# Kerberos与ADFS 2.0的最终用户SAML SSO的 Jabber配置示例

### 目录

<u>简介</u> <u>先决条件</u> <u>要求用的组件</u> <u>背景置</u> <u>验</u>障排除

## 简介

本文档介绍如何使用Active Directory联合身份验证服务(ADFS)2.0配置Kerberos。

## 先决条件

#### 要求

本文档没有任何特定的要求。

#### 使用的组件

本文档不限于特定的软件和硬件版本。

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。

## 背景信息

最终用户安全断言标记语言(SAML)单点登录(SSO)配置要求配置Kerberos,以便允许最终用户 SAML SSO用于Jabber使用域身份验证。使用Kerberos实施SAML SSO时,轻量目录访问协议 (LDAP)处理所有授权和用户同步,而Kerberos管理身份验证。Kerberos是一种身份验证协议,旨在 与启用LDAP的实例结合使用。 在加入Active Directory域的Microsoft Windows和Macintosh计算机上,用户可以无缝登录Cisco Jabber,而无需输入用户名或密码,甚至看不到登录屏幕。未登录其计算机上的域的用户仍会看到 标准登录表单。

由于身份验证使用从操作系统传递的单个令牌,因此无需重定向。令牌根据已配置的密钥域控制器 (KDC)进行验证,如果该令牌有效,则用户登录。

#### 配置

以下是使用ADFS 2.0配置Kerberos的步骤。

- 1. 在计算机上安装Microsoft Windows Server 2008 R2。
- 2. 在同一台计算机上安装Active Directory域服务(ADDS)和ADFS。
- 3. 在安装了Microsoft Windows Server 2008 R2的计算机上安装Internet信息服务(IIS)。
- 4. 为IIS创建自签名证书。
- 5. 将自签名证书导入IIS,并将其用作HTTPS服务器证书。
- 6. 在另一台计算机上安装Microsoft Windows7并将其用作客户端。

将域名服务器(DNS)更改为安装ADDS的计算机。

将此计算机添加到您在安装ADDS时创建的域。

转到"**开始**"。右键单击Computer。单击 Properties。单击窗口右侧的**更改设置**。单击 Computer Name 选项卡。单击 Change。添加您创建的域。

				the second se	A CONTRACTOR OF THE OWNER OWNER OF THE OWNER	rasnaikii Seare
System Properties		8	<ul> <li>User Management</li> </ul>	t      Bulk Administration	Help 👻	
Computer Name/Domain Ch	hanges 🔜	ote				
You can change the name and computer. Changes might affect More information	the membership of this ct access to network resources.	mputer				
Computer name:		y/s	Security   System	• • • •	Search Control Pane	
JabberPC1			asis information	about your computer		€ â
Full computer name: JabberPC1.mangolab.com			s edition	about your computer		
Member of Domain: mangolab.com Workgroup:	More	: ID	tows 7 Professional rright © 2009 Microso ce Pack 1 nore features with a n	ft Corporation. All rights res	erved.	<b>~</b>
	OK Cancel		ig: essor: lled memory (RAM):	System rating is not availab Intel(R) Xeon(R) CPU E7- 28 2.00 GB	ble 870 @ 2.40GHz 2.40 Gi	Hz
	OK Cancel	Apply	em type:	64-bit Operating System		
		_	and Touch:	No Pen or Touch Input is a	vailable for this Display	
out Cisco Unified Commun		Compu	ter name, domain, and	workgroup settings		
Support please visit our ]		Co	mputer name:	JabberPC1	9	Change settings
		Ful	computer name:	JabberPC1.mangolab.com		
		Co	mputer description:	JabberPC1		
	See also	Do	main:	mangolab.com		
	Action Center	Windo	ws activation			
	Windows Update	Wir	ndows is activated			ask for .
	Performance Information and Tools	Pro	duct ID: 00371-221-876	7124-86146 Change produ	uct key	genuine

7. 检查Kerberos服务是否在两台计算机上生成。

以管理员身份登录到服务器计算机并打开命令提示符。然后执行以下命令:

cd \windows\System32Klist票



以域用户身份登录到客户端并执行相同的命令。

:\Users\rashaikh>cd \windows\System32
:\Windows\System32>Klist tickets
Aurrent LogonId is 0:0x558ba
ached Tickets: <5>
Olient: rashaikh @ MANGOLAB.COM Server: krbtgt/MANGOLAB.COM @ MANGOLAB.COM KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96 Ticket Flags Øx60a00000 -> forwardable forwarded renewable pre_authent Start Time: 12/10/2014 18:35:23 (local> End Time: 12/11/2014 4:34:59 (local> Renew Time: 12/17/2014 18:34:59 (local> Session Key Type: AES-256-CTS-HMAC-SHA1-96
1> Client: rashaikh @ MANGOLAB.COM Server: krbtgt/MANGOLAB.COM @ MANGOLAB.COM KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96 Ticket Flags 0x40e00000 -> forwardable renewable initial pre_authent Start Time: 12/10/2014 18:34:59 (local> End Time: 12/11/2014 4:34:59 (local> Renew Time: 12/17/2014 18:34:59 (local> Session Key Type: AES-256-CTS-HMAC-SHA1-96
2> Client: rashaikh @ MANGOLAB.COM Server: LDAP/win2k8.mangolab.com/mangolab.com @ MANGOLAB.COM KerbIicket Encryption Type: AES-256-CIS-HMAC-SHA1-96 Ticket Flags 0x40a40000 -> forwardable renewable pre authent ok as deleg
te Start Time: 12/10/2014 19:05:15 (local) End Time: 12/11/2014 4:34:59 (local) Renew Time: 12/17/2014 18:34:59 (local) Session Key Type: AES-256-CTS-HMAC-SHA1-96
Client: rashaikh @ MANGOLAB.COM Server: HITP/win2k8.mangolab.com @ MANGOLAB.COM KerbIicket Encryption Type: AES-256-CTS-HMAC-SHA1-96 Ticket Flags 0x40a40000 -> forwardable renewable pre_authent ok_as_deleg
Start Time: 12/10/2014 18:35:23 (local) End Time: 12/11/2014 4:34:59 (local) Renew Time: 12/17/2014 18:34:59 (local) Session Key Type: AES-256-CIS-HMAC-SHA1-96
M4> Client: rashaikh @ MANGOLAB.COM Server: LDAP/win2k8.mangolab.com @ MANGOLAB.COM KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96 Ticket Flags Øx40a40000 -> forwardable renewable pre_authent ok_as_deleg
te Start Time: 12/10/2014 18:35:05 (local) End Time: 12/11/2014 4:34:59 (local) Renew Time: 12/17/2014 18:34:59 (local) Session Key Type: AES-256-CTS-HMAC-SHA1-96
::\Windows\System32>

#### 8. 在安装ADDS的计算机上创建ADFS Kerberos标识。

Microsoft Windows管理员以<domainname>\administrator的身份登录到Microsoft Windows域 (例如在Microsoft Windows域控制器上),创建ADFS Kerberos标识。ADFS HTTP服务必须 具有名为服务主体名称(SPN)的Kerberos身份,格式如下

: HTTP/DNS\_name\_of\_ADFS\_server。

此名称必须映射到代表ADFS HTTP服务器实例的Active Directory用户。使用Microsoft Windows **setspn**实用程序,该实用程序在Microsoft Windows 2008 Server上应默认可用。 步骤 注册ADFS服务器的SPN。在Active Directory域控制器上,运行setspn命令。

例如,当ADFS主机为**adfs01.us.renovations.com**,而Active Directory域为 US.RENOVES.COM时,命令为:

setspn -a HTTP/adfs01.us.renovations.com

SPN的HTTP/部分适用,即使ADFS服务器通常由安全套接字层(SSL)(即HTTPS)访问。

使用setspn命令检查是否已正确创建ADFS服务器的SPN并查看输出。

setspn -L



9. 配置Microsoft Windows客户端的浏览器设置。

导航至"工具">"Internet选项">"高级"以启用集成Windows身份验证。

#### 选中启用集成Windows身份验证复选框:

Internet Options
General Security Privacy Content Connections Programs Advanced
Settings
Allow active content from CDs to run on My Computer* Allow active content to run in files on My Computer* Allow software to run or install even if the signature is inv. Block unsecured images with other mixed content Check for publisher's certificate revocation Check for server certificate revocation* Check for signatures on downloaded programs Check for signatures on downloaded programs Do not save encrypted pages to disk Empty Temporary Internet Files folder when browser is ck Fnable DOM Storage Fnable Integrated Windows Authentication* Enable Integrated Windows Authentication* Enable native XMLHTTP support Enable SmartScreen Filter *Takes effect after you restart Internet Explorer
Restore advanced settings
Reset Internet Explorer settings Resets Internet Explorer's settings to their default Condition. You should only use this if your browser is in an unusable state.
OK Cancel Apply

导航至工具> Internet选项>安全>本地Intranet >自定义级别……以便选择仅在Intranet区域中自动登录。

Internet Options	- 🖴 🗟 さ 🗙 🚓 Cisco Unified Serviceability 🛛 🛛
General       Security       Privacy       Content       Connections       Programs       Advanced         Select a zone to view or change security settings.       Image: Content View or change security settings.       Image: Content View or change security settings.         Internet       Local intranet       Trusted sites       Restricted sites         Internet       Local intranet       Trusted sites       Restricted sites         Image: Content View of this zone       This zone is for all websites that are found on your intranet.       Sites         Security level for this zone       Allowed levels for this zone       Allowed levels for this zone         Allowed levels for this zone       Allowed levels for this zone       Allowed levels for this zone         Allowed levels for this zone       Allowed levels for this zone       Allowed levels for this zone         Allowed levels for this zone       Allowed levels for this zone       Allowed levels for this zone         Allowed levels for this zone       Allowed levels for this zone       Allowed level to the to the this zone intranet         Image: Allowed level for this zone       Allowed level to the t	asso Cisco Unified Serviceability       ×         curity Settings - Local Intranet Zone       ×         Settings       Disable       >         Enable       Enable       >         Scripting of Java applets       Disable       >         Disable       Enable       >         Enable       Prompt       >         User Authentication       >       >         Automatic logon       Automatic logon only in Intranet zone       >         Automatic logon with current user name and password       >       >         *Takes effect after you restart Internet Explorer       >       >         Reset to:       Medium-kow (default)       Reset       OK       Cancel

导航至**工具> Internet选项>安全>本地Intranet >站点>高级**,以便将入侵检测和防御 (IDP)URL添加到本地Intranet站点。

**注意:**选中Local intranet对话框中的所有复选框,然后单击Advanced**选项卡**。

Internet Options   General Security Privacy Content Connections Programs Advance	S3 - ■ ≅ C × atto Cisco Unified Serviceability ×
Select a zone to view or change security settings.	Local intranet E3
Security level for this zone Allowed levels for this zone: All 	What are intranet settings?       Advanced       OK       Cancel         Local intranet       Image: Concel       Ima
OK Cancel Apply	Require server verification (https:) for all sites in this zone

导航至**工具>安全>受信任站点>站点**,以便将CUCM主机名添加到受信任站点:

Internet Options 💡 👪	
Convert Security Design Context Converting Designed Advanced	→ B B C X O sso-44.com X
General Seconcy Privacy Content Connections Programs Advanced	
Select a zone to view or change security settings.	Trusted sites
Internet Local intranet Trusted sites Restricted sites	You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.
Trusted sites Stee	Add this website to the zone:
<ul> <li>This zone contains websites that you trust not to damage your computer or your files.</li> </ul>	Websites:
You have websites in this zone.	https:// CUCM1.domainname.com Remove
Security level for this zone	https:// CUCM2.domainname.com
Allowed levels for this zone: All	2.5
Medium     Reports before developeing aptentially upgafe	
Content     C	Require server verification (https:) for all sites in this zone
Enable Protected Mode (requires restarting Internet Explorer)	Close
Custom level Default level	and local country laws governing import, export, transfer and use. De
Pecet all soper to default level	with U.S. and local country laws. By using this product you agree to co
Reset al zones to deraut rever	und at our Export Compliance Product Rep
	ur <u>Unified Communications System Docum</u> Loading, please
OK Cancel Apply	

## 验证

本节介绍如何验证使用的身份验证(Kerberos或NT LAN Manager(NTLM)身份验证)。

- 1. 将Fiddler工<u>具下载</u>到您的客户机并安装它。
- 2. 关闭所有 Internet Explorer 窗口。
- 3. 运行Fiddler工具,并检查File菜单下是否启用了Capture Traffic选项。

Fiddler充当客户端计算机和服务器之间的传递代理并侦听所有流量,这会临时设置Internet Explorer设置,如下所示:

Local Area	Network (L	AN) Settings	in and	23		
Automa Automa use of r Auto Use	Automatic configuration Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration. Automatically detect settings Use automatic configuration script					
Proxy s Use dial-	a proxy serv up or VPN co	er for your LAN (These settings will n nnections).	not app	ly to		
		the second second				
Servers	Туре	Proxy address to use	F	Port		
	HTTP:	127.0.0.1	:	8888		
	Secure:	127.0.0.1	:	8888		
	FTP:		:			
	Socks:		:			
	🔲 Use the	same proxy server for all protocols				
Exception	ons					
5	Do not use	proxy server for addresses beginnin	g with:			
	<-loopbac	k>		<u>^</u>		
	Use semicol	ons (;) to separate entries.				

- 4. 打开Internet Explorer,浏览到您的客户关系管理(CRM)服务器URL,然后单击几个链接以生 成流量。
- 5. 返回Fiddler主窗口,选择结果为200(成功)的帧之一:

Fidd	ler Web D	lebugger				
File E	dit Rule	ts Tools	View Help GET /b	oook 🔛 GeoEdge		
Q 4	Replay 🕻	K- 🕨 Go	🗣 Stream 🎉 Deco	ode   Keep: All sessions = 🕀 Any Proces	15 👫 Find 📓 Save 1 🎼 🔗 🏉 Browse 🔹 🔆 Clear Cache 🎢 TextWizard 🛛 🔛 Tearoff 🛛 MSDN Search	
	Result	Protocol	Host	URL ^	🕐 Statistics 🕌 Inspectors 🦸 AutoResponder 🧭 Composer 🔲 Niters 🔳 Log 🚍 Timeline	
01	200	HTTP	www.default-searc	/?sid=476baid=1000itype=n6wer=1307;	Headers TextWew WebForms HexWew Auth Cookies Raw JSON XNL	
492	200	HTTP	www.default-searc	/?sid=4768aid=1008itype=n6wer=1307:	No Proxy-Authorization Header is present.	
M 3	200	HTTP	Tunnel to	vos-cm35.sso-44.com/443	buthorization Header (Negotiate) appears to contain a Kerberos ticket:	
<24	200	HTTPS	vos-cm35.sso-44.com	/		-
55	302	HTTPS	vos-cm35.sso-44.com	/conadmin/showHome.do	30 82 06 03 A0 30 30 2E 06 09 2A 86 48 82 F7 12 0 00* H +.	
56	302	HTTPS	vos-cm35.sso-44.com	/ssosp/sami/login?relayurl=%2Fccmadnir	28 06 01 04 01 82 37 02 02 1E 06 0A 28 06 01 04 + 7+	
曲7	200	HTTP	Tunnel to	vos-cm44.sso-44.com/443	01 02 37 02 02 0A A2 02 05 CD 04 02 05 C9 60 02 . 74 .IE 05 C5 06 09 2A 86 48 86 F7 12 01 02 02 01 00 6E .A* H +n	
58	302	HTTPS	vos-cm44.sso-44.com	/adfs/is/?SAMLRequest=nVLLbtswELznKv	82 05 84 30 82 05 80 A0 03 02 01 05 A1 03 02 01 .'0 .*	
2 9	401	HTIPS	vosicm44.ssp.44.com	ladisikia thintee atedi?SAM Requester	04 3A 30 82 04 36 A0 03 02 01 05 A1 0C 18 0A 53 .:0 .6	
10	200	HTTPS	vos-cm44.sso-44.com	/adfs/k/auth/integrated/?SAMLRequestr	53 4F 20 34 34 2E 43 4F 40 A2 26 30 24 A0 03 02 90-44.COM4A05	
(f) 11	200	HTTP	Tunnel to	vos-cm35.sso-44.com:8443	73 20 63 60 34 34 2E 73 73 6F 20 34 34 2E 63 6F s-cm44.sso-44.co	
2012	302	HTTPS	vos-cm35.sso-44.c	/ssosp/sani/S50/alias/vos-cm35.sso-44.4	60 A3 92 03 F7 30 92 03 F3 A0 03 02 01 17 A1 03 m6 .+0 .0	
5 13	302	HTTPS	vos-cn35.sso-44.c	(ssosp(relay	aa 13 na ad 20 9a n9 63 68 66 69 n5 67 dn n8 d1 3 11 8 76 "Na	•
<>14	200	HTTPS	vos-cm35.sso-44.c	/conadmin/showHome.do	Get SyntaxNew Transformer Hooders TextNew ImageNew HexNew WebMew Auth Co	aching
曲 15	200	HTTP	Tunnel to	vos-cm35.sso-44.com/8443	Cookies Raw ISON XML	- 1
<u>m</u> 16	200	HTTP	Tunnel to	vos-cm35.sso-44.com/8443		_
曲 17	200	HTTP	Tunnel to	vos-cm35.sso-44.com:8443	Response Headers [Raw] Header Detro	ions]
m 18	200	HTTP	Tunnel to	vos-cm35.sso-44.com:8443	HTTP/1.1 200 0K	
m 19	200	HTTP	Tunnel to	vos-cm35.sso-44.com:8443	Cache	-
<u>m</u> 20	200	HTTP	Tunnel to	vos-cm35.sso-44.com:0443	Cache-Control: no-cache	
m 21	200	HTTP	Tunnel to	vos-cm35.sso-44.com:8443	Date: Fri, 25 Jul 2014 13:07:58 GMT	
4	300	UTTR	Tunnelin	100 m3E ma A4 man.9445	Expres: -1	-
DOM: NO	ect ALT+0	) s hype HEI	P		<	•
111						
E Capt	uning	<ul> <li>Al Proces</li> </ul>	ses 1/30	https://vos-cm44.sso-44.com/adfs/is/au	Atvintegrated(754MLRequest=nkLLDtswEL2nkwTeFVqWDEL/EZcONEdRA2IR20Nva3qVEXBUJU67d%2BALh6wWBOHrqguh	IMEST /

如果身份验证类型为NTLM,则在帧的开头看到**协商 — NTLMSSP**,如下所示:

🕑 Statistics 🔛 Inspectors 🚿 AutoResponder 🗳 Request Builder 🔲 Filters 🗉 Log 🚍 Timeline
Headers TextView WebForms HexView Auth Raw XML
No Proxy-Authorization Header is present.
Authorization Header is present: Negotiate
4E 54 4C 4D 53 53 50 00 03 00 00 18 00 18 00 NTLMSSP
78 00 00 00 18 00 18 00 90 00 00 00 10 00 10 00 x
48 00 00 00 10 00 10 00 58 00 00 00 10 00 10 00 HX
68 00 00 00 00 00 00 A8 00 00 05 82 88 A2 h ¢
05 01 28 0A 00 00 00 0F 49 00 4E 00 54 00 57 00(I.N.T.W.

# 故障排除

目前没有针对此配置的故障排除信息。