Cisco Unified Communications Manager の SSO を解決して下さい

目次

概要

この資料に Cisco Unified Communications Manager （ CUCM ）の単一 サインオン（ SSO ）を設定する方法を記述されています。

前提条件

要件

Cisco はトピックのナレッジがあることを推奨します:

- CUCM
- Active Directory フェデレーション サービス (ADFS)

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

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

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

設定

CUCM の単一 サインの設定を参照して下さい。

- 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

Cisco Unified Communications アプリケーション用の SAML SSO 配置ガイド、リリース 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。

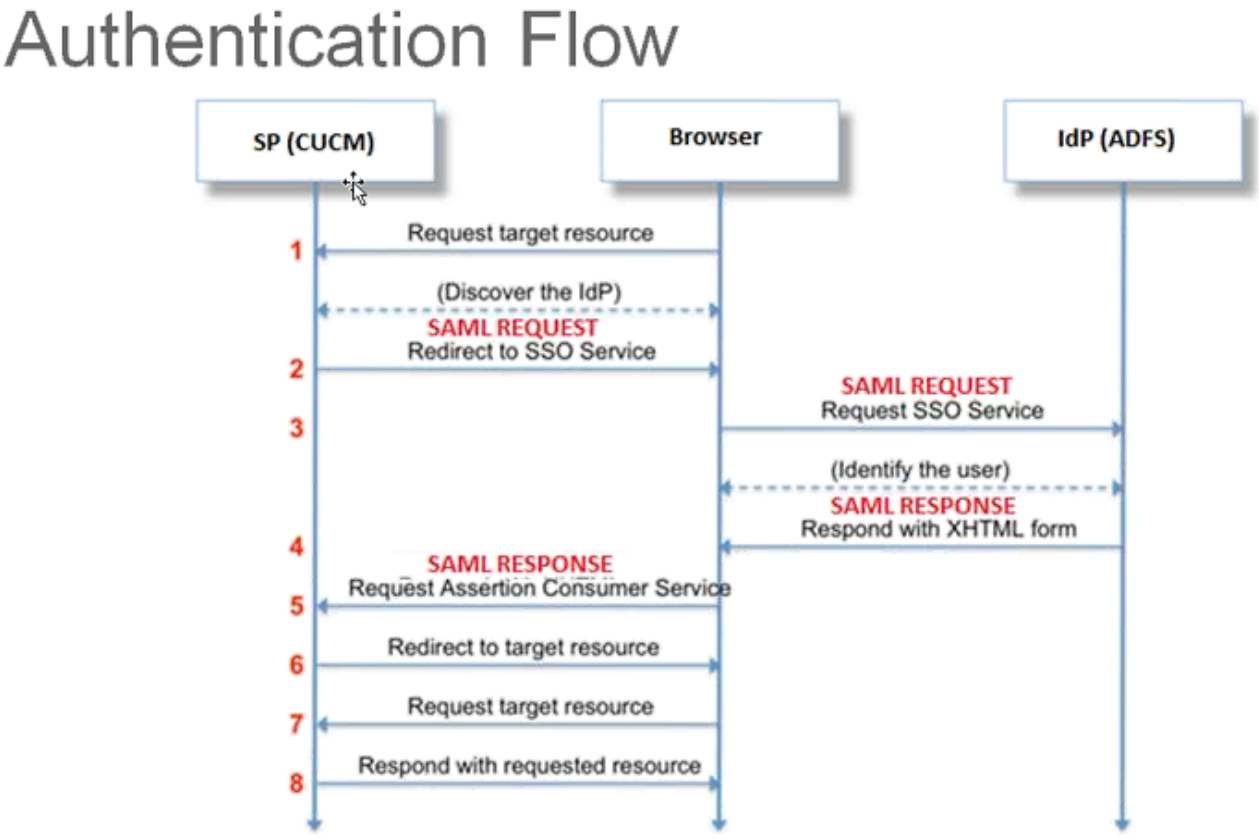
- https://tools.ietf.org/html/rfc6595

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

SSO のフローをログインして下さい



SAML デコード応答

Notepad++ のプラグインの使用

これらのプラグインをインストールして下さい:

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

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

SSO ログでストリング「authentication.SAMLAuthenticator を- SAML 応答次のとおりです捜して下さい:: 」符号化された応答が含まれている。

XML 応答があるためにこのプラグインかオンライン SAML デコードを使用して下さい。 応答は使用インストール済み Pretty プリント プラグインの可読フォーマットで調節することができます。

CUCM SAML 応答の新しいバージョンで「SPACSUtils.getResponse の検索によって検索することができる XML 形式にあります: 得られた response=<samlp:

応答 xmlns: samlp= は「Pretty プリント プラグインの使用とそれから印刷し。

使用バイオリン弾き:

このユーティリティがリアルタイム転送を得、デコードするのに使用することができます。 同じのためのガイドはここにあります; https://www.techrepublic.com/blog/software-engineer/using-fiddler-to-debug-http/。

SAML 要求:

```
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 応答 (非暗号化) :

```
<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
```

SAML 応答がそれから暗号化されれば完全情報を見られますし、完全な応答が表示されるために侵入検知及び防止（IDP）の暗号化を無効に しなければならないのを。 暗号化に使用する証明書の詳細は SAML 応答の「ds:X509IssuerSerial の下に」あります。

ログおよび CLI コマンド

CLI コマンド:

utils sso ディセーブル

このコマンドは両方（OpenAM SSO か SAML SSO）ベースの認証を無効に します。 このコマンド リスト SSO が有効に なる Webアプリケーション。 指定されたアプリケーションのための SSO を無効に するためにプロンプト表示された場合**はい**入力して下さい。 クラスタで両方のノードのこのコマンドを実行して下さい。 SSO はまたグラフィカル ユーザ インターフェイス（GUI）から無効に なり、Cisco Unity Connection 管理の特定の SSO の下で **Disable ボタンを**、選択できます。

コマンドの構文
utils sso ディセーブル

utils sso ステータス

このコマンドは SAML SSO のステータスおよびコンフィギュレーションパラメータを表示するものです。 それは SSO ステータスの、各ノードのイネーブルまたはディセーブル、それぞれ確認を助けます。

コマンドの構文
utils sso ステータス

utils sso イネーブル

このコマンドは管理者は GUI からのだけ SSO 機能を有効に することができることプロンプト表示する情報テキスト メッセージを返します。 OpenAM は両方このコマンドで SSO および SAML によって基づいた SSO を有効に なることができません基づかせていました。

コマンドの構文
utils sso イネーブル

utils sso リカバリ URL イネーブル

このコマンドはリカバリ URL SSO モードを有効に します。 この URL が正常にはたらくことをまた確認します。 クラスタで両方のノードのこのコマンドを実行して下さい。

コマンドの構文
utils sso リカバリ URL イネーブル

utils sso リカバリ URL ディセーブル

このコマンドはそのノードのリカバリ URL SSO モードを無効に します。 クラスタで両方のノードのこのコマンドを実行して下さい。

コマンド構文
utils sso リカバリ URL ディセーブル

samltrace 水平な <trace-level> を設定 して下さい

このコマンドはエラー、デバッグ、情報、警告または致命的見つけることができるトレース レベルおよび特定のトレースを有効にします。 クラスタで両方のノードのこのコマンドを実行して下さい。

コマンド構文
samltrace 水平な <trace-level> を設定 して下さい

水平な samltrace を示して下さい

このコマンドは SAML SSO のための口グ水平なセットを表示するものです。 クラスタで両方のノードのこのコマンドを実行して下さい。

コマンド構文
水平な samltrace を示して下さい

の時に検知 するトレースは解決します:

SSO ログは詳しいレベルにデフォルトで設定 されません。

封切りはデバッグするためにコマンドによって**設定 される samltrace レベル デバッグ** ログを設定 するために水平になりましたり問題および収集をログのこれらのセット 再現 します。

RTMT から:

Cisco Tomcat

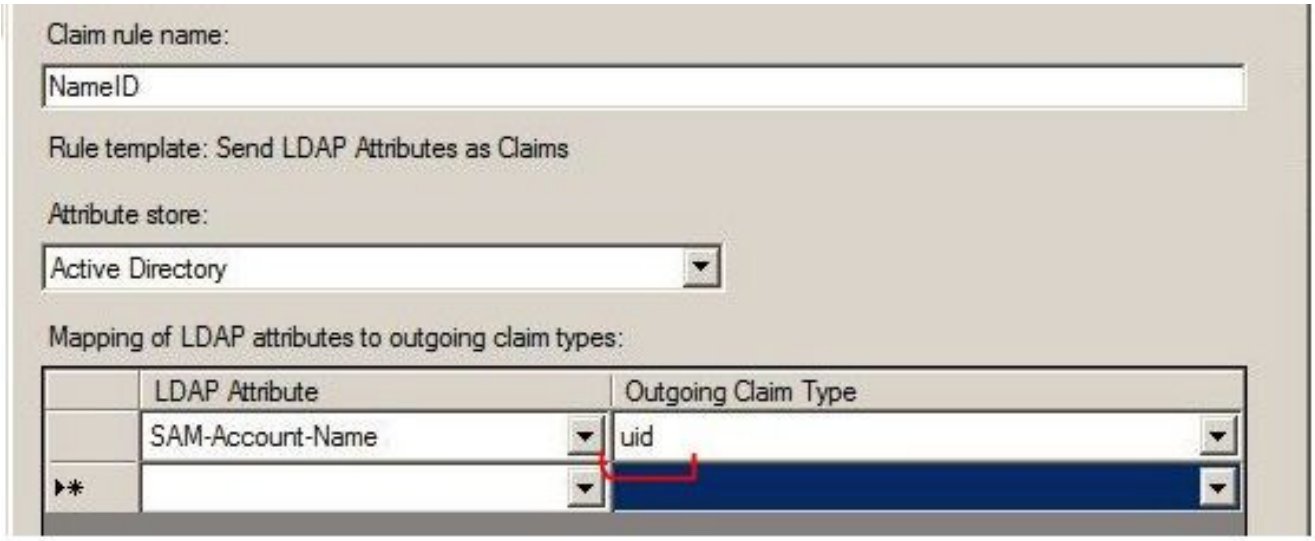
Cisco Tomcat セキュリティ

Cisco SSO

一般的な問題

ユニークな Indentifier （ UID ）の不正確な値:

それは丁度 UID であるはずで、事実でなければ、CUCM はそれを理解することができません。



不正確なクレーム ルールか NameID 間違ったポリシー:

たぶんユーザ名 および パスワードはこのシナリオで敏速ではないです。

SAML 応答に有効なアサーションがないし、ステータス スコードはのようにあります:

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

クレーム ルールが IDP 側で正確に定義されることを確認して下さい。

/名前クレーム ルールで定義される違い:

クレーム ルールの CUCM FQDN は実際のサーバで規定 されるものと完全に一致する必要があります。

メタデータのエントリを比較できます**ネットワークはクラスタ/ネットワーク etho 詳細に** CUCM の CLI のコマンドを**示すことを示す**実行による CUCM のものの IDP の XML ファイルが。

不正確な時間:

CUCM と IDP 間の NTP に配置ガイドで認められる 3 秒より大きい違いがあります。

信頼されないアサーション署名者:

IDP と CUCM （ サービス プロバイダー ）間のメタデータの交換の時。

証明書は交換され、できている証明書の取り消しがあればメタデータは再度交換する必要があります。

DNS Misconfiguration/No 設定

DNS ははたらく SSO のための第一の必要条件です。 **示しますネットワーク etho 詳細を**、**utils** DNS/Domain が正しく設定されることを確認するために**診断します** CLI の**テストを**実行して下さい。

既知の障害

CSCuj66703

ADFS 署名証明書は CUCM （ SP ）に戻って IDP 応答に 2 つの署名 certs をこうして欠陥に動作するために引き起こします更新し、追加します。 必要とならない署名証明書を削除しなければなりません

CSCvf63462

CCM Admin からの SAML SSO ページにナビゲート するとき SSO ステータス」をノードネームに先行させていて調べる試みの間に「次のサーバによって失敗しましたプロンプト表示されます。

CSCvf96778

CTI によって基づく SSO は CUCM サーバを CCMAdmin//System/Sever の IP アドレスと定義すると失敗します。