使用AD FS版本2.0為每個群集配置單個SAML IdP連線/協定

目錄

<u>
簡介</u>
<u>
必要條件</u> <u>
需求</u> <u>
採用元件</u> <u>
背景資訊</u> 設定 <u>
步驟1.從CUCM匯出SP後設資料</u> <u>
步驟2.從AD FS下載IDP後設資料</u> <u>
步驟3.設定IdP</u> <u>
步驟4.啟用SAML SSO</u> 驗證 <u>
疑難排解</u>

簡介

本文檔介紹如何使用Active Directory聯合身份驗證服務(AD FS)為每個群集配置單一安全斷言標籤 語言(SAML)身份提供程式(IdP)連線/協定。

必要條件

需求

思科建議您瞭解以下主題:

- Cisco Unified Communications Manager(CUCM)11.5或更高版本
- Cisco Unified Communications Manager IM and Presence版本11.5或更高版本
- Active Directory聯合身份驗證服務版本2.0

採用元件

本檔案中的資訊是根據以下軟體版本:

- 作為IdP的Active Directory聯合身份驗證服務版本2.0
- 思科整合通訊管理員版本11.5
- Cisco IM和狀態伺服器版本11.5

背景資訊

對於SAML SSO,需要在服務提供商(SP)和IdP之間形成一個信任圈。 當交換信任(後設資料)時

,此信任作為SSO啟用的一部分建立。 從CUCM下載後設資料並將其上傳到IdP,同樣,從IdP下載 後設資料並將其上傳到CUCM。

在CUCM 11.5之前的版本中,始發節點生成後設資料檔案,同時從集群中的其他節點收集後設資料 檔案。 它將所有後設資料檔案新增到單個zip檔案,然後呈現給管理員。管理員必須解壓縮此檔案 並在IdP上預配每個檔案。例如,8個節點群集的8個後設資料檔案。

每個集群的單個SAML IdP連線/協定功能是從11.5引入的。作為此功能的一部分,CUCM為集群中 的所有CUCM和IMP節點生成單個服務提供商後設資料檔案。後設資料檔案的新名稱格式為 <hostname>-single-agreement.xml

基本上,一個節點建立後設資料並將其推送到群集中的其他SP節點。這可實現輕鬆的配置、維護和 管理。例如,8節點群集有1個後設資料檔案。

群集範圍的後設資料檔案使用Multiserver tomcat證書,該證書確保群集中所有節點使用的金鑰對相同。後設資料檔案還包含群集中每個節點的斷言使用者服務(ACS)URL清單。

CUCM和Cisco IM and Presence版本11.5支援SSO模式、集群範圍(每個集群一個後設資料檔案)和每個節點(現有模型)。

本文檔介紹如何使用AD FS 2.0配置SAML SSO的集群範圍模式。

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

步驟1.從CUCM匯出SP後設資料

開啟Web瀏覽器,以管理員身份登入到CUCM,然後導**覽至System > SAML Single Sign On。**

預設情況下,Cluster Wide單選按鈕處於選中狀態。按一下**匯出所有後設資料。**以名稱 <hostname>-single-agreement.xml向管理員顯示的後設資料資料檔案



步驟2.從AD FS下載IDP後設資料

要下載IdP後設資料,請參閱連結<u>https:// <ADFS的FQDN>/federationmetadata/2007-</u> 06/federationmetadata.xml

步驟3.設定IdP

如圖所示,導航到AD FS 2.0 Management/Trust Relationship Ships/Reliding Party trust。按一下新

增信賴方信任。

📬 AD F5 2.0			_ D ×
🙀 File Action View Window Help			_8×
💠 🧼 🖄 🗊 🔢 🗊			
AD F5 2.0	Relying Party Trusts	Actions	
Service Trust Relationships	Display Name	Relying Party Trusts	*
Claims Provider Trusts		Add Relying Party Trust	
Attribute Stores	1	View New Window from Here	•
	1	C Refresh	
	×	Melp	

將開啟「新增信賴方信任嚮導」(如圖所示),然後按一下**「開始」**。

📬 Add Relying Party Trus	t Wizard
Welcome	
Steps Velcome Select Data Source Choose Issuance Authorization Rules Ready to Add Trust Finish	Welcome to the Add Relying Party Trust Wizard This wizard will help you add a new relying party trust to the AD FS configuration database. Relying parties consume claims in security tokens that are issued by this Federation Service to make authentication and authorization decisions. The relying party trust that this wizard creates defines how this Federation Service recognizes the relying party and issues claims to it. You can define issuance transform rules for issuing claims to the relying party after you complete the wizard.
	< Previous Start Cancel Help

從檔案中按一下有關信賴方的匯入資料。瀏覽從CUCM SAML SSO配置頁下載的SP後設資料。然 後按一下「Next」,如下圖所示:

Add Relying Party True	st Wizard
Select Data Source	
Select Data Source Steps Welcome Select Data Source Choose Issuance Authorization Rules Ready to Add Trust Finish	Select an option that this wizard will use to obtain data about this relying party: Import data about the relying party published online or on a local network. Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata address (host name or URL): Example: fs.contoso.com or https://www.contoso.com/app Import data about the relying party from a file Use this option to import the necessary data and certificates from a relying party organization that has 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\Cluster.Wide\cucm1150-single-agreement.xm
	Enter data about the relying party manually Use this option to manually input the necessary data about this relying party organization.

鍵入信賴方的顯示名稱和任何可選註釋。按一下「**Next**」,如下圖所示:

📬 Add Relying Party Trust	Wizard	×
Specify Display Nam	8	
Steps	Type the display name and any optional notes for this relying party.	
 Welcome Select Data Source 	Display name:	
Specify Display Name	CUCM_Cluster_Wide_Relying_Party_trust	
 Choose Issuance Authorization Rules Ready to Add Trust Finish 	Notes:	
	< Previous Next > Can	el Help

選擇**允許所有使用者訪問此信賴方**以允許所有使用者訪問此信賴方,然後按一下**下一步**,如下圖所 示:

Add Relying Party Trus	Wizard X
Choose Issuance Au	thorization Rules
Steps Welcome Select Data Source Specify Display Name Choose Issuance Authorization Rules Ready to Add Trust Finish	Issuance authorization rules determine whether a user is permitted to receive claims for the relying party. Choose one of the following options for the initial behavior of this relying party's issuance authorization rules. • Permit all users to access this relying party The issuance authorization rules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access. • Deny all users access to this relying party The issuance authorization rules will be configured to deny all users access to this relying party. You must later add issuance authorization rules to enable any users to access this relying party. You must later add issuance authorization rules for this relying party trust by selecting the relying party trust and clicking Edit Claim Rules in the Actions pane.
	< Previous Next > Cancel Help

在**Ready to Add Trust**頁面下,您可以檢視已配置的信賴方信任的設定。現在按一下**Next**,如下圖 所示:

teps	The relying party trust has been configured. Review the following settings, and then click Next to add the
Welcome Select Data Source	relying party trust to the AD FS configuration database.
Specify Display Name	Monitoring Identifiers Encryption Signature Accepted Claims Organization Endpoints N.
Choose Issuance Authorization Rules	Specify the monitoring settings for this relying party trust.
Ready to Add Trust	Relying party's rederation metadata URL:
	 Monitor relying party Automatically update relying party This relying party's federation metadata data was last checked on: < never > This relying party was last updated from federation metadata on: < never >

完成頁確認信賴方信任已成功新增到AD FS配置資料庫。取消選中該框並按一下**Close**,如下圖所示 :

Add Relying Party Trus	t Wizard	×
Finish		
Steps • Welcome • Select Data Source • Specify Display Name • Choose Issuance Authorization Rules • Ready to Add Trust • Finish	The relying party trust was successfully added to the AD FS configuration database. You can modify this relying party trust by using the Properties dialog box in the AD FS 2.0 Management snapin.	
]

按一下右鍵**信賴方信任**,然後按一下**編輯宣告規則**,如下圖所示:

📬 AD FS 2.0			and the second second second second	
🙀 File Action View Window	Help			_@×
AD F5 2.0	Relying Party Trusts			Actions
E Servce Trust Relationships Claims Provider Trusts Relying Party Trusts	Display Name CUCM_Cluster_Wide_Relying_Party_Inust	Enabled Yes	Identifies cucm1150.adls.ucce.com	Relying Party Trusts Add Relying Party Trust Add Relying Party Trust New Window from Here Refresh Party Trust Help CUCM_Cluster_Wide_Relying_Party_trust Update from Federation Metadata Edit Claim Rules Disable Properties X Delete
	<u>د</u>		<u>×</u>	Help 🗸

現在,按一下「Add Rule」,如下圖所示:

Edit Claim Rules for CUCM_Cluster_Wide_Rely	ing_Party_trust	_ 🗆 🗙
Issuance Transform Rules Issuance Authorization Rul	es Delegation Authorization R	ules
The following transform rules specify the claims that w	ill be sent to the relying party.	
Order Bule Name	Issued Claims	
		1
Add Rule Edit Rule Remove Rule		
	I	
ОК С	ancel Apply	Help

開啟Add Transform Claim Rule後,使用預設宣告規則模板Send LDAP Attributes as Claims按一下 Next,如下圖所示:

iteps	Select the template for the claim rule that you want to create from the following list. The description
Choose Rule Type	provides details about each claim rule template.
Configure Claim Rule	Claim rule template:
	Send LDAP Attributes as Claims
	Claim rule template description:
	store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to colu send
	Individual group memberships, use the Send Group Membership as a Claim rule template.
	Individual group memberships, use the Send Group Membership as a Claim rule template.
	Individual group memberships, use the Send Group Membership as a Claim rule template.
	Individual group memberships, use the Send Group Membership as a Claim rule template.
	Individual group memberships, use the Send Group Membership as a Claim rule template.
	Individual group memberships, use the Send Group Membership as a Claim rule template.

按一下「**Configure Claim Rule**」,如下圖所示。LDAP屬性必須與CUCM中LDAP目錄配置中的 LDAP屬性匹配。以**uid**身份管理傳出宣告型別。按一下「**Finish**」,如下圖所示:

Add Transform Claim R	ule Wizard				×
Configure Rule					
Steps Choose Rule Type Configure Claim Rule	You o which issued Claim	an configure this rule to send the to extract LDAP attributes. Spe d from the rule. rule name:	e values of L cify how the	DAP attributes as claims. Select an attribute store from attributes will map to the outgoing claim types that will b	e
	Rule	emplate: Send LDAP Attributes a ute store:	as Claims		
	Mapp	e Directory ing of LDAP attributes to outgoin	ng claim type		-
		SAM-Account-Name	•	uid going claim Type	-
	*		•	2	-
			< Pre	evious Finish Cancel Help	

為信賴方新增自定義規則。按一下Add rule。選擇Send Claims using a Custom Rule,然後按一下 Next,如下圖所示:

🎁 Add Transform Claim Ri	Jle Wizard			
Select Rule Templat	B			
Steps	Select the template for the claim rule that you want to create from the following list. The description			
Choose Rule Type	provides details about each claim rule template.			
 Configure Claim Rule 	Claim rule template:			
	Claim rule template description:			
	Using a custom rule, you can create rules that can't be created with a rule template. Custom rules are written in the AD FS 2.0 claim rule language. Capabilities that require custom rules include: Sending claims from a SQL attribute store Sending claims on a solut attribute store Sending claims only when 2 or more incoming claim sare present Sending claims only when an incoming claim value matches a complex pattern Sending claims for use only in later rules Teal me more about this rule template			
	< Brevious Next > Cancel Help			

在配置宣告規則中,在嚮導的Custom Rule欄位中鍵入Claim Rule Name,然後複製給定和過去的 宣告規則,修改宣告規則中的namequalifier和spname限定符。按一下「**Finish**」,如下圖所示:

報銷申請規則:

c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]

=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer =
c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"urn:oasis:names:tc:SAML:2.0:nameid-format:transient",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"] =
"http:// <fqdn adfs="" of="">/adfs/com/adfs/services/trust",</fqdn>
<pre>Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =</pre>
" <entity id="" in="" metadata="" sp="" the="">");</entity>

Entity ID = Open the SP metadata and check the Entity ID. Basically, its the CUCM Publisher's FQDN.

Steps Choose Rule Type Configure Claim Rule	You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extra claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and issuance statement using the AD FS 2.0 claim rule language. Claim rule name:	cts an
	Cluster_Side_Claim_Rule	
	Rule template: Send Claims Using a Custom Rule Cystom rule:	
	<pre>ntname"] => issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier ", Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType, Properties ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/form at"] = "urn:oasis:names:tc:SAML:2.0:nameid-format:transient", Properties ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/name qualifier"] = "http://win- jd4ia7ugmrm.adfs.ucce.com/adfs/com/adfs/services/trust", Properties ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spna mequalifier"] = "cucml150.adfs.ucce.com");</pre>	1
	More about the claim rule language	

```
如圖所示,按一下Apply,然後OK。
```

Na Na Clu	imelD ister_Side_Clain	n_Rule	uid <see claim="" rule=""></see>	
				-
∖dd Rule	. <u>E</u> dit Rule	e <u>R</u> emove R	ule	

步驟4.啟用SAML SSO

開啟Web瀏覽器,以管理員身份登入CUCM,然後導**覽至System > SAML Single Sign On**。 預設情況下,**Cluster Wide**單選按鈕處於選中狀態。按一下「**Enable Saml SSO**」,如下圖所示:



如圖所示,彈出視窗將通知Web伺服器重新啟動警告以及根據idp選擇群集範圍的SAML SSO或每節 點SAML SSO的資訊。按一下「**Continue**」(繼續)。



啟用群集範圍的SSO的條件是:必須已經部署多伺服器tomcat證書。按一下「**Test for Multi-Server tomcat Certificate**」,如下圖所示:

SAML Single Sign-On Configuration
Hext
Status
(i) Status: Ready
Test for Multi-Server tomcat certificate
The criteria for enabling dusterwide SSD is that you must have a multiserver tomcat certificate already deployed. If you have not done this already please follow the below steps:
1) Login to Cisco Unified OS Administration Page and Navigate to Certificate Management under Security Menu
2) Click on Generate CSR
3) Select Certificate Purpose as Tomcat
4) Select Distribution as "Multi-Server"
5) Click Generate
6) Download the CSR and get it signed from the CA of your choice
7) Once the certificate is issued by the CA, upload it via the "Upload Certificate/ Certificate chain" option on the Certificate Management page
8) Restart Tomcat service on all the nodes in the cluster
9) Restart TFTP service on all the TFTP nodes in the cluster
If the above steps have been completed, click Test below which will confirm if the multi-server tomcat certificate is deployed before proceeding to the next stage
Test for Multi-Server tomcat certificate
Next Cancel

確認後,所有節點都具有多伺服器證書(Multi Server Certificate)將顯示**所有節點都具有多伺服器證 着(All Nodes have Multi Server Certificate**),然後按一下**下一步**,如下圖所示:

SAML Single Sign-On Configuration
Next
Status
(i) Status: Ready
All nodes have Multi Server Certificate
Test for Multi-Server tomcat certificate
The criteria for enabling clusterwide SSO is that you must have a multiserver tomcat certificate already deployed. If you have not done this already please follow the below steps:
1) Login to Cisco Unified OS Administration Page and Navigate to Certificate Management under Security Menu
2) Click on Generate CSR
3) Select Certificate Purpose as Tomcat
4) Select Distribution as "Multi-Server"
5) Click Generate
6) Download the CSR and get it signed from the CA of your choice
7) Once the certificate is issued by the CA, upload it via the "Upload Certificate/ Certificate chain" option on the Certificate Management page
8) Restart Tomicat service on all the hodes in the duster
9) Restart TFTP service on all the TFTP houes in the cluster
If the above stars have been completed, sick Test below which will confirm if the multi-senser terrist certificate is dealayed before proceeding to the payt stars
a die autore aceps nere been competent, die nest below which will commin in die mont-server compatient de begingen beloke proceeding to die next stage
Tex for multi-server contract certificate
Next Cancel
μ回所示,按一下 下一步 。
CANI Circle Circ On Conferencian
SAME Single Sign-On Configuration
Next
I NEAL
r Status
(i) Status: Ready
Download Identity provider(IdP) Metadata Trust File
To configure the trust relationship between the IdP and your devices, you must first obtain trust metadata from your IdP and
import it to your servers. You will need to manually obtain the file from the IdP before you can upload it to your Collaboration
servers.

This is a manual step! 1)Log in to your IdP and download the metadata trust file to your local server. 2)Click Next once you have this file available locally.

Next Cancel

瀏覽並選擇下載的IdP後設資料。按一下「Import IdP Metadata」,如下圖所示:

SAML Single Sign-On Configuration
Next .
Status
(i) Status: Ready
Ready to import Identity Provider metadata trust file to cluster servers
TIMPORT THE IdP Metadata Trust File
This step uploads the file acquired from the IdP in the previous manual step to the Collaboration servers.
1)Select the IdP Metadata Trust File
Browse federationmetadata.xml
2)Import this file to the Collaboration servers
This action must be successful for at least the Publisher before moving on to the next task in this wizard.
Import IdP Metadata
Next Cancel

此頁確認所有伺服器的匯入成功,然後按一下**下一步**,如下圖所示:

SAML Single Sign-On Configuration
Next
Status
i Status: Ready
Import succeeded for all servers
Import the IdP Metadata Trust File
This step uploads the file acquired from the IdP in the previous manual step to the Collaboration servers.
1)Select the IdP Metadata Trust File
Browse No file selected.
2)Import this file to the Collaboration servers
This action must be successful for at least the Publisher before moving on to the next task in this wizard.
Import IdP Metadata Import succeeded for all servers
Next Cancel

如圖所示,按一下**下一步**,因為已從初始SAML SSO配置頁匯出SP後設資料。

SAML Single Sign-On Configuration
Back Next
Status Image: Status: Ready Image: Status: Ready
Download Server Metadata and install on the IdP Download the metadata trust file from Collaboration servers and manually install it on the IdP server to complete SSO setup. 1)Download the server metadata trust files to local storage Download Trust Metadata File Image: This is a manual step! 2)Log in to your IdP and upload the server metadata trust file. 3)Click Next once you have installed the server metadata on the IdP.
Back Next Cancel

CUCM必須與LDAP目錄同步。嚮導顯示了LDAP目錄中配置的有效管理員使用者。選擇使用者並按 一下**運行SSO測試**,如下圖所示:

SAML Single Sign-On Configuration

Back

Status

9

1 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 on any server for troubleshooting once SSO has been enabled. SSO setup cannot be completed unless this test is successful.

1)Pick a valid username to use for this test

You must already know the password for the selected username. This user must have administrator rights and also exist in the IdP.

Please use one of the Usernames shown below. Using any other Username to log into the IdP may result in administrator lockout.

samlus	er	A
-		-
2)Launc	h SSO test page	
Run S	SSO Test	

Authentication	Required
0	Enter username and password for https://win-jd4ia7ugmrm.adfs.ucce.com
User Name:	samluser
Password:	••••••
	OK Cancel

如圖所示彈出可確認測試已成功。

	SSO Test Succeeded!
Co	ongratulations on a successful SAML SSO configuration test. Please close this window and click "Finish" on the SAML configuration wizard to complete the setup.
	Close
	0

如圖所示,按一下Finish即可完成啟用SSO的組態。

System - Ca	all Routing 💌	Media Resources 💌	Advanced Features *	Device •	Application -	User Management 🔻	Bulk Administra
SAML Single	e Sign-On Co	onfiguration					
de Back	Finish						
Status							
SSO Me	SSO Metadata Test Successful						
┌ Ready to Enable SSO							
Clicking "Finis being update	sh" will completed.	te enabling SSO on a	all the servers in this d	uster. There	e will be a short	t delay while the appli	ications are
To verify the SSO status of each server, check the main SSO Configuration page. Additional testing and manual uploads may be performed from the main page if neccessary.							
Back Fi	inish Cano	cel					

圖中所示的頁面確認SAML SSO啟用進程已在所有伺服器上啟動。

tatus	
SAML SSO enablement process initiated on all servers.	
There will be a short delay while the applications are being updated on each server.	
To verify the SSO status of each server, check the main SSO Configuration page.	

註銷並使用SAML SSO憑據重新登入到CUCM。導航到System >SAML Single Sign On。按一下群 集中其他節點的**運行SSO測試**,如下圖所示:

SAML Single Sign-On							
SSO Mode Cluster wide (One metadat Per node (One metadata fi	ta file per cluster le per node)	. Requires m	nulti-server Tomcat certificate))			
X Disable SAML SSO	Export All Metadat	a 🔞 Upda	ale kiP Metadata File 🧳 Fix.	All Disabled Ser	vers		
SAML Single Sign-On (1)). You can chang I - 3 of 3)	je SSO for R	TMT <u>here.</u>			Row	s per Page 50 🔻
Server Name	SSO Status	Re-Import Metadata	Last Hetadata Import	Export Metadata	Last Metadata Export	SSO Test	
cucm1150.adfs.ucce.com	SAML	N/A	June 21, 2016 9:28:39 PM IST	🏄 File	June 21, 2016 7:46:56 PM IST	Passed - June 21, 2016 9:29:14 PM IST	Run SSO Test
cucm1150sub.adfs.ucce.com	SAML	🔶 IdP	June 21, 2016 9:28:39 PM IST	🏄 File	June 21, 2016 7:46:56 PM IST	Never	Run SSO Test
imp115.adfs.ucce.com	SAML	🔶 IdP	June 21, 2016 9:28:39 PM IST	🏄 File	June 21, 2016 7:46:56 PM IST	Never	Run SSO Test

驗證

使用本節內容,確認您的組態是否正常運作。

確認已啟用SAML SSO的節點的SSO測試成功。導航到System >SAML Single Sign On。成功的 SSO測試顯示「通過」狀態。

ware ongie orgin on							
SO Mode Cluster wide (One metadat Per node (One metadata fi	a file per dus le per node)	ster. Requires n	nulti-server Tomcat certificate)	1			
🗙 Disable SAML SSO 👔 I	Export All Meta	idata 🔞 Upd	iate IdP Metadata File 🥜 Fix /	All Disabled Ser	vers		
Status	You can ch	ange SSO for R	TMT bere.				
RTMT is enabled for SSO SAML SSO enabled SAML Single Sign-On (1)	t - 3 of 3)	Re Innest		Email		Rows	s per Page 50 💌
SAML SSO enabled SAML SSO enabled SAML Single Sign-On () Server Name	t - 3 of 3) SSO Status	Re-Import Metadata	Last Metadata Import	Export Metadata	Last Metadata Export	Rows SSO Te	s per Page SD ▼ est
SAML SSO enabled SAML SSO enabled SAML Single Sign-On (1 Server Name cucm1150.adfs.ucce.com	t - 3 of 3) SSO Status SAML	Re-Import Metadata N/A	Last Metadata Import June 20, 2016 9:57:30 AM IST	Export Metadata	Last Metadata Export June 20, 2016 10:06:27 PM IST	Rows SSO Te Passed - June 20, 2016 9:59:02 PM IST	s per Page SD ▼ est Run SSO Test
ATMT is enabled for SSO SAML SSO enabled SAML Single Sign-On (1 Server Name cucm1150.adfs.ucce.com cucm1150sub.adfs.ucce.com	t - 3 of 3) SSO Status SAML SAML	Re-Import Metadata N/A	Last Metadata Import June 20, 2016 9:57:30 AM IST June 20, 2016 10:15:46 PM IST	Export Metadata La File	Last Metadata Export June 20, 2016 10:06:27 PM IST June 20, 2016 10:06:26 PM IST	Rows SSO Te Passed - June 20, 2016 9:59:02 PM IST Passed - June 20, 2016 10:11:39 PM IST	s per Page 50 • est Run SSO Test Run SSO Test

啟用SAML SSO後,CUCM登入頁面將列出已安裝應用程式和平台應用程式,如下圖所示。



Platform Applications

- Disaster Recovery System
- Cisco Unified Communications OS Administration

啟用SAML SSO後,系統會為IM and Presence登入頁列出已安裝應用程式和平台應用程式,如下 圖所示:

Installed Applications

- Cisco Unified Communications Manager IM and Presence
 Recovery URL to bypass Single Sign On (SSO)
- Cisco Unified Reporting
- Cisco Unified Serviceability

Platform Applications

- Disaster Recovery System
- Cisco Unified Communications OS Administration

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

若要將SSO日誌設定為調試,請使用命令set samItrace level DEBUG

使用RTMT或使用CLI從activelog /tomcat/logs/ssosp/log4j/*.log位置收集SSO日誌。

SSO日誌的示例顯示了生成的後設資料並傳送到其他節點

2016-05-28 14:59:34,026 DEBUG [http-bio-443-exec-297] cluster.SAMLSSOClusterManager - Call GET API to generate Clusterwide SP Metadata in the Local node. 2016-05-28 14:59:47,184 DEBUG [http-bio-443-exec-297] cluster.SAMLSSOClusterManager - Call to post the generated SP Metadata to other nodes 2016-05-28 14:59:47,185 INFO [http-bio-443-exec-297] cluster.SAMLSSOClusterManager -Begin:postClusterWideSPMetaData 2016-05-28 14:59:47,186 DEBUG [http-bio-443-exec-297] cluster.SAMLSSOClusterManager - Nodes [cucm1150, cucm1150sub.adfs.ucce.com] 2016-05-28 14:59:47,186 DEBUG [http-bio-443-exec-297] cluster.SAMLSSOClusterManager - Post ClusterWideSPMetadata to the cucm1150 2016-05-28 14:59:47,187 DEBUG [http-bio-443-exec-297] cluster.SAMLSSOClusterManager - Post ClusterWideSPMetadata to the cucm1150