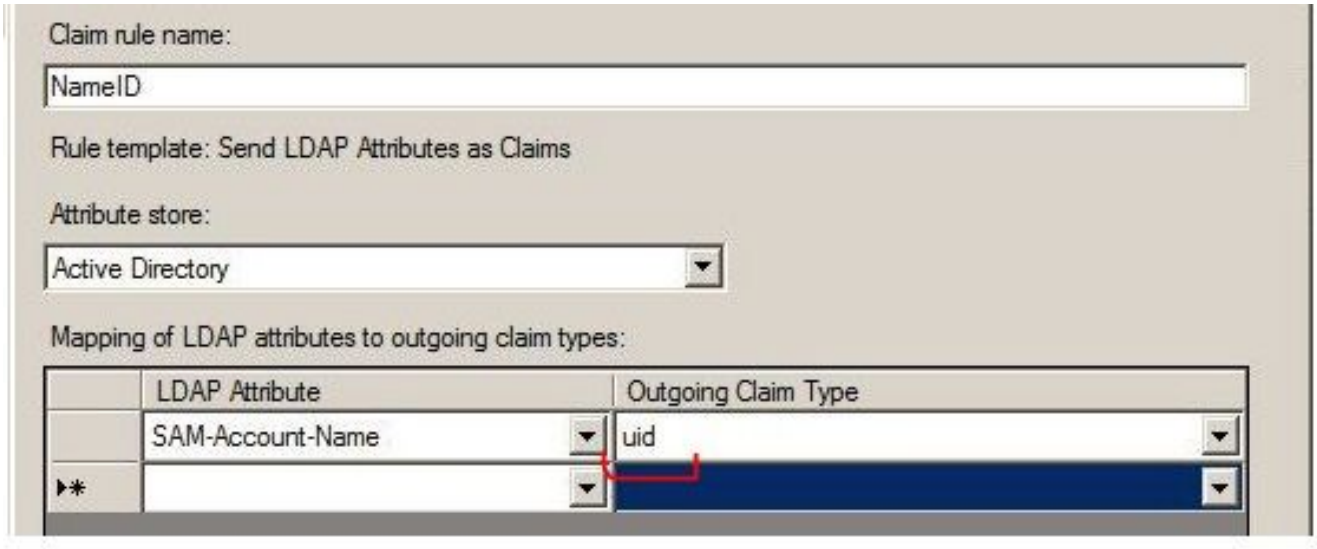
Cisco Tomcat安全

Cisco SSO

常見問題

唯一識別符號(UID)的值不正確：

它應該正好是UID，如果不是，CUCM無法理解這一點。



宣告規則不正確或NameID策略錯誤：

在此案例中，很可能沒有提示輸入使用者名稱和密碼。

SAML響應中沒有任何有效的斷言，狀態代碼將如下所示：

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

驗證在IDP端是否正確定義了宣告規則。

索賠規則中定義的案件/名稱差異：

宣告規則中的CUCM FQDN應與實際伺服器上指定的規則完全匹配。

通過在CUCM的CLI上運行**show network cluster/show network etho details**命令，可以將IDP的後設資料xml檔案中的條目與CUCM上的條目進行比較。

時間不正確：

CUCM和IDP之間的NTP差異大於《部署指南》中允許的3秒。

Assertion Signer Not Trusted:

在IDP和CUCM（服務提供商）之間交換後設資料時。

交換證書，如果證書被吊銷，應再次交換後設資料。

DNS配置錯誤/無配置

DNS是SSO工作的主要要求。運行**show network ethoo detail**,**utils diagnostic test**在CLI上驗證DNS/域是否正確配置。

已知瑕疵

CSCuj66703

ADFS簽名證書會續訂，並將兩個簽名證書新增到IDP響應返回到CUCM(SP)，因此會導致您運行缺陷。您必須刪除不需要的簽名證書

CSCvf63462

當您從CCM Admin導航到SAML SSO頁面時，系統提示您輸入「以下伺服器在嘗試獲取SSO狀態時失敗」，後跟節點名稱。

CSCvf96778

在CCMAdmin//System/Server中將CUCM伺服器定義為IP地址時，基於CTI的SSO失敗。