ADFS/IdS故障排除和常見問題

目錄

簡介 必要條件 需求 採用元件 背景資訊 可在調試過程中方便使用的應用程式和日誌 包含調試選項的流程圖 Cisco IdS的Authcode請求處理 在此過程中遇到的常見錯誤 1.未完成客戶註冊 2.使用者使用IP地址/備用主機名訪問應用程式 通過Cisco IdS啟動SAML請求 在此過程中遇到的常見錯誤 1.未將AD FS後設資料新增到思科IdS AD FS的SAML請求處理 在此過程中遇到的常見錯誤 1. AD FS沒有最新的Cisco IdS SAML證書。 由AD FS傳送的SAML響應 在此過程中遇到的常見錯誤 1. AD FS中未啟用表單身份驗證 Cisco IdS的SAML響應處理 在此過程中遇到的常見錯誤 1. Cisco IdS中的AD FS證書不是最新的。 2. Cisco IdS和AD FS時鐘不同步。 3. AD FS中的錯誤簽名演算法(SHA256與SHA1) 4.傳出宣告規則配置不正確 5.聯合AD FS中的傳出宣告規則配置不正確 6.未正確配置自定義宣告規則 7.對AD FS的請求過多。 8. AD FS未配置為對斷言和消息進行簽名。 相關資訊

簡介

思科身份服務(IdS)和Active Directory聯合身份驗證服務(AD FS)之間通過瀏覽器進行的安全宣告標 籖語言(SAML)互動是單點登入(SSO)登入流程的核心。本文檔將幫助您調試與Cisco IdS和AD FS中 的配置相關的問題,以及解決這些問題的建議操作。

Cisco IdS部署模式

產品 部署

UCCX 共住者 PCCE 與CUIC(思科統一情報中心)和LD(即時資料)共存 UCCE 與CUIC和LD共駐以進行2k部署。 獨立式,適用於4k和12k部署。

必要條件

需求

思科建議您瞭解以下主題:

- Cisco Unified Contact Center Express(UCCX)版本11.5或Cisco Unified Contact Center Enterprise版本11.5或Packaged Contact Center Enterprise(PCCE)版本11.5(如果適用)。
- Microsoft Active Directory Windows Server上安裝的AD
- IdP(身份提供程式) Active Directory聯合服務(AD FS)版本2.0/3.0

採用元件

本文件所述內容不限於特定軟體和硬體版本。

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。

背景資訊

在Cisco IdS和AD FS之間建立信任關係後(請參閱此處瞭解詳細資訊,常見於UCCX和UCCE),管理 員應運行Identity Service Management的「設定」頁中的「測試SSO設定」,以確保Cisco IdS和 AD FS之間的配置正常工作。如果測試失敗,請使用本指南中提供的適當應用程式和建議來解決問 題。

可在調試過程中方便使用的應用程式和日誌

應用程式/日誌 詳細資料

Cisco IdS日誌 Cisco IdS記錄器將記錄Cisco IdS中發生的任何錯誤。

Fedlet日誌 Fedlet日誌將提供有關在Cisco IdS中發生的任何SAML錯誤的詳細資訊

Cisco IdS API指標 idS處理的請求數

AD FS中的事件檢 允許使用者檢視系統中的事件日誌。處理SAML請求/傳送SAML響應時,AD 在Window 視器 FS中的任何錯誤都會記錄在此處。

航到Cisco 使用RTMT Fedlet日誌 Fedlet日誌 使用RTMT 請將顯示在 authorize_ 在AD FS Services L 在Window 在Window

工具的位置

使用RTMT 《RTMT使

請注意 F

SAML檢視器 SAML Viewer將幫助檢視從/傳送到Cisco IdS的SAML請求和響應。 此瀏覽器應用程式對於分析SAML請求/響應非常有用。 請檢視您的

2. SAM

3. SAM

包含調試選項的流程圖

SSO身份驗證的各種步驟以及每個步驟中的調試工件(如果該步驟中發生故障)都顯示在影象中。

下表詳細說明如何在瀏覽器中識別SSO每個步驟的故障。還介紹了不同的工具以及它們如何幫助調 試。

步驟	如何在瀏覽器中識別故障	工具/日誌
Cisco IdS的驗證碼要 求處理	如果失敗,瀏覽器不會重定向到SAML終端或AD FS,Cisco IdS會顯示 ISON錯誤 這表示客戶端ID或重定向URI 無效。	Cisco IdS logs — 表示 Cisco IdS API指標 — 表
示處理 通過Cisco IdS啟動 SAML請求	出現故障時,瀏覽器不會重定向到AD FS,Cisco IdS將顯示錯誤頁面/消息。	Cisco IdS Iogs — 指示 Cisco IdS API指標 — 君 AD FS中的事件檢視器
AD FS的SAML請求 處理	處理此請求的任何失敗都將導致AD FS伺服器顯示錯誤頁 ,而不是登入頁。	誤。 SAML瀏覽器外掛 — 幫 求。
由AD FS傳送 SAML響應	傳送響應的任何失敗都會導致AD FS伺服器在提交有效憑證 後顯示錯誤頁面。	AD FS中的事件檢視器 誤。
Cisco IdS的SAML響 應處理	Cisco IdS將顯示一個500錯誤及錯誤原因和一個快速檢查頁 面。	AD FS中的事件檢視器 應沒有成功狀態代碼,」 SAML瀏覽器外掛 — 幫 ,確定問題所在。 Cisco IdS log — 表示處 Cisco IdS API指標 — 君

Cisco IdS的Authcode請求處理

就Cisco IdS而言,SSO登入的出發點是從啟用了SSO的應用程式請求授權代碼。完成API請求驗證 以檢查它是否是來自註冊客戶端的請求。成功驗證導致瀏覽器被重定向到Cisco IdS的SAML終端。 請求驗證中的任何失敗都會導致從Cisco IdS傳送回錯誤頁面/JSON(JavaScript對象表示法)。

在此過程中遇到的常見錯誤

1.未完成客戶註冊

問題摘要 登入請求失敗,瀏覽器上出現401錯誤。

瀏覽器:

此消息出現401錯誤:{"error":"invalid_client","error_description":"Invalid ClientId。"} 錯誤消息 Cisco IdS日誌:

2016-09-02 00:16:58.604 IST(+0530)[IdSEndPoints-51] WARN com.cisco.ccbu.ids IdSConfigImpl.ja org.apache.oltu.oauth2.common.exception.OAuthProblemException:invalid_client Invalid Client com.cisco.ccbu.ids.auth.validator.IdSAuthorizeValidator.validateRequiredParameters(IdSAuthor

可能的原因 使用Cisco IdS的客戶端註冊不完整。

建議的操作 導航到Cisco IdS管理控制檯,並確認客戶端是否已成功註冊。如果沒有,則在繼續SSO之前註 2.使用者使用IP地址/備用主機名訪問應用程式 問題摘要 登入請求失敗,瀏覽器上出現401錯誤。

- **瀏覽器:** 錯誤消息
- ^{単の内心} 此消息出現401錯誤:{"error":"invalid_redirectUri","error_description":"Invalid Redirect Uri"} 使用者使用IP地址/備用主機名訪問應用程式。
- **可能的原因**在SSO模式下,如果使用IP訪問應用程式,則無法正常工作。應用程式應該使用在Cisco IdS中 名進行訪問。如果使用者訪問了未向Cisco IdS註冊的備用主機名,則可能會發生此問題。

導航到Cisco IdS管理控制檯,確認客戶端是否使用正確的重定向URL註冊,並且使用正確的重 **建議的操作** 問應用程式。

通過Cisco IdS啟動SAML請求

思科IdS的SAML端點是基於SSO的登入中SAML流的起點。Cisco IdS和AD FS之間的互動在此步驟 中觸發。此處的先決條件是,思科IdS應該知道要連線的AD FS,因為相應的IdP後設資料應該上傳 到思科IdS才能成功完成此步驟。

在此過程中遇到的常見錯誤

1. AD FS後設資料未新增到思科IdS

問題摘要 登入請求失敗,瀏覽器上出現503錯誤。

- **錯誤消息** 资意器:
- **9167月** 503錯誤與以下消息:{"error":"service_unavailable","error_description":"SAML後設資料未初始 **可能的原因** Idp後設資料在Cisco IdS中不可用。Cisco IdS和AD FS之間的信任建立不完整。
- **建議的操作**^{Ⅲ™座□□□⊥戦IOP}′度設資料。 如果不是,請上載從AD FS下載的IdP後設資料。 有關更多詳細資訊,請<u>參閱此處</u>。

AD FS的SAML請求處理

SAML請求處理是SSO流中AD FS的第一步。在此步驟中,由Cisco IdS傳送的SAML請求由AD FS讀取、驗證和解密。成功處理此請求會導致兩種情況:

 如果是瀏覽器中的新登入,AD FS將顯示登入表單。如果是從現有瀏覽器會話重新登入已經過 身份驗證的使用者,則AD FS會嘗試將SAML響應直接傳送回。

附註:此步驟的主要先決條件是AD FS配置回複方信任。

在此過程中遇到的常見錯誤

1. AD FS沒有最新的Cisco IdS SAML證書。

問題摘要 AD FS未顯示登入頁,而是顯示錯誤頁。
 瀏覽器
 AD FS顯示類似於以下內容的錯誤頁:
 訪問站點時出現問題。再次嘗試瀏覽到該站點。
 如果問題仍然存在,請聯絡此站點的管理員並提供參考編號以識別問題。
 參考編號: 1ee602be-382c-4c49-af7a-5b70f3a7bd8e

AD FS事件檢視器

聯合身份驗證服務處理SAML身份驗證請求時遇到錯誤。

其他資料

Microsoft.IdentityModel.Protocols.XmlSignature.SignatureVerificationFailedException:MSIS003 Microsoft.IdentityServer.Service.SamlProtocolService.ProcessRequest(Message requestMessageMe

- 可能的原因 未建立信賴方信任或思科IdS證書已更改,但不會將相同內容上傳到AD FS。 使用最新的Cisco IdS證書在AD FS和Cisco IdS之間建立信任。
- **建議的操作** 請確保思科IdS證書未過期。您可以在思科身份服務管理中檢視狀態控制面板。如果是,請在「 有關如何在ADFS和Cisco Id之間建立後設資料信任的更多詳細資訊,請參閱<u>此處</u>

由AD FS傳送的SAML響應

成功驗證使用者後,ADFS會通過瀏覽器將SAML響應傳送回Cisco IdS。ADFS可以發回帶有狀態代碼的SAML響應,狀態代碼指示成功或失敗。如果在AD FS中未啟用表單身份驗證,則這將指示失敗響應。

在此過程中遇到的常見錯誤

1. AD FS中未啟用表單身份驗證

問題摘要 瀏覽器顯示NTLM登入,然後失敗且未成功重定向到Cisco IdS。

- 失敗步驟 傳送SAML響應
- ☆三のAII 翻覧器: ※■■===
- [┓]₩^{月息} 瀏覽器顯示NTLM登入,但在成功登入後,它因許多重定向而失敗。
- 可能的原因 Cisco IdS僅支援基於表單的身份驗證,AD FS中未啟用表單身份驗證。

有關如何啟用表單身份驗證的詳細資訊,請參閱:

建議的操作 <u>ADFS 2.0窗體身份驗證設定</u> <u>ADFS 3.0窗體身份驗證設定</u>

Cisco IdS的SAML響應處理

在此階段,Cisco IdS從AD FS獲得SAML響應。此響應可能包含指示成功或失敗的狀態代碼。來自 AD FS的錯誤響應導致錯誤頁,必須調試該錯誤頁。

在成功的SAML響應期間,由於以下原因,處理請求可能會失敗:

- IdP(AD FS)後設資料不正確。
- 無法從AD FS檢索預期的傳出宣告。
- Cisco IdS和AD FS時鐘不同步。

在此過程中遇到的常見錯誤

1. Cisco IdS中的AD FS證書不是最新的。

問題摘要 登入請求失敗,瀏覽器上出現500錯誤,錯誤代碼為invalidSignature。

失敗步驟 SAML響應處理

瀏覽器: 瀏覽器中此消息出現500錯誤:

錯誤代碼:簽名無效

錯誤消息 消息:簽名證書與實體後設資料中定義的內容不匹配。

AD FS事件檢視器:

無錯誤

Cisco IdS日誌:

2016-04-13 12:42:15.896 IST(+0530)default ERROR [IdSEndPoints-0] com.cisco.ccbu.ids IdSEndPo com.sun.identity.saml2.protocol.impl.StatusResponseImpl.isSignatureValid(StatusResponseImpl

- **可能的原因** SAML響應處理失敗,因為IdP證書與Cisco IdS中的可用證書不同。
- 從以下位置下載最新的AD FS後設資料: https://<ADFSServer>/federationmetadata/2007-06/f 建議的操作 並通過身份服務管理使用者介面將其上傳到Cisco IdS。

有關詳細資訊,請參閱配置Cisco IdS和AD FS

2. Cisco IdS和AD FS時鐘不同步。

問題摘要 登入請求失敗,瀏覽器上出現500錯誤,狀態代碼為:urn:oasis:名稱:tc:SAML:2.0:狀態: 失敗步驟 SAML響應處理

瀏覽器:

此消息出現500錯誤:

IdP配置錯誤:SAML處理失敗

SAML斷言從IdP失敗,狀態代碼為:urn:oasis:names:tc:SAML:2.0:status:成功。請驗證IdP Cisco IdS日誌

2016-08-24 18:46:56.780 IST(+0530)[IdSEndPoints-SAML-22] ERROR com.cisco.ccbu.ids IdSSAMLAsy 錯誤消息 com.sun.identity.saml2.common.SAML2Utils.verifyResponse(SAML2Utils.java:609)com.sun.identity com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processSamlPostResponse(IdSSAMLAsyncServlet java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:111114) 5)at java SAML檢視器:

查詢NotBefore和NotOnOrAfter欄位

<條件NotBefore="2016-08-28T14:45:03.325Z" NotOnOrAfter="2016-08-28T15:45:03.325Z">

可能的原因 Cisco IdS和IdP系統中的時間不同步。

建議的操作 同步Cisco IdS和AD FS系統中的時間。建議使用NTP伺服器對AD FS系統和Cisco Id進行時間

3. AD FS中的錯誤簽名演算法(SHA256與SHA1)

登入請求失敗,瀏覽器上出現500錯誤,狀態代碼為:urn:oasis:names:tc:SAML:2.0:status:Re 問題摘要 AD FS事件檢視日誌中的錯誤消息 — AD FS中的錯誤簽名演算法(SHA256與SHA1)

失敗步驟 SAML響應處理

瀏覽器

此消息出現500錯誤:

IdP配置錯誤:SAML處理失敗

SAML斷言從IdP失敗,狀態代碼為:urn:oasis:names:tc:SAML:2.0:status:Responder。請驗證 錯誤消息 AD FS事件檢視器:

未使用預期簽名演算法對SAML請求進行簽名。使用簽名演算法http://www.w3.org/2001/04/xm 預期的簽名演算法為http://www.w3.org/2000/09/xmldsig#rsa-sha1

Cisco IdS日誌:

com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:298 - SAMLcom.sun.identity.saml2.common.SAML2com laSyncServlet.getAttributesMapFromSAMLResponse(IdSSAMLAsyncServlet.java:472)

可能的原因 AD FS配置為使用SHA-256。

更新AD FS以使用SHA-1進行簽名和加密。

- 1. RDP到AD FS系統。
- 2. 開啟AD FS控制檯。
- 3. 選擇信賴方**信任,然後**按一下「屬**性」**
- 4. 選擇Advanced頁籤。

5. 從下拉選單中選擇SHA-1。

_	uccx115p1.toi.com Properties							
[Monitoring	Identifiers	Encryption	Signature	Acc	epted Claims		
	Organization	Endpoints	Proxy End	lpoints I	Notes	Advanced		
	Specify the secure hash algorithm to use for this relying party trust.							
	Secure hash algorithm: SHA-1							
			ОК	Cano	cel	Apply		

4. 傳出宣告規則配置不正確

問題摘要 登入請求失敗,瀏覽器上出現500錯誤,顯示消息「無法從SAML響應檢索使用者識別符號。/魚 未在傳出宣告中設定uid和/或user_principal。

失敗步驟 SAML響應處理

瀏覽器: 此消息出現500錯誤: IdP配置錯誤:SAML處理失敗。 3. 無法從SAML響應檢索使用考證5

錯誤消息 無法從SAML響應檢索使用者識別符號。/無法從SAML響應檢索使用者主體。
AD FS事件檢視器:
無錯誤

Cisco IdS日誌:

com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:294 - SAMLcom.sun.identity.saml.common.SAMLExcep com.cisco.ccbu.ids.auth.api.IdSSAMLASSAMLAndPointRequest(IdSSAMLAsyncServlet.java:176)

在「宣告規則」中未正確配置強制傳出宣告(uid和user_principal)。

可能的原因,如果尚未配置NameID宣告規則,或者未正確配置uid或user_principal。

[▲] 如果NameID規則未配置或user_principal未正確對映,Cisco IdS會指示未檢索user_principal, 如果uid對映不正確,Cisco IdS將指示未檢索uid。

在AD FS宣告規則下,確保「user_principal」和「uid」的屬性對映定義如《IdP配置指南》(「 1. RDP到AD FS系統。

2. 編輯信賴方信任的宣告規則。

elp File Action View Window Help AD FS Display Name Claims Provider Trusts Claims Provider Trusts Coder Fule Name Coder Fule Name		
Image: Service Image	Help	🖬 File Action View Window Help
AD FS AD FS Claims Provider Trusts Code Registration Service Uccult5p1toi.com Code Registration Rules Code Rule Name Source Trust Rule Issued Claims Code Rule Name Claims Code Rule Code Ru	II 🖬 🔟	🗢 🔿 📶 🖬 🖬
b Service a Trust Relationships b Claims Provider Trusts Conso Claims Provider Trusts conso Relying Party Trusts		AD FS Relying Party Trusts
A Claims Provider Trusts Claims Provider Trusts Claims Provider Trusts Relying Party Trusts Edit Claim Rules for uccx115p1.toi.com Edit Claim Rules for uccx115p1.toi.com Statuto Trustom Rules Issuance Transform Rules Issuance Transform Rules Issuance Authorization Rules Delegation Authorization Rules The following transform rules specify the claims that will be sent to the relying party. Order Rule Name Issued Claims Add Rule Edit Rule Remove Rule OK Cancel Apply		Display Name
Claims Provider Trusts Uucck115p1.toi.com	7	Trust Relationships Device Registration Service
OnsZone Solid Issuance Transform Rules Issued Claims Issue Claims Issue Claims Issue Claims Issue Claims <td< td=""><td>ip Zones</td><td>Claims Provider Trusts uccx115p1.toi.com</td></td<>	ip Zones	Claims Provider Trusts uccx115p1.toi.com
Prescon Scores addr.at warders Edit Claim Rules for uccx115p1.toi.com Issuance Transform Rules Issuance Authorization Rules Delegation Authorization Rules The following transform rules specify the claims that will be sent to the relying party. Order Rule Name Issued Claims (In the following transform rules specify the claims that will be sent to the relying party. Order Rule Name (In the following transform rules specify the claims that will be sent to the relying party. Order Rule Name Issued Claims (In the following transform rules specify the claims that will be sent to the relying party. Order Rule Name Issued Claims (In the following transform rules specify the claims that will be sent to the relying party. Order Rule Name Issued Claims (In the following transform rules specify the claims that will be sent to the relying party. Order Rule Name Issued Claims (In the following transform rules specify the claims that will be sent to the relying party. Order Rule Name (In the following transform rules specify the claims that will be sent to the rule number to		Relying Party Trusts
Issuance Transform Rules Issuance Authorization Rules Delegation Authorization Rules InsZones The following transform rules specify the claims that will be sent to the relying party. Order Rule Name Issued Claims warder Issued Claims Image: Claim State S	9	Edit Claim Rules for uccx115p1.toi.com
DisZones Zones addr.at warders	ſ	Issuance Transform Rules Issuance Authorization Rules Delegation Authorization Rules
Arsten in the transformer in the		The following transform rules specify the claims that will be sent to the relying party.
Jorder Hule Name Solution addr.at warders Image: Solution of the term of t	1DnsZon	
addr.a warders Add Rule Edit Rule Remove Rule OK Cancel Apply	p Zones	Order Rule Name Issued Claims
warders	n-addr.ar	
Add Rule Edt Rule Remove Rule OK Cancel Apply		
Add Rule Edt Rule N Apply	rwarders	
Add Rule Edt Rule Remove Rule OK Cancel		
Add Rule Edt Rule NK Cancel Apply		
A 28 A 1 A 1 A 1 A 1 A T T TANKING		
ARE I I I I I I E E T TRIHADA		
A 5%		
Add Rule Edit Rule Remove Rule OK Cancel Apply		
Add Rule Edt Rule Remove Rule OK Cancel Apply		
Add Rule Edit Rule Remove Rule OK Cancel Apply		
A 324 A 140		
A 32 A 1 A 1 A 1 A 1 A 7 A 1 A 1 A 1 A 1 A 1		
Add Rule Edit Rule Remove Rule OK Cancel Apply		
		Add Rule Edit Rule Remove Rule
		OK Cancel Apply
#證USer principal和UId是否止惟到映	驗證usor	principal和uid是否正確對映

-	modes toi com				11 12			
	Nisuesitor.com		Pake	Add Transfo	rm Claim Rule	Wizard		
	Configure Rul	е						
	Steps Choose Rule Typ Configure Claim R	e Iule	You ca which issued Claim r Namel Rule te Attribut Active Mappir	an configure this rule to s to extract LDAP attribute from the rule. ule name: D emplate: Send LDAP Attributes te store: Directory ng of LDAP attributes to LDAP Attribute (Select add more) SAM-Account-Name User-Principal-Name	eend the values of L ss. Specify how the nbutes as Claims outgoing claim type t or type to	DAP attributes as c attributes will map to s: Outgoing Claim Ty uid user_principal	laims. Select o the outgoin	an attri g claim
						< Previo	ous f	inish

5.聯合AD FS中的傳出宣告規則配置不正確

問題摘要 登入請求失敗,瀏覽器上出現500錯誤,顯示消息「無法從SAML響應檢索使用者識別符號」。 失敗步驟 SAML響應處理

瀏覽器

此消息出現500錯誤: IdP配置錯誤:SAML處理失敗 無法從SAML響應檢索使用者識別符號。/無法從SAML響應檢索使用者主體。

錯誤消息 AD FS事件檢視器:

~ 無錯誤

Cisco IdS日誌:

com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:294 - SAMLcom.sun.identity.saml.common.SAMLExcep com.cisco.ccbu.ids.auth.api.IdSSAMLASSAMLAndPointRequest(IdSSAMLAsyncServlet.java:176)

可能的原因 在聯合AD FS中,可能缺少所需的更多配置。 **建議的操作** 按照<mark>配置Cisco IdS和AD FS中</sub>針對聯合AD FS的多域配置</mark>一節,檢查聯合AD中的AD FS配置是

6.未正確配置自定義宣告規則

問題摘要 登入請求失敗,瀏覽器上出現500錯誤,顯示消息「無法從SAML響應檢索使用者識別符號。/魚 未在傳出宣告中設定uid和/或user principal。

失敗步驟 SAML響應處理

瀏覽器

此消息出現500錯誤:

SAML斷言從IdP失敗,狀態代碼為: urn:oasis:names:tc:SAML:2.0:status:Requester/urn:oasis

AD FS事件檢視器:

SAML身份驗證請求具有無法滿足的NamelD策略。

申請人:<u>myids.cisco.com</u>

名稱識別符號格式:urn:oasis: 名稱:tc:SAML:2.0:nameid-format:transient

錯誤消息 SPNameQualifier:myids.cisco.com

異常詳細資訊:

MSIS1000:SAML請求包含的NameIDPolicy未由頒發的令牌滿足。請求的名稱IDPolicy:AllowC 此請求失敗。

使用者操作

使用AD FS 2.0管理單元配置發出所需名稱識別符號的配置。

Cisco IdS日誌:

2016-08-30 09:45:30.471 IST(+0530)[IdSEndPoints-SAML-82] INFO com.cisco.ccbu.ids SAML2SPAdag </samlp:StatusCode> </samlp:StatusCode> </samlp:StatusAuthnRequest:n/a 2016-08-30 09:45:30 com.sun.identity.saml2.common.SAML2Utils.verifyResponse(SAML2Utils.java:425)com.sun.identity

可能的原因 未正確配置自定義宣告規則。

在AD FS宣告規則下,確保「user_principal」和「uid」的屬性對映定義如配置指南(哪個指南 1. RDP到AD FS系統。

2. 編輯自定義宣告規則的宣告規則。



3. 驗證是否提供了AD FS和Cisco IdS完全限定域名。

Edit Rule - uccx115p1.toi.com

You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that ext claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and issuance statement using the AD FS claim rule language.

Claim rule name:

uccx.contoso.com

Rule template: Send Claims Using a Custom Rule

Custom rule:



[OK	Ca

7.對AD FS的請求過多。

問題摘要 登入請求失敗,瀏覽器上出現500錯誤,狀態代碼為:urn:oasis:names:tc:SAML:2.0:status:Re AD FS事件檢視日誌中的錯誤消息表示對AD FS的請求過多。

失敗步驟 SAML響應處理

瀏覽器

此消息出現500錯誤:

IdP配置錯誤:SAML處理失敗

錯誤消息 SAML斷言從IdP失敗,狀態代碼為:urn:oasis:names:tc:SAML:2.0:status:Responder。請驗證 AD FS事件檢視器:

Microsoft.IdentityServer.Web.InvalidRequestException:

MSIS7042:同一個客戶端瀏覽器會話在最後一個

16秒。請聯絡您的管理員以瞭解詳細資訊。

在Microsoft.IdentityServer.Web.FederationPassiveAuthentication.UpdateLoopDetectionCoc 在Microsoft.IdentityServer.Web.FederationPassiveAuthentication.SendSignInResponse(MS

Xml:<Event xmlns="<u>http://schemas.microsoft.com/win/2004/08/events/event</u>"> <System> <Provides <EventRecordID>29385</EventRecordID> <Correlation ActivityID="{98778DB0-869A-4DD5-B3B6-05653 ns2="<u>http://schemas.microsoft.com/win/2004/08/events</u>" xmlns="<u>http://schemas.microsoft.com/Ac</u> Microsoft.IdentityServer.Web.FederationPassiveAuthentication.SendSignInResponse(MSISSignInResponse(MSISSignInResponse)

2016-04-15 16:19:01.220 EDT(-0400)[IdSEndPoints-1] com.cisco.ccbu.ids IdSEndPoint.java:102 - com.sun.identity.saml2.profile.SPACSUtils.processResponseForFedlet(SPACSUtils.java:2038)last

- **可能的原因** 從同一瀏覽器會話進入AD FS的請求過多。 這通常不應在生產中發生。但是如果您遇到這種情況,您可以:
- **建議的操作** 1. 檢查AD FS Windows事件檢視器。
 - 2. 重新檢查信賴方信任設定。有關更多詳細資訊*,請參閱<mark>配置Cisco IdS和AD FS</mark> 3. 重新登入。*
- 8. AD FS未配置為對斷言和消息進行簽名。

問題摘要 登入請求失敗,瀏覽器上出現500錯誤,錯誤代碼: invalidSignature

失敗步驟 SAML響應處理

瀏覽器

此消息出現500錯誤: 錯誤代碼:無效簽名

- 錯誤消息 消息: ArtifactResponse中的簽名無效。
- Cisco IdS日誌:

2016-08-24 10:53:10.494 IST(+0530)[IdSEndPoints-SAML-241] INFO saml2error.jsp saml2error_jsp com.sun.identity.saml2.profile.SPACSUtils.getResponseFromPost(SPACSUtils.java:994)com.sun.idenSSAMLAsyncServlet.getAttributesMapFromSAMLResponse(IdSSAMLAsyncServlet.java:472)

可能的原因 AD FS未配置為對斷言和消息進行簽名。

- 1. 運行AD FS powershell命令:Set-ADFSRelingPartyTrust -TargetName < 信賴方信任識別
- 2. RDP到AD系統。
- 3. 開啟Powershell。
- 4. 將Windows PowerShell管理單元新增到當前會話。如果您正在使用ADFS 3.0,則中可能



5. 為消息和斷言新增AD FS信賴方信任。



相關資訊

這與文章中介紹的身份提供程式配置有關:

- https://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-centerexpress/200612-Configure-the-Identity-Provider-for-UCCX.html
- 技術支援與文件 Cisco Systems