在(SSO)证书和配置的统一的联络中心企业 (UCCE)单个符号

Contents

Introduction Requirements Components Used 部分A. SSO Message消息流 部分B.在IDP和IDS的Certificates Used 部分C. IDP详细Certification和配置 SSL认证(SSO) 配置SSO的(有签字的内部CA的本地实验室SSL认证的步骤) 令牌的签署的认证 Cisco IDS服务器如何获得令牌的唱歌认证公共密钥? 加密不是启用的 部分D. Cisco IDS边认证 SAML认证

Introduction

本文描述对于UCCE SSO是必需的认证配置。此功能的配置介入HTTPS、数字签名和加密的几证书 。

Requirements

Cisco 建议您了解以下主题:

- UCCE版本11.5
- Microsoft激活目录(AD) -在Windows服务器上安装的AD
- 激活目录联邦服务(ADFS)版本2.0/3.0

Components Used

UCCE 11.5

Windows 2012个R2

部分A. SSO Message消息流



当SSO是启用的,当代理程序登录到精良桌面:

- •精良服务器重定向代理程序浏览器与身份服务(IDS)联络
- IDS重定向代理程序浏览器对身份供应商(IDP)与SAML请求
- IDP生成SAML令牌并且通过对IDS服务器
- 当令牌生成了,在代理程序访问对ppplication时候,使用此有效令牌登录

部分B.在IDP和IDS的Certificates Used



IDP证书

- SSL认证(SSO)
- 令牌的签署的认证
- 令牌--解码

File Action View Window Help 🔿 🔿	3					
AD FS	Certificates					
Service	Subject	Issuer	Effective Date	Expiration Date	Status	Primary
Certificates	Service communications	CN=col115-COL115-CA,	12/30/2016	12/30/2017		
Trust Relationships Claims Provider Trusts Relving Party Trusts	CN=ADFS Encryption - col115dc.col115.org.au	CN=ADFS Encryption - co	12/30/2016	12/30/2017		Primary
Attribute Stores Authentication Policies Per Relving Party Trust	CN=ADFS Signing - col115dc.col115.org.au	CN=ADFS Signing - col11	12/30/2016	12/30/2017		Primary



- SAML认证
- 签名键
- 加密密钥



部分C. IDP详细Certification和配置

SSL认证(SSO)

- •此认证使用在IDP和客户端之间。客户端必须委托SSO认证
- 放置SSL认证加密在客户端和IDP服务器之间的会话。此认证不是特定的对ADFS,然而特定对 IIS
- SSL认证的主题必须与用于ADFS配置的名字配比



配置SSO的(有签字的内部CA的本地实验室SSL认证的步骤)

步骤1.用认证署名请求(CSR)创建SSL认证和符号由ADFS的内部CA。

- 1. 打开服务器管理器。
- 2. 点击工具。
- 3. 点击互联网信息服务(IIS)管理器。
- 4. 选择当地服务器。
- 5. 选择服务器证明。
- 6. 点击开放功能(动作面板)。
- 7. 点击创建证书请求。
- 8. 留下密码服务提供商在默认值。
- 9. 更改比特长度到2048。
- 10. 单击 Next。
- 11. 选择一个位置保存请求的文件。
- 12. 单击 完成。

							_	_	
		• (*)।	ľ.,	Manage	Tools	View	He	lp
	Mindaus Astro		Active Active Active	Directory Directory Directory	y Administra y Domains a y Module fo	ative Center and Trusts or Windows I	Powers	Shell	
Performance counters not started 1/10/2017	12:59:07 PM Not activated		Active Active AD FS ADSI E	Directory Directory Manager dit	y Sites and S y Users and ment	Services Computers			
			Certifie Comp Comp Defrac	cation Au onent Ser uter Man ament an	ithority rvices agement d Optimize	Drives			
			DNS Event Group Interne	Viewer Policy M et Inform	lanagement ation Servic	es (IIS) 6.0 M	lanage	er	

\$ 3	Internet Information Services (IIS) Manager	- 🗆 X
0	4 ► FS01 →	2 🗟 🏠 🔞 -
File View	Request Certificate	<
Start	Cryptographic Service Provider Properties	Request
- <i>i</i> ⊉ A ⊳-iii Si	Select a cryptographic service provider and a bit length. The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance. Cryptographic service provider:	rtificate
	Microsoft RSA SChannel Cryptographic Provider	
	Bit length:	
	2048 V	
	Previous inex raisin Cancer	·
<	III Features View Content View	
Ready		• <u>1</u> .:

步骤2. CA签署从step1生成的CSR。

- 1. 打开CA服务器唱此CSR http://CA服务器IP地址/certsrv/。
- 2. 点击请求认证。
- 3. 点击先进的证书请求。
- 4. 复制CSR到Based-64编码的证书请求。
- 5. 提交。
- 6. 下载签名的证书。

Microsoft Active Directory Certificate Services -- col115-COL115-CA

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your ide communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to v pending request.

For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

Select a task: <u>Request a certificate</u> <u>View the status of a pending certificate request</u> <u>Download a CA certificate, certificate chain, or CRL</u>

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:	
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	
Additional Attributes:	
Attributes:	
	Submit >

步骤3.安装签名的证书回到ADFS服务器并且分配到ADFS功能。

1. 安装签名的证书回到ADFS服务器。为了执行此,请**打开服务器manager>Tools>Click互联网信息** Services(IIS) Manager>。

本地Server>Server Certificate>Open功能(动作面板)。

2. 点击完全证书请求。

3. 选择路径对您从第三方认证供应商完成并且下载的完全CSR文件。

4. 进入认证的友好名称。

5. 选择私有作为证书存储。

6. 单击 Ok。

🕤 📲 🕨 COL115 🕨	Complete Certificate Request ? X
View Help ctions	Specify Certificate Authority Response
Start Page COL115 (COL1150\Adminit Poplication Pools Sites	Complete a previously created certificate request by retrieving the file that contains the certificate authority's response. File name containing the certification authority's response: Friendly name: ADFS Select a certificate store for the new certificate: Personal

7. 在此阶段,所有认证被添加了。现在, SSL需要认证分配。

8. **扩展本地server>Expand Sites>Select默认网站>Click捆绑**(动作面)。

9.Click**添加**。

10. 更改类型到HTTPS。

11. 选择您的认证从下拉菜单。

12. 单击 Ok。

	OL115 🔸	Sites Default Web Site	
View Help		Site Bindings ? X	
ections Start Page COL115 (COL1 COL15 (COL15 (Type http https	Add Site Binding Type: IP address: Port: https All Unassigned 443 Host name: Require Server Name Indication	issi ing lica al (
		SSL certificate: Not selected View OK Cancel	Vet 90 () 643

现在,ADFS服务器的SSL认证分配。

Note:在ADFS功能的安装时,必须使用早先SSL认证。

令牌的签署的认证

ADFS生成令牌的签署的认证的自签证书。默认情况下它是有效在一年内。

IDP生成的SAML令牌由ADFS专用密钥(令牌的签署的认证专用部分)烧焦。然后, IDS使用ADFS公 共密钥验证。这保证签字的令牌不是获得修改。

用户需要获得访问到一个取决于的当事人应用程序每次使用的令牌的签署的认证(Cisco IDS)。

🐑 File Action View Window Help	Certificate
	General Details Certification Path
AD FS Certificates Certificates Certificates Claim Descriptions Claims Provider Trusts Claims Provider Trusts Attribute Stores Attribute Stores Per Relying Party Trust CN=ADFS Signing - col115dc.col115.org.au CN=ADFS Signing CN=ADFS S	Certificate Information This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store. Issued to: ADFS Signing - collistic.collis.org.au Issued by: ADFS Signing - collistic.collis.org.au Valid from 12/30/2016 to 12/30/2017 Install Certificate Issuer Statement

Cisco IDS服务器如何获得令牌的唱歌认证公共密钥?

这由加载ADFS元数据到IDS服务器,然后通过ADFS的公共密钥完成对IDS服务器。这样, IDS获 取ADFS服务器公共密钥。

您需要从ADFS**下载**IDP元数据。为了下载IDP元数据,请参见链路https:// ADFS>/federationmetadata/2007-06/federationmetadata.xml <FQDN。

	54	
	85	
	86	- <keydescriptor use="signing"></keydescriptor>
l	87 88	
l	89 90	- <keyinfo xmlns="http://www.w3.org/2000/09/xmldsig#"></keyinfo>
l	91 92 93	- <x509data></x509data>
	94	<pre><x509certificate>MIIC6DCCAdCgAwIBAgIQFpYJVa99CK9LN50rMdF5nDANBgkqhkiG9w0BAQ#FADAwMS4wLAYDVQQDEyVBREZTIFNpZ25pbmcgLSBjb2wxMTVkYy5jb2wxMTVk 4XDTE2MTIzMDAxMDMyOFoXDTE3MTIzMDAxMDMyOFowMDEuMCwGAJUEAxM1QURGUyBTaWduaW5nIC0gY29sMTE1ZGMuY29sMTE1Lm9yZy5hdTCCASIwDQYJWcZIhwcNAQEBBQADggE gEBAKfeys1epEkwWapH4gIB2hG+h1z+zhbjwS49Ja7FXMUPN3HIMBOCBMNB5fFIddqSQD/wlot4+2kks6povXjNpzfuUMU7tqge1kWDBLoSKuZE70UzDHdg6HwW2HX0KWSj+1v1h wmcAndreskyKeys1epEkwWapH4gIB2hG+h1z+zhbjwS49Ja7FXMUPN3HIMBOCBMNB5fFIddqSQD/wlot4+2kks6povXjNpzfuUMU7tqge1kWDBLoSKuZE70UzDHdg6HwW2HX0KWSj+1v1h wmcAndreskyKeys1epEkwWapH4gIB2hG+h1z+zhbjwS49Ja7FXMUPN3HIMBOCBMNB5fFIddqSQD/wlot4+2kks6povXjNpzfuUMU7tqge1kWDBLoSKuZE70UzDHdg6HwW2HX0KWSj+1v1h wmcAndreskyKeys1epEkwWapH4gIB2hG+h1z+zhbjwS4gJa7FXMUPN3HIMBOCBMNB5fFIddqSQD/wlot4+2kks6povXjNpzfuUMU7tqge1kWDBLoSKuZE70UzDHdg6HwW2HX0KWSj+1v1h wmcAndreskyKeys1epEkwWapH4gIB2hG+h1z+zhbjwS4gJa7FXMUPN3HIMBOCBWNB5fFIddqSQD/wlot4+2kks6povXjNpzfuUMU7tqge1kWDBLoSKuZE70UzDHdg6HwW2HX0KWSj+1v1h wmcAndreskyKeys1epEkwWapH4gIB2hG+h1z+zhbjwS4gJa7FXMUPN3HIMBOCBWNB5fFIddq5D/wlot4+2kks6povXjNpzfuUMU7tgge1kWDBLoSKuZE70UzDHdg6HwW2HX0KWSj+1v1h wmcAndreskyKeys1epEkwWapH4gIB2hG4h1z+zhbjwS4gJa7FXMUPN3HMAGCBWAJASKANG4AMAGANAGYFFIAMTANAGKANG4AMAGANAGYFFIAMTANAGKANG4AMAGANAGANAGANAGANAGANAGANAGANAGANAGANAG</x509certificate></pre>
Ŵ	A	DFS元数据



加载ADFS元数据到IDS **令牌的解密**

此认证由ADFS服务器自动地生成(自已签署的)。如果令牌需要加密, ADFS使用IDS公共密钥解码 它。但是,当您看到ADFS令牌dcrypting时,不意味着令牌被加密。

IDOICPTI WITCOW	Δ						
\$		AD FS					
输 File Action View Window Help							
🗢 🔿 🙍 📰 🛛 🖬							
ad FS	Certificates						Actions
⊿ Service	Subject	Issuer	Effective Date	Expiration Date	Status	Primary	Certificates
Certificates	Service communications						Add Token-
Claim Descriptions	CN=col115dc.col115.org.au, OU=TAC, O=Cisco	CN=col115-COL115-CA,	12/30/2016	12/30/2017			Add Token
4 📑 Trust Relationships	roken-decrypting						
Claims Provider Trusts	CN=ADFS Encryption - col115dc.col115.org.au	CN=ADFS Encryption - co	12/30/2016	12/30/2017		Primary	Set Service 0
📔 Relying Party Trusts	Token signing						View
Attribute Stores	CN=ADFS Signing - col115dc.col115.org.au	CN=ADFS Signing - col11	12/30/2016	12/30/2017		Primary	New Windo
Authentication Policies Per Relving Party Trust							C Refresh
							Help
							CN=col115do
							View Certifie

如果要发现令牌的加密是否为一个特定取决于的当事人应用程序是启用的,您需要检查在一个特定 取决于的当事人应用程序的Encryption选项。

此镜像显示,令牌的加密不是启用的。

• 🔿 🖄 📰 🔢 🖬		
AD FS	Relying Party Trusts	
 Service Endpoints Certificates Claim Descriptions Trust Relationships Claims Provider Trusts Relying Party Trusts Attribute Stores Authentication Policies 	Display Name Device Registration col115idspub.col11!	Enabled Type Identifier coll15idspub.coll15.org.au Properties Organization Endpoints Proxy Endpoints Notes Advanced Monitoring Identifiers Encryption Signature Accepted Claims Specify the encryption certificate for this relying party trust. Encryption certificate: Issuer: Issuer: Subject: Effective date: Expiration date: Browse View Remove

加密不是启用的

部分D. Cisco IDS边认证

- SAML认证
- 加密密钥
- 签名键

SAML认证

此认证是由IDS服务器生成的(自已签署的)。默认情况下它是有效在3年内。

Identity Servi	ce Management	administ
Nodes	\$	
Notes	nary Node	
Node	Status	SAML Certificate Expiry
col115idspub	.col115.org.au 🗙 🔹 In Service	• 12-14-2019 18:58 (930 days left)
Settings File Action View Window AD FS Service Endpoints	Col115idspub.col115.org.au Properties	General Details Certification Path
Certificates Claim Descriptions Trust Relationships Claims Provider Trusts Relying Party Trusts Attribute Stores Authentication Policies	Subject Issuer Effective Date Expiration CN=col115ids CN=col115idspu 12/14/2016 6:5 12/14/2	This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.
Per Keying Party Hust		Issued to: col115idspub.col115.org.au Issued by: col115idspub.col115.org.au Valid from 12/14/2016 to 12/14/2019
	Add View Remove	Install Certificate Issuer Statement

此认证用于签署SAML请求,并且发送到IDP (ADFS)。此公共密钥在IDS元数据,并且必须导入 ADFS服务器。

1.Download SAML从IDS服务器的SP元数据。

2. 对https:// <ids服务器FQDN>:8553/idsadmin/的Broswer。

3. 选择设置和下载SAML SP元数据并且保存它。

🗲 🛈 🔒 https://coll15idspub.coll15.org.au/3553/idsedmin/Main.jsp#/	Settings C Q Search	
Identity Service Management		administ
Settings	IdS Trust	Security Troubleshooting
Nodes Settings	$\overline{\forall}$	
8	Download SAML SP Metadata	
Clients Begin configure Server (idS) by to configure true	ng the trust relationship between the Identity Provider(IdP) and the Id obtaining a SAML SP metadata file from the IdS Server. Use this me st relationship in Identity Provider (IdP).	lentity tadata file
	Download Metadata File	
		Next
 元数据从IDS服务器导入		
<pre><?xml version="1.0" encoding="UTF-8"?> <entitydescriptor -="" <keydescriptor="" entityid="col115idspub.col115.org <SPSSODescriptor protocolSupportEnumeration=" urr="" use="signing"></entitydescriptor></pre>	au" xmlns="urn:oasis:names:tc:SAML:2.0:metadata"> n:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSigne 'g/2000/09/xmldsig#"> gAwIBAgIEWD4KtDANBgkqhkiG9w0BAQUFADAlMSMw1 eFw0xNjEyMTQwNzU4MjVaFw0xOTEyMTQwNzU4MjVaM	id="true" AuthnRequestsSigned="true"> QYDVQQDExpjb2wxMTVpZHNw ICUxIzAhBgNV

BAMTGmNvbDExNWlkc3B1Yi5jb2wxMTUub3JnLmF1MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB

40	Add Relying Party Trust Wizard						
Select Data Source							
Steps	Select an option that this wizard will use to obtain data about this relving party;						
 Welcome 							
Select Data Source	Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.						
 Configure Multi-factor Authentication Now? 							
 Choose Issuance Authorization Rules 	rederation metadata address (nost name or UNL):						
Ready to Add Trust	Example: fs.contoso.com or https://www.contoso.com/app						
 Finish 	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:						
	Browse						
	O Enter data about the relying party manually						
	Use this option to manually input the necessary data about this relying party organization.						

到ADFS服务器

· · · · · · · · · · · · · · · · · · ·	1010	
File Action View Window	col115idspub.col115.org.au Properties	Certificate
AD FS	Organization Endpoints Proxy Endpoints Notes Advanced	General Details Certification Path
Endpoints Certificates	Specify the signature verification certificates for requests from this relying party.	Certificate Information
Claim Descriptions Trust Relationships Claims Provider Trusts Relying Party Trusts Attribute Stores	Subject Issuer Effective Date Expiration CN=col115ids CN=col115idspu 12/14/2016 6:5 12/14/2	This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.
📔 Per Relying Party Trust		Issued to: col115idspub.col115.org.au
		Issued by: col115idspub.col115.org.au
		Valid from 12/14/2016 to 12/14/2019
	< III >	
	Add View Remove	Instal Certificate Issuer Statement
	OK Cancel Apply	

AD F

从ADFS边验证

当IDS重新生成时进行元数据交换的SAML认证这一用于签署SAML请求。

加密/签名键

默认情况下加密没有被启用。如果加密是启用的,需要被加载到ADFS。

col115idspub.col115.org.au P	roperties					
Organization Endpoints Proxy Endpoints	Notes Advanced					
Monitoring Identifiers Encryption Signatu	Ire Accepted Claims					
Specify the encryption certificate for this relying party trust.			AD	FS		
Encryption certificate:						
Issuer:	Select an Encryption Certificate					
Subject: Effective date:	⊚ ⊚ ∞ ↑ 🍺	« Windows	► ADFS ►	~ ¢	Search ADFS	م
Expiration date:	Organize 👻 New f	older				· 🔟 🔞
Browse View Remove	😭 Favorites	^ Nam	e		Date modified	Туре
	Desktop		ar		8/23/2013 1:39 AM	File folde
	🐌 Downloads	🔒 t	og		8/23/2013 1:39 AM	File folde
	🖳 Recent places		5		8/23/2013 1:39 AM	File folde
		📄 🔒 d	da		8/23/2013 1:39 AM	File folde
	🌉 This PC	= 🔒 d	de		8/23/2013 1:39 AM	File folde
	膧 Desktop	📄 🔒 e	el		8/23/2013 1:39 AM	File folde
	Documents	📄 🔒 e	en		12/30/2016 11:59	File folde
	🗼 Downloads	🔋 🔒 e	en-US		12/30/2016 11:59	File folde
	🐌 Music	🔋 🔒 e	5		8/23/2013 1:39 AM	File folde
ОК С) Pictures	— 🔒 e	et		8/23/2013 1:39 AM	File folde
	📑 Videos	🛛 🔒 f	i		8/23/2013 1:39 AM	File folde
	📷 Local Disk (C:)	📃 🔒 f	r		8/23/2013 1:39 AM	File folde
	🖆 DVD Drive (D:) I	R ~ <				>
		File name:		~	Certificate Files (*.cer;*.s	sst;*.p7t ∨
					Open	Cancel

Referecne :

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/icm_enterprise/i cm_enterprise_11_5_1/Configuration/Guide/UCCE_BK_U882D859_00_ucce-featuresguide/UCCE_BK_U882D859_00_ucce-features-guide_chapter_0110.pdf