使用CUCM和AD FS 2.0配置單點登入

目錄 簡介 必要條件 需求 <u>採用元件</u> <u>背景資訊</u> 在Windows伺服器上下載並安裝AD FS 2.0 <u>在Windows伺服器上配置AD FS 2.0</u> 將Idp後設資料匯入CUCM /下載CUCM後設資料 將CUCM後設資料匯入AD FS 2.0伺服器並建立宣告規則 <u>在CUCM上完成SSO啟用並運行SSO測試</u> 疑難排解 <u>將SSO日誌設定為調試</u> 查詢聯合身份驗證服務名稱 無點證書和聯合身份驗證服務名稱 <u>CUCM和IDP伺服器之間的時間不同步</u> <u>相關資訊</u>

簡介

本文檔介紹如何在Cisco Unified Communications Manager和Active Directory聯合身份驗證服務上 配置單一登入(SSO)。

必要條件

需求

思科建議您瞭解以下主題:

- 思科整合通訊管理員(CUCM)
- Active Directory聯合身份驗證服務(AD FS)的基本知識

要在您的實驗環境中啟用SSO,您需要以下配置:

- 安裝了AD FS的Windows伺服器。
- 配置了LDAP同步的CUCM。
- 已選擇標準CCM超級使用者角色的終端使用者。

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- 採用AD FS 2.0的Windows伺服器
- CUCM 10.5.2

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。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

背景資訊

提供了在Windows Server 2008 R2上安裝AD FS 2.0的過程。這些步驟也適用於Windows Server 2016上的AD FS 3.0。

在Windows伺服器上下載並安裝AD FS 2.0

步驟 1.導覽至<u>Download AD FS 2.0</u>。

- 步驟 2.確保根據Windows Server選擇適當的下載。
- 步驟 3.將下載的檔案移動到Windows伺服器。

步驟 4.繼續安裝:

步驟 5.出現提示時,選擇Federation Server:

👔 Acti	ve Directory Federation Services 2.0 Setup Wizard
Serve	er Role
You one o	can configure this computer in either the federation server role or the federation server proxy role. Select of the following roles for this computer.
æ	Federation server
	A federation server is an authentication and trust management provider that issues security tokens to enable access to claims-based applications in your organization or in federated partner organizations.
C	Federation server proxy
	A federation server proxy redirects requests from Internet clients to federation servers that are behind a firewall on your corporate network. It also forwards security tokens issued by federation servers to clients.
	< Previous Next > Cancel

步驟6.自動安裝某些依賴項 — 完成後,按一下完成。

現在您的伺服器上已安裝AD FS 2.0,您需要新增一些配置。

在Windows伺服器上配置AD FS 2.0

步驟 1.如果在安裝後沒有自動開啟AD FS 2.0視窗,可以按一下Start並搜尋AD FS 2.0管理以手 動開啟該視窗。

步驟 2.選擇AD FS 2.0 Federation Server Configuration Wizard。



步驟3.下一步,按一下建立新的聯合身份驗證服務。

AD FS 2.0 Federation Server Configuration Wizard
--

Welcome

Steps	Welcome to the AD ES 2.0 Federation Server Configuration Wizard
Welcome	
Select Deployment Type Endersting Service Name	This wizard helps you configure Active Directory Federation Services (AD FS) 2.0 software on this computer, which sets up the computer as a federation server. An instance of AD FS is referred to as a Federation Service.
 Federation Service Name Summary Results 	 Create a new Federation Service Select this option to set up either a stand-alone federation server or the first server in a federation server farm. Add a federation server to an existing Federation Service Select this option to join this computer to an existing federation server farm.
	< Previous Next > Cancel Help

步驟 4.對於大多數環境,獨立聯合伺服器就足夠了。

x

ps	You can create either a stand-alone federation server for evaluation numbers or a small production
Velcome	environment, or you can create a federation server in a new farm for load balancing and high availability.
Select Deployment Type	Select one of the following options. Either of these options will use the Windows Internal Database to store
ederation Service Name	coningenetion read.
xisting Database	O New federation server farm
ummary	This option will create a new Federation Service with settings for high availability and load balancing. This computer will be the primary federation server in the farm. Later, you can scale out this farm by
Results	adding more federation servers.
	 that has sufficient permissions in Active Directory to create a container object (for sharing certificates) and to set an SPN (for the service account), such as an account that is a member of the Domain Admins group. Stand-alone federation server
	This option will create a new Federation Service on this computer. This option is recommended for evaluation purposes or a small production environment. If you select this option, you will not be able to add more servers to create a farm.
	You can use SQL Server with AD FS 2.0 to take advantage of the full feature set and achieve maximum scalability. To set up AD FS to use SQL Server, use the command-line version of this wizard. For more information, click Help

步驟 5.接下來,系統會要求您選擇憑證。只要伺服器有證書,此欄位就會自動填充。

teps	This wizard determines the Federation Sen	vice name from t	he Subject fiel	d of the S	SI certificate for the
Welcome Select Deployment Type	Default Web Site. If the wizard cannot del must select a certificate.	termine the Fede	ration Service	name from	m the SSL settings, yo
Federation Service Name	CCI actificato	Construction.		Port	
Existing Database	sso.win2k8	*	View	443	*
Results	Federation Service name:	-			
	Win2k8.sckiewer.lab	-			

步驟 6.如果伺服器上已經有一個AD FS資料庫,則需要將其刪除才能繼續。

步驟 7.最後,您將進入一個摘要螢幕,您可以在其中按一下下一步。

將Idp後設資料匯入CUCM /下載CUCM後設資料

步驟 1.使用您的Windows伺服器主機名/FQDN更新URL並從AD FS伺服器下載後設資料 — <u>https://hostname/federationmetadata/2007-06/federationmetadata.xml</u>

步驟 2.導覽至Cisco Unified CM Administration > System > SAML Single Sign-On。

步驟 3.按一下Enable SAML SSO。

步驟 4.如果收到有關Web伺服器連線的警報,請按一下Continue。

步驟 5.接下來,CUCM會指示您從IdP下載後設資料檔案。 在此方案中,您的AD FS伺服器是 IdP,您在第1步中下載了後設資料,因此按一下下一步。

步驟 6.按一下Browse > Select the .xml from Step 1 > Import IdP Metadata。

步驟 7.有一條消息表明匯入成功:

System 🔻 C	Call Routing 👻 Media Resource	ces 🔻 Advanced Featu	ures 🔻 Device 🔻	Application -	User Management 🔻
SAML Singl	e Sign-On Configuratio	on			
Next					
Status —					
Import	succeeded for all servers				
Import the	e IdP Metadata Trust Fil	le			
This step up	ploads the file acquired fro	m the IdP in the prev	ious manual step	to the Collabora	ation servers.
1)Select the File	e IdP Metadata Trust				
Browse	No file selected.				
2)Import th	is file to the Collaboration	servers			
This action	must be successful for at l	least the Publisher bef	fore moving on to	o <mark>the next task i</mark> r	n this wizard.
Import I	dP Metadata	V Import succeede	ed for all servers	l.	
Next 0	Cancel				

步驟 8.按「Next」(下一步)。

步驟 9.現在您已將IdP後設資料匯入CUCM,因此需要將CUCM的後設資料匯入IdP。

步驟 10.按一下下載信任後設資料檔案。

步驟 11.按「Next」(下一步)。

步驟 12.將.zip檔案移動到Windows Server並將內容解壓到資料夾中。

將CUCM後設資料匯入AD FS 2.0伺服器並建立宣告規則

步驟 1.按一下Start並搜尋AD FS 2.0 Management。

步驟 2.按一下Required: Add a trusted relisting party。

🔌 註:如果您沒有看到此選項,您需要關閉視窗並重新開啟它。

步驟 3.開啟Add Relisting Party Trust Wizard後,單擊Start。

步驟 4.在此,您需要匯入在步驟12中抽取的XML檔案。選擇Import data about the relisting party from a file,瀏覽到資料夾檔案,然後為發佈者選擇XML。

💊 注意:對於要使用SSO的任何Unified Collaboration伺服器,請使用上述步驟。

Select Data Source

Steps	Select an option that this wizard will use to obtain data about this relying party:				
Welcome	C Import data about the relying party published online or on a local network				
Select Data Source	Use this option to import the necessary data and certificates from a relying party organization that				
Specify Display Name	publishes its federation metadata online or on a local network.				
 Choose Issuance Authorization Rules 	Federation metadata address (host name or URL):				
 Ready to Add Trust Finish 	Example: fs.contoso.com or https://www.contoso.com/app				
	Import data about the relying party from a file				
	exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file. Federation metadata file location: C:\Users\Administrator\Desktop\SPMetadata_1cucm1052 sckiewer.lab.xml Browse				
	C Enter data about the relying party manually				
	Use this option to manually input the necessary data about this relying party organization.				
	< Previous Next > Cancel Help				

步驟 5.按「Next」(下一步)。

步驟 6.編輯顯示名稱,然後按一下下一步。

步驟 7.選擇Permit all users to access this relisting party,然後按一下Next。

步驟 8.再次按一下Next。

步驟 9.在此螢幕上,確保選中嚮導關閉時已為此信賴方信任開啟「編輯宣告規則」對話框,然 後按一下「關閉」。

步驟 10.此時將開啟「編輯宣告規則」視窗:

×

Order	Rule Name		Issued Claims	
				<u>^</u>
Add R	ule Edit F	Rule. Remove R	ule	

步驟 11.在此視窗中,按一下Add Rule。

步驟 12.對於宣告規則模板,選擇Send LDAP Attributes as Claims,然後按一下Next。

步驟 13.在下一頁上,輸入NamelD作為索賠規則名稱。

步驟 14.為屬性儲存選擇Active Directory。

步驟 15.為LDAP Attribute選擇SAM-Account-Name。

步驟 16.輸入uid作為傳出宣告型別。

註:uid不是下拉選單中的選項 — 必須手動輸入它。

📬 Add Transform Claim R	ule Wizard					×	
Configure Rule							
Steps	You c	an configure this rule to send the	e values of l	DAP attributes as claims	elect an attribute st	tore from	
Choose Rule Type	which	which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.					
Configure Claim Rule	Claim	rule name:					
	Name	ID					
	Rule t	emplate: Send LDAP Attributes a ite store:	as Claims				
	Active	e Directory		•			
	Марр	ing of LDAP attributes to outgoin	ıg claim type	15:			
	LDAP Attribute Outgoing Claim Type						
		SAM-Account-Name	•	uid		_	
	▶*		•				
			< Pr	evious Finish	Cancel	Help	

步驟 17.按一下「Finish」(結束)。

步驟 18.第一條 規則現在已完成。再次按一下Add Rule。

步驟 19.選擇Send Claims Using a Custom Rule。

步驟 20.輸入申請規則名稱。

步驟 21.在Custom rule欄位中,貼上以下文本:

c:[鍵入== "<u>http://schemas.microsoft.com/ws/2008/06/identity/</u>claims/windowsaccountname"] =>問題(型別= "<u>http://schemas.xmlsoap.org/ws/2005/05/identity/cl</u>aims/nameidentifier", Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType, Properties["<u>http://schemas.xmlsoap.org/ws/2005/05/</u>identity/claimperities/format"] = "urn:oasis:names:tc:SAML:2.0:nameid-format:transient",屬性 ["<u>http://schemas.xmlsoap.org/ws/2005/05/</u>identity/claimperities/namequalifier"] = "<u>http://ADFS_FEDERATION_SERVICE_NAME/com/adfs/service/trust</u>", Properties["<u>http://schemas.xmlsoap.org/ws/2005/05/</u>identity/claimperities/spnamequalifier"] = "CUCM_ENTITY_ID");

步驟 22.確保將AD_FS_SERVICE_NAME和CUCM_ENTITY_ID更改為相應的值。

註:如果您不確定AD FS服務名稱,可以按照步驟查詢它。 CUCM實體ID可以從CUCM後設 資料檔案中的第一行提取。 檔案第一行上有一個entityID,如下所示 , entityID=1cucm1052.sckiewer.lab。您需要在索賠規則的相應部分輸入帶下劃線的值。

Steps Choose Bule Type	You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an
Capfigure Claim Pule	issuance statement using the AD FS 2.0 claim rule language.
	Claim rule name:
	CUCM SSO Custom Rule
	Rule template: Send Claims Using a Custom Rule
	Custom rule:
	=> issue(Type =
	<pre>""""""""""""""""""""""""""""""""""""</pre>
	<pre>qualifier"] = "http://win2k8.sckiewer.lab/adfs/com/adfs/service/trust", Properties ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spna mequalifier"] = "1cucm1052.sckiewer.lab");</pre>
	More about the claim rule language

步驟 23.按一下「Finish」(結束)。

步驟 24.按一下「OK」(確定)。

✤ 注意:對於要使用SSO的任何Unified Collaboration伺服器,都需要宣告規則。

在CUCM上完成SSO啟用並運行SSO測試

步驟 1.現在,AD FS伺服器已完全配置,您可以返回到CUCM。

步驟 2.您在最終配置頁面上關閉:

Back	tion
Status The server metadata file must	be installed on the IdP before this test is run.
Test SSO Setup	
This test verifies that the metadata	files are correctly configured and will allow SSO to start up on the servers. This test can be run or
1)Pick a valid username to use for t	this test
This user must have administrator r Please use one of the Usernan Valid administrator Usernames	rights and also exist in the IdP. mes shown below. Using any other Username to log into the IdP may result in administrator lockou
sckiewer	
2)Launch SSO test page	

步驟 3.選擇已選擇「標準CCM超級使用者」角色的終端使用者,然後按一下運行SSO測試……

步驟 4. 確保您的瀏覽器允許彈出視窗, 並在提示中輸入您的憑據。

Test SAML - Firefox Developer Edition	0-0	\times
https://1cucm1052.sckiewer.lab:8443/ssosp/pages/TestSSO.jsp		

SSO Test Succeeded!

Congratulations on a successful SAML SSO configuration test. Please close this window and click "Finish" on the SAML configuration wizard to complete the setup.

-				
\sim		-	~	
C .1	U	5	е	
-	~	-	~	

步驟 5.在彈出視窗中按一下Close,然後按一下Finish。

步驟 6.在短暫重新啟動Web應用程式後, 啟用SSO。

疑難排解

將SSO日誌設定為調試

要將SSO日誌設定為調試,必須在CUCM的CLI中運行此命令:set samItrace level debug 可以從RTMT下載SSO日誌。日誌集的名稱為Cisco SSO。

查詢聯合身份驗證服務名稱

要查詢聯合身份驗證服務名稱,請按一下Start並搜尋AD FS 2.0 Management。

·按一下「編輯聯盟服務屬性……」 ·在「常規」頁籤上,查詢聯合身份驗證服務名稱

無點證書和聯合身份驗證服務名稱

如果在AD FS配置嚮導中收到此錯誤消息,則需要建立新證書。

所選證書不能用於確定聯合身份驗證服務名稱,因為所選證書具有無點(短名稱)使用者名稱。請 選擇沒有無點(短名稱)使用者名稱的其他證書,然後重試。

步驟 1.按一下「開始」並搜尋iis,然後開啟「Internet資訊服務(IIS)管理器」



步驟 2.按一下伺服器的名稱。



步驟 3.按一下「伺服器證書」。



步驟 4.點選Create Self-Signed Certificate。



步驟 5.輸入您想要用作證書別名的名稱。

Create Self-S	Signed Certificate			? ×
P	Specify Friendly Name			
Specify a f for signing	ile name for the certificate request.	This information can be s	sent to a certificate authority	
Specify a f	riendly name for the certificate:			
sso.win2k8).pkinane.lab			
			ОК	Cancel

CUCM和IDP伺服器之間的時間不同步

如果在從CUCM運行SSO測試時收到此錯誤,則需要將Windows伺服器配置為使用與CUCM相同的 NTP伺服器。

無效的SAML響應。當Cisco Unified Communications Manager和IDP伺服器之間的時間不同步時 ,可能會造成這種情況。請驗證兩台伺服器上的NTP配置。從CLI運行「utils ntp status」以檢查 Cisco Unified Communications Manager上的此狀態。

在Windows Server指定了正確的NTP伺服器後,您需要執行另一個SSO測試並檢視問題是否仍然存在。在某些情況下,有必要歪曲宣告的有效期。關於這一過程的更多詳<u>細資訊。</u>

相關資訊

• <u>技術支援與文件 - Cisco Systems</u>

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。