使用AD FS版本2.0为每个集群配置单个SAML IdP连接/协议

目录

<u>简介</u> <u>先决条件</u> 要求 使用的组件 背景信息 配置 步骤1.从CUCM导出SP元数据 步骤2.从AD FS下载IDP元数据 步骤3.调配IdP 步骤4.启用SAML SSO 验证 故障排除

简介

本文档介绍如何使用Active Directory联合身份验证服务(AD FS)为每个集群配置单一安全断言标记 语言(SAML)身份提供程序(IdP)连接/协议。

先决条件

要求

Cisco 建议您了解以下主题:

- •思科统一通信管理器(CUCM)11.5或更高版本
- 思科统一通信管理器IM和在线状态版本11.5或更高版本
- Active Directory联合身份验证服务版本2.0

使用的组件

本文档中的信息基于以下软件版本:

- 作为IdP的Active Directory联合身份验证服务版本2.0
- 思科统一通信管理器11.5版
- 思科即时消息和在线状态服务器版本11.5

背景信息

对于SAML SSO,需要是服务提供商(SP)和IdP之间的信任圈。 当交换信任(元数据)时,此信任

会作为SSO启用的一部分创建。 从CUCM下载元数据并将其上传到IdP,同样从IdP下载元数据并将 其上传到CUCM。

在CUCM 11.5之前,始发节点生成元数据文件,也从集群中的其他节点收集元数据文件。 它将所 有元数据文件添加到单个zip文件,然后向管理员显示。管理员必须解压此文件并在IdP上调配每个 文件。例如,8个节点群集的8个元数据文件。

从11.5引入了单个SAML IdP连接/协议每个集群功能。作为此功能的一部分,CUCM为集群中的所 有CUCM和IMP节点生成单个服务提供程序元数据文件。元数据文件的新名称格**式为<hostname>**single-agreement.xml

基本上,一个节点创建元数据并将其推送到群集中的其他SP节点。这可简化调配、维护和管理。例 如,8节点群集的1个元数据文件。

集群范围的元数据文件使用Multiserver tomcat证书,确保密钥对用于集群中的所有节点相同。元数 据文件还包含集群中每个节点的断言使用者服务(ACS)URL列表。

CUCM和思科即时消息和在线状态版本11.5支持SSO模式、**集群范**围(每个集群一个元数据文件)和节点(现有模型)。

本文档介绍如何使用AD FS 2.0配置SAML SSO的集群范围模式。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您使用的是真实网络,请确保您已经了解所有命令的潜在影响。

配置

步骤1.从CUCM导出SP元数据

打开Web浏览器,以管理员身份登录到CUCM,然后导航到System >SAML Single Sign On。

默认情况下,选**择"集群**范围"单选按钮。单击"导**出所有元数据"。**以名称<hostname>-singleagreement.xml向管理**员显示的元数据数据文件**



步骤2.从AD FS下载IDP元数据

要下载IdP元数据,请参阅链接https:// <FQDN of ADFS>/federationmetadata/2007-06/federationmetadata.xml

步骤3.调配IdP

如图所示,导航至AD FS 2.0管理/信任关系发运/信赖方信任。单击"添加信赖方信任"。

🃬 AD F5 2.0			- 0 ×
🙀 File Action View Window Help			_8×
In I			
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		View New Window from Here	•
	1	G Refresh	
		Melp	

"添加信赖方信任向导"(Add Reling Party Trust Wizard)打开,如图所示,现在单击"**开始"**。

📬 Add Relying Party Trus	st 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.	
	CPrevious Start Cancel Help	1

单击有关从文件中信赖方的导入数据。浏览从CUCM SAML SSO配置页下载的SP元数据。然后单 击**Next**,如图所示:

http://www.commons.com/actions/action/actions/action/actio	st Wizard
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 colline or on a local network. Eederation 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. Evelopeiton metadata file location: Evelopeiton metadata file location: Evelopeiton metadata about the relying party manually Use this option to manually input the necessary data about this relying party organization.
	< <u>Previous</u> <u>N</u> ext> Cancel <u>H</u> elp

键入信赖方的显示名称和任何可选注释。单击Next,如图所示:

📬 Add Relying Party Trust	Wizard	×
Specify Display Nam	B	
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

选择**允许所有用户访问此信赖方**以允许所有用户访问此信赖方,然后单击**下一步**,如图所示:

Add Relying Party Trust	: Wizard
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 to relable any users to access this relying party are relying party trust by selecting the relying party trust and clicking Edit Claim Rules in the Actions pane.
	< Previous Next > Cancel Help

在"**准备添加信任"(Ready to Add Trust)页**面下,您可以查看已配置的信赖方信任的设置。现在单击 Next,如图所示:

iteps	The relying party trust has been configured. Review the following settings, and then click Next to add the
Welcome	relying party trust to the AD FS configuration database.
Select Data Source Specify Display Name	Monitoring Identifiers Encryption Signature Accepted Claims Organization Endpoints N.
Authorization Rules	Specify the monitoring settings for this reging 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"页确认信赖方信任已成功添加到AD FS配置数据库。取消选中"Box(框)" ,然后单击 "**Close(关闭)**" ,如图所示:

📬 Add Relying Party Trus	t Wizard	x
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 snap-in.	
	Close]

右键单击"信**赖方信任"**,然后单击"**编辑领款申**请规则",如图所示:

📬 AD FS 2.0			and all the second s		×
🙀 File Action View Window	/ Help				×
AD FS 2.0	Relying Party Trusts			Actions	
E Service	Display Name 💌	Enabled	Identifier	Relying Party Trusts 🔶	-
Claims Provider Trusts	CUCM_Cluster_Wide_Relying_Party_trust	Yes	cucm1150.ad/s.ucce.com	Add Relying Party Trust	
Relying Party Trusts				View	
withbute stores	1			New Window from Here	
	1			G Refresh	
				🕅 Help	
				CUCM_Cluster_Wide_Relying_Party_trust	
	1			Update from Federation Metadata	
	1			Edit Claim Rules	
	1			Disable	
	1			Properties	
	1			🔀 Delete	
9	4			Help	-
	Reality				-

Edit Claim Rules for CUCM_Clust	ter_Wide_Relying_Party_trust Authorization Rules Delegation Authorization F	_ 🗆 🗙 Rules
The following transform rules specify Order Rule Name	the claims that will be sent to the relying party.	1
Add Rule	Remove Rule	
	OK Cancel Apply	Help

当"添**加转换声明规**则"(Add Transform Claim Rule)打开时,单**击使用默**认声明规则模板"**将LDAP属 性作为声明发送"(Send LDAP Attributes as Claims)的"下一步"(Next),如图所示:**

💱 Add Transform Claim R	ule Wizard	×
Select Rule Templat	e	
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:	
	Send LDAP Attributes as Claims	
	Claim rule template description:	
	Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute 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 only send individual group memberships, use the Send Group Membership as a Claim rule template. Tell me more about this rule template]
	<previous next=""> Cancel Help</previous>	

单击**Configure Claim Rule**,如下图所示。LDAP属性必须与CUCM中LDAP目录配置中的LDAP属性 匹配。将传出声明类型管理**为uid**。单击**完成**,如图所示:

🙀 Add Transform Claim R	ule Wizard				×
Configure Rule					
Steps Choose Rule Type Configure Claim Rule	You o which issued Claim Name Rule I	an configure this rule to send the to extract LDAP attributes. Spe d from the rule. rule name: ID emplate: Send LDAP Attributes :	e values of L cify how the as Claims	DAP attributes as claims. Select an attribute store fr attributes will map to the outgoing claim types that v	om nill be
	Attribu	ute store: e Directory	1	•	
	Mapp *	Ing of LDAP attributes to outgoin LDAP Attribute SAM-Account-Name	ig claim type	s: Outgoing Claim Type uid	-
			< Pre	svious Finish Cancel H	elp

为信赖方添加自定义规则。单击**Add rule**。选择**使用自定义规则发送声明**,然后单**击下**一步,如图 所示:

🎁 Add Transform Claim Ri	ule Wizard	×		
Select Rule Templat	e			
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:			
	Send Claims Using a Custom Rule			
	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 from an LDAP attribute store using a custom LDAP filter 			
	Sending claims from a custom attribute store Sending claims only when 2 or more incoming claims are present			
	 Sending claims only when an incoming claim value matches a complex pattern Sending claims with complex changes to an incoming claim value. 			
	Creating claims for use only in later rules			
	Tell me more about this rule template			
	< <u>Previous</u> <u>Next</u> Cancel <u>H</u> elp			

在配置领款申请规则中,键入领款申请规则名称,然后在修改领款申请规则中名称限定符和 spname限定符的向导的"自定义规则"字段中,复制指定和过去的领款申请规则。单击**完成**,如图所 示:

领款申请规则:

```
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,
<pre>Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =</pre>
"urn:oasis:names:tc:SAML:2.0:nameid-format:transient",
<pre>Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"] =</pre>
"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.

teps 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	

如图所示,单击"应用"**,然后单击**"确**定"**。

Order Ru 1 Na 2 Clu	ule Name amelD uster_Side_Claim	_Rule	Issued Claims uid <see claim="" ru<="" th=""><th>le></th></see>	le>
				4
Add Bule	Edit Rule	Remove Ru		

步骤4.启用SAML SSO

打开Web浏览器,以管理员身份登录CUCM,然后导航到System >SAML Single Sign On。 默认情况下,选**择"集群**范围"单选按钮。单击Enable Saml SSO,如图所示:



如图所示,弹出窗口会通知Web服务器重新启动的警告和信息,以根据idp选择集群范围的SAML SSO或每节点SAML SSO。单击 **Continue**。



启用集群范围SSO的条件是必须已部署多服务器Tomcat证书。单击**Test for Multi-Server Tomcat** Certificate(测试多服务器Tomcat证书),如图所示:

SAML Single Sign-On Configuration
Nest .
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

确认后,所有节点的"多服务器证书"(Multi Server Certificate)都会显示"**所有节点都有多服务器证书 "(All Nodes have Multi Server Certificate)**,然后单击**"下一步"(Next),如图所示:**

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
 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 duster
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
如图所示,单击"下一 步" 。

SAML Single Sign-On Configuration	
I Next	
Status	
(i) Status: Ready	
Download Identity provider(IdP) Metadata Trus	: File
To configure the trust relationship between the IdP ar import it to your servers. You will need to manually of servers.	nd your devices, you must first obtain trust metadata from your IdP and otain the file from the IdP before you can upload it to your Collaboration
This is a manual step!	
1)Log in to your IdP and download the metadata trus	t file to your local server.
2)Click Next once you have this file available locally.	

浏览并选择下载的IdP元数据。单击**导入IdP元数据**,如图所示:

SAML Single Sign-On Configuration
Next
Status
(i) Status: Ready
Ready to import Identity Provider metadata trust file to cluster 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 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

该页确认Import succeeded for all servers,然后单击**Next**,如图所示:

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 Vimport succeeded for all servers
Next Cancel

如图所示,单击**Next**,因为已从初始SAML SSO配置页导出SP元数据。

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必须与LDAP目录同步。向导显示在LDAP目录中配置的有效管理员用户。选择用户,然后单 击**运行SSO测**试,如图所示:

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	*
		-
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

弹出窗口(如图所示)确认测试成功。

	SSO Test Succeeded!
Congra clos	atulations on a successful SAML SSO configuration test. Please se this window and click "Finish" on the SAML configuration wizard to complete the setup.
	Close
	D

如图所示,单击**完成**以完成启用SSO的配置。

System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administra
SAML Single Sign-On Configuration
Back Finish
Status SSO Metadata Test Successful
Ready to Enable SSO
Clicking "Finish" will complete enabling SSO on all the servers in this cluster. There will be a short delay while the applications are being updated.
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 Finish Cancel

图中显示的页面确认SAML SSO启用进程在所有服务器上启动。

Status	
SAML SSO enablement process initiated on all servers.	
W 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.	

使用SAML SSO凭证注销并重新登录CUCM。导航至**系统>SAML单点登录。单**击运行**SSO测试以**查 找群集中的其他节点,如图所示:

SAML Single Sign-On							
SSO Mode Cluster wide (One metadat Per node (One metadata fi	ta file per cluster. le per node)	Requires m	ulti-server Tomcat certificate))			
🗙 Disable SAML SSO 🔐 I	Export All Metadata	🔞 Upda	tle kdP Metadata File 🥜 Fix.	All Disabled Sen	vers		
SAML Single Sign-On (1)). You can change t - 3 of 3)	SSO for R	rmt <u>here.</u>			Row	s per Page 50 🔻
Server Name	SSO Status	ke-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

验证

使用本部分可确认配置能否正常运行。

确认已启用SAML SSO的节点的SSO测试成功。导航至**System >SAML Single Sign On**。成功的 SSO测试显示状态已通过。

SAML Single Sign-On							
SSO Mode Cluster wide (One metada Per node (One metadata f	ta file per clu: ile per node)	ster. Requires m	nulti-server Tomcat certificate))			
🗙 Disable SAML SSO 👔	Export All Meta	idata 🔞 Upda	ate IdP Metadata File 🥜 Fix /	All Disabled Ser	vers		
Status TMT is enabled for SSC SAML SSO enabled SAML Single Sign-On (2)). You can ch 1 - 3 of 3)	ange SSO for R	TMT <u>here.</u>			Rows	per Page 50 V
Server Name	SSO Status	Re-Import Metadata	Last Metadata Import	Export Metadata	Last Metadata Export	SSO Test	
cucm1150.adfs.ucce.com	SAML	N/A	June 20, 2016 9:57:30 AM IST	🎂 File	June 20, 2016 10:06:27 PM IST	Passed - June 20, 2016 9:59:02 PM IST	Run SSO Test
cucm1150sub.adfs.ucce.com	SAML	💠 IdP	June 20, 2016 10:15:46 PM IST	🎂 File	June 20, 2016 10:06:26 PM IST	Passed - June 20, 2016 10:11:39 PM IST	Run SSO Test
imp115.adfs.ucce.com	SAML	n Idp	June 20, 2016 10:15:46 PM IST	🎂 File	June 20, 2016 10:06:26 PM IST	Passed - June 20, 2016 10:12:40 PM IST	Run SSO Test
Disable SAML SSO Exp	ort All Metad	ata Update	IdP Metadata File Fix All I	Disabled Serve	rs		

激活SAML SSO后,将为CUCM登录页列出已安装的应用和平台应用,如下图所示。



Platform Applications

- Disaster Recovery System
- Cisco Unified Communications OS Administration

激活SAML SSO后,会为IM and Presence登录页列出Installed Applications和Platform Applications,如下图所示:

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

故障排除

本部分提供的信息可用于对配置进行故障排除。

要将SSO日志设置为调试,请使用命令set samItrace level DEBUG

使用RTMT或从活动日志/tomcat/logs/ssosp/log4j/*.log位置使用CLI收集SSO日志。

SSO日志示例显示生成的元数据并发送到其他节点

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