Exemplo de Kerberos com ADFS 2.0 para SAML SSO de usuário final para configuração Jabber

Contents

Introduction Prerequisites Requirements Componentes Utilizados Informações de Apoio Configuração Verificar Troubleshoot

Introduction

Este documento descreve como configurar o Kerberos com o Ative Diretory Federation Services (ADFS) 2.0.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informações de Apoio

A configuração do SSO (Single Sign On, login único) SAML (End User Security Assertion Markup Language) exige que o Kerberos seja configurado para permitir que o SSO SAML do usuário final para o Jabber trabalhe com autenticação de domínio. Quando SAML SSO é implementado com

Kerberos, o Lightweight Diretory Access Protocol (LDAP) manipula toda a autorização e a sincronização do usuário, enquanto Kerberos gerencia a autenticação. Kerberos é um protocolo de autenticação que deve ser usado em conjunto com uma instância habilitada para LDAP.

Em máquinas Microsoft Windows e Macintosh que estão associadas a um domínio do Ative Diretory, os usuários podem fazer login no Cisco Jabber sem precisar inserir um nome de usuário ou senha e nem mesmo ver uma tela de login. Os usuários que não estão conectados ao domínio em seus computadores ainda veem um formulário de login padrão.

Como a autenticação usa um único token passado dos sistemas operacionais, não é necessário redirecionamento. O token é verificado em relação ao KDC (Key Domain Controller) configurado e, se for válido, o usuário está conectado.

Configuração

Este é o procedimento para configurar Kerberos com ADFS 2.0.

- 1. Instale o Microsoft Windows Server 2008 R2 em uma máquina.
- 2. Instale os Serviços de Domínio do Ative Diretory (ADDS) e o ADFS na mesma máquina.
- 3. Instale o Internet Information Services (IIS) na máquina instalada do Microsoft Windows Server 2008 R2.
- 4. Crie um certificado autoassinado para o IIS.
- 5. Importar o certificado autoassinado para o IIS e usá-lo como certificado do servidor HTTPS.
- 6. Instale o Microsoft Windows7 em outra máquina e use-o como um cliente.

Altere o Domain Name Server (DNS) para a máquina onde você instalou o ADDS.

Adicione esta máquina ao domínio criado na instalação do ADDS.

Vá para **Start (Iniciar)**.Clique com o botão direito do mouse em **Computador**.Clique em Propriedades.Clique em **Alterar configurações** no lado direito da janela.Clique na **guia Nome do computador**.Clique em **Alterar**.Adicione o domínio criado.

		rasnaikn s
ystem Properties	8	✓ User Management ▼ Bulk Administration ▼ Help ▼
Computer Name/Domain Changes	ote	
You can change the name and the membership of this computer. Changes might affect access to network resources. More information	mputer	
Computer name:	y/s	Security
JabberPC1		ania information about your computer
Full computer name: JabberPC1 mangolab.com		s edition
More Member of © Domain:	: ID	right © 2009 Microsoft Corporation. All rights reserved. ce Pack1
mangolab.com	9 e	nore features with a new edition of Windows 7
OK Cancel		rg: System rating is not available essor: Intel(R) Xeon(R) CPU E7- 2870 @ 2.40GHz 2.40 GHz
		Iled memory (RAM): 2.00 GB
OK Cancel	Apply	em type: 64-bit Operating System
		and Touch: No Pen or Touch Input is available for this Display
Cisco Unified Commun	Comp	puter name, domain, and workgroup settings
pport please visit our]	Co	Computer name: JabberPC1 @Change settings
	Ful	full computer name: JabberPC1.mangolab.com
	Co	Computer description: JabberPC1
See also	Do	Domain: mangolab.com
Action Center	Windo	dows activation
Windows Update	Wi	Windows is activated
Performance Information an Tools	d Pro	Product ID: 00371-221-8767124-86146 Change product key Settinare

7. Verifique se o serviço Kerberos é gerado em ambas as máquinas.

Faça login como administrador na máquina do servidor e abra o prompt de comando. Em seguida, execute estes comandos:

cd \windows\System32Bilhetes Klist

C:\Users	s\Administrator.WIN2K8>cd \windows\System32
C:\Windo	ows\System32>Klist tickets
Current	LogonId is 0:0x3d6072
Cached I	lickets: <1>
#0>	Client: Administrator @ MANGOLAB.COM Server: krbtgt/MANGOLAB.COM @ MANGOLAB.COM KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96 Ticket Flags Øx40e00000 -> forwardable renewable initial pre_authent Start Time: 12/10/2014 18:06:04 (local) End Time: 12/11/2014 4:06:04 (local) Renew Time: 12/17/2014 18:06:04 (local) Session Key Type: AES-256-CTS-HMAC-SHA1-96

Faça login como usuário de domínio na máquina cliente e execute os mesmos comandos.

:\Users\rashaikh>cd \windows\System32
:\Windows\System32>Klist tickets
Current LogonId is 0:0x558ba
ached Tickets: <5>
Olient: rashaikh @ MANGOLAB.COM Server: krbtgt/MANGOLAB.COM @ MANGOLAB.COM KerbIicket Encryption Type: AES-256-CTS-HMAC-SHA1-96 Ticket Flags 0x60a00000 -> 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
H> 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 KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96 Ticket Flags 0x40a40000 -> forwardable renewable pre_authent ok_as_del
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 KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96 Ticket Flags 0x40a40000 -> forwardable renewable pre_authent ok_as_del
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
4> Client: rashaikh @ MANGOLAB.COM Server: LDAP/win2k8.mangolab.com @ MANGOLAB.COM KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96 Ticket Flags 0x40a40000 -> forwardable renewable pre_authent ok_as_del
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-CIS-HMAC-SHA1-96
:\Windows\System32>

8. Crie a identidade do Kerberos do ADFS na máquina onde você instalou o ADDS.

O administrador do Microsoft Windows fez login no domínio do Microsoft Windows (como <nome do domínio>\administrador), por exemplo no controlador de domínio do Microsoft Windows, cria a identidade do Kerberos do ADFS. O serviço HTTP do ADFS deve ter uma identidade Kerberos chamada Nome do Principal do Serviço (SPN - Service Principal Name) neste formato: HTTP/DNS_name_of_ADFS_server.

Esse nome deve ser mapeado para o usuário do Ative Diretory que representa a instância

do servidor HTTP do ADFS. Use o utilitário **setspn** do Microsoft Windows, que deve estar disponível por padrão em um Microsoft Windows 2008 Server.

Procedimento Registre os SPNs para o servidor ADFS. No controlador de domínio do Ative Diretory, execute o comando **setspn**.

Por exemplo, quando o host ADFS é **adfs01.us.renovations.com**, e o domínio do Ative Diretory é **US.RENOVATIONS.COM**, o comando é:

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

A parte **HTTP**/SPN se aplica, mesmo que o servidor ADFS seja normalmente acessado pela SSL (Secure Sockets Layer), que é HTTPS.

Verifique se os SPNs do servidor ADFS foram criados corretamente com o comando **setspn** e veja a saída.

```
setspn -L
```

```
:\Windows\System32>setspn -L win2k8
Begistered ServicePrincipalNames for CN=WIN2K8,OU=Domain Controllers,DC=mangolab
.DC=com:
    HTTP/win2k8.mangolab.com
    ldap/win2k8.mangolab.com/ForestDnsZones.mangolab.com
    ldap/win2k8.mangolab.com/DomainDnsZones.mangolab.com
    Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EEB04/win2k8.mangolab.com
    Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EEB04/win2k8.mangolab.com
    Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EEB04/win2k8.mangolab.com
    Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EEB04/win2k8.mangolab.com
    Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EEB04/win2k8.mangolab.com
    Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EEB04/win2k8.mangolab.com
    Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EEB04/win2k8.mangolab.com
    DKS/win2k8.mangolab.com/mangolab.com
    RestrictedKrbHost/WIN2K8
    HOSI/WIN2K8.mangolab.com/MANGOLAB
    HOSI/WIN2K8.mangolab.com/MANGOLAB
    HOSI/WIN2K8.mangolab.com/mangolab.com
    E3514235-4B06-11D1-AB04-00C04FC2DCD2/bf221b06-fbc5-4dc3-b472-562f9238374
//mangolab.com
    ldap/WIN2K8/MANGOLAB
    ldap/WIN2K8.mangolab.com/MANGOLAB
    ldap/WIN2K8.mangolab.com
    ldap/win2k8.mangolab.com
    ldap/win2k8.mangolab.com
    ldap/win2k8.mangolab.com/mangolab.com
    ldap/win2k8.mangolab.com/mangolab.com
    ldap/win2k8.mangolab.com/mangolab.com
    ldap/win2k8.mangolab.com/mangolab.com
    ldap/win2k8.mangolab.com/mangolab.com
    ldap/win2k8.mangolab.com/mangolab.com
    ldap/win2k8.mangolab.com/mangolab.com
    ldap/win2k8.mangolab.com/mangolab.com
    l
```

9. Defina as configurações do navegador do Microsoft Windows Client.

Navegue até **Ferramentas > Opções da Internet > Avançado** para habilitar a Autenticação Integrada do Windows.

Marque a caixa de seleção Ativar autenticação integrada do Windows:

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 signatures on downloaded programs Do not save encrypted pages to disk Empty Temporary Internet Files folder when browser is ck Fnable DOM Storane 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

Navegue até Ferramentas > Opções da Internet > Segurança > Intranet local > Nível personalizado... para selecionar Logon automático somente na zona Intranet.

Internet Options	- ≜ ≅ C × at Cisco Unified Serviceability ×
General Security Privacy Content Connections Programs Advanced Select a zone to view or change security settings. Image: Content of the security settings. Image: Content of the security settings. Internet Local intranet Trusted sites Restricted sites Internet Local intranet Trusted sites Sites Internet Local intranet Sites Internet Local intranet Sites Internet Trusted sites Sites Internet Local intranet Sites Internet Local intranet Sites Internet Trusted sites sites Sites Internet Proventantent Sites Internet Internet Sites Internet Proventantent Sites Internet Proventante Sites Security level for this zone Allowed levels for this zone Allowed levels for this zone Allowed levels for this zone Allowed levels for the zone Internet Insigned ActiveX controls will not be downloaded Same as Medum level without prompting you Insigned ActiveX con	Security Settings - Local Intranet Zone Settings Enable Enable Enable Scripting of Java applets Disable Enable Scripting of Java applets Disable Enable Enable Frompt User Authentication Logon Automatic logon only in Intranet zone Automatic logon only in Intranet zone Prompt for user name and password Prompt for user name and password Trakes effect after you restart Internet Explorer Reset to: Medium-low (default) Reset OK Cancel

Navegue até Ferramentas > Opções da Internet > Segurança > Intranet Local > Sites > Avançado para adicionar o URL da IDP (Intrusion Detection & Prevention, Detecção e Prevenção de Intrusão) a sites de intranet locais.

Note: Marque todas as caixas de seleção na caixa de diálogo Intranet local e clique na **guia Avançado**.

Internet Options	↔ e a a c × atta Cisco Unified Serviceability ×						
General Security Privacy Content Connections Programs Advance Select a zone to view or change security settings. Internet Internet <th colspan="7">add add Cisco Unified Serviceability × ed add Cisco Unified Serviceability × ed Local intranet Cocal intranet add Cisco Unified Serviceability × Use the settings below to define which websites are included in the local intranet zone. Automatically detect intranet network. Include all local (intranet) sites not listed in other zones Include all sites that bypass the proxy server Include all network paths (UNCs) What are intranet settings? What are intranet add Cancel Local intranet add Cancel</th>	add add Cisco Unified Serviceability × ed add Cisco Unified Serviceability × ed Local intranet Cocal intranet add Cisco Unified Serviceability × Use the settings below to define which websites are included in the local intranet zone. Automatically detect intranet network. Include all local (intranet) sites not listed in other zones Include all sites that bypass the proxy server Include all network paths (UNCs) What are intranet settings? What are intranet add Cancel Local intranet add Cancel						
Appropriate for vebsites on your total intervers Approximate for vebsites on your total intervers Approximate for vebsites on your total intervers Approximate for vebsites on your total intervers Custom level Reset all zones to default level	You can add and remove websites from this zone. All websites in this zone will use the zone's security settings. Add this website to the zone: Add Websites: https:// <hostname idp="" of=""> Remove</hostname>						
OK Cancel Apply	Require server verification (https:) for all sites in this zone						

Navegue até Ferramentas > Segurança > Sites confiáveis > Sites para adicionar os nomes

de host do CUCM a sites confiáveis:

Internet Ontions	
General Security Privacy Content Connections Programs Advanced	
Salast a sana la view ar change convitu sattings	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	Add this website to the zone:
This zone contains websites that you Sites	Add
 trust not to damage your computer or your files. 	Webstes:
tou nave 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 Prompts before downloading potentially unsafe content Unsigned ActiveX controls will not be downloaded	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 with U.S. and local country laws. By using this product you agree to co
Reset all zones to default level	und at our Export Compliance Product Rep
	ur <u>Unified Communications System Docum</u> Loading, please
OK Cancel Apply	

Verificar

Esta seção explica como verificar qual autenticação (autenticação Kerberos ou NT LAN Manager (NTLM) é usada).

- 1. Baixe a Fiddler Tool em sua máquina cliente e instale-a.
- 2. Feche todas as janelas do Internet Explorer.
- 3. Execute a ferramenta Fiddler e verifique se a opção **Capture Traffic** está ativada no menu File (Arquivo).

O Fiddler funciona como um proxy de passagem entre a máquina cliente e o servidor e ouve todo o tráfego, o que temporariamente define suas Configurações do Internet Explorer como esta:

Local Area	Network (LA	N) Settings	-	23								
Automa Automa use of r Auto Use Add	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 Address											
Proxy setting	erver a proxy serve up or VPN con ings	r for your LAN (These settings will no nections).	t app	ly to								
Servers	Type HTTP: Secure: FTP: Socks:	Proxy address to use 127.0.0.1 127.0.0.1 ame proxy server for all protocols	 : (] : (Port 8888 8888								
Exception	Do not use p <-loopback Use semicolo	roxy server for addresses beginning > ns (;) to separate entries.	with:	*								

- 4. Abra o Internet Explorer, navegue até a URL do servidor do CRM (Customer Relationship Management, gerenciamento de relacionamento com o cliente) e clique em alguns links para gerar tráfego.
- 5. Consulte a janela principal do Fiddler e escolha um dos Quadros em que o Resultado é 200

```
(sucesso):
```

🔷 Fid	dler Web D	lebugger				
File	Edit Rule	s Tools	View Help GET /b	ook 🔛 GeoEdge		
94	Replay >	K- 🕨 Go	🔹 Stream 🌆 Deco	ade Keep: All sessions + 🕀 Any Proces	is 👬 Find 😡 Save 📲 🧑 🏉 Browse 🔹 🅀 Clear Cache 🎢 TextWizard 📴 Tearoff 🛛 MSDN Search	
	Result	Protocol	Host	URL	🕐 Statistics 👫 Impactors 🗲 AutoResponder 🎯 Composer 🔲 Niters 🗉 Log 🚍 Timeline	
01	200	HTTP	www.default-searc	Pad=476baid=1000Evpa=ptwar=1307	Headers TextWew WebForms HexWew Auth Cookies Raw 250N XML	
432	200	HTTP	www.default-searc	Rsid=4768aid=1008itype=n6wer=1307.	No Proxy-Authorization Header is present.	
(f) 3	200	HTTP	Tunnel to	vos-cm35.sso-44.com:443		- âl
\$24	200	HTTPS	vos-cm35.sso-44.com	1	Authorization Header (Negotiate) appears to contain a Kerberos ticketi	=
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=%2Fccmadmir	28 06 01 04 01 82 37 02 02 1E 06 0A 28 06 01 04 t 7t.	
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	
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 .*	
29	401	HTTPS	Voc-m44.ssn-44.com	ladicikia thintogratedi?SAM Request-	04 3A 30 92 04 36 A0 03 02 01 05 A1 0C 18 0A 52 .:0 .6	
\$10	200	HTTPS	vos-cm44.sso-44.com	/adfs/is/auth/integrated/?SAMLRequestr	53 4F 20 34 34 2E 43 4F 40 A2 26 30 24 A0 03 02 50-44.COM44.05	
(f) 11	200	HTTP	Tunnelto	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	
2 12	302	HTTPS	vos-cm35.sso-44.c	/ssosp/saml/S50/alias/vos-cm35.sso-44.c	60 A3 92 03 F7 30 92 03 F3 A0 03 02 01 17 A1 03 m6 .+0 .0	
5 13	302	HTTPS	vos-cm35.sso-44.c	/ssosp(relay	a 12 na al 3/ 4a na 22 an al 22 an al 22 an na 21 3 1 3 40 ha	-
<\$14	200	HTTPS	vos-cm35.sso-44.c	/conadmin/showHome.do	Get SyntaxView Transformer Headers TextView ImageWiew HexView WebMew Auth C	aching
曲 15	200	HTTP	Tunnel to	vos-cm35.sso-44.com/8443	Confine Days 19761 Vite	
16	200	HTTP	Tunnel to	vos-cm35.sso-44.com/8443	Contrast Rainy Look Inte	
曲 17	200	HTTP	Tunnel to	vos-cm35.sso-44.com:8443	Response Headers (Raw) Header Detro	lons]
m 18	200	HTTP	Tunnel to	vos-cm35.sso-44.com:8443	HTTP/1.1 200 0K	
19	200	HTTP	Tunnel to	vos-cm35.sso-44.com:8443	Cache	
<u></u> <u> </u> <u> </u> <u> </u> 20	200	HTTP	Tunnel to	vos-cm35.sso-44.com:8443	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	
1 22	200	UTTR	Turned in	100 m3E con 64 com/9445	Expres: -1	-
The second s	Vector T+C	1 s bine HEI	P		4 II	
NR. C						
E Ca	sturing	T AI Proces	sses 1/30	https://vos-cn+t4.sso-t4.com/adfs/ls/au	<pre>Afvintegrated("SAMLRequest=nMLLDtswELznkwTePVqWbEuE2cONEdRA2iR20Nva3qVExB0Uu57d%2BAUh5wW8OHngguh</pre>	IM25

Se o tipo de autenticação for NTLM, você verá **Negotiate - NTLMSSP** no início do quadro, como mostrado aqui:

\otimes	Stat	istics	5	E I	nspe	ctors	s 🔡	51	Autof	Resp	onde	er i	4	Requ	Jest B	Builder		Fi	ters		Log	Timelin	e
Headers TextView WebForms HexView Auth Raw XML																							
No	No Proxy-Authorization Header is present.									Π													
AL	tho	riz a	atio	n H	lead	ler	15	pr	eser	nt:	Neg	ot	iate	•									
146	54	40	4D 00	18	53	18	00	90	00	00	00	18	00	18	00	NTL	ISSP						
48	00	õõ	õõ	10	õõ	10	ŏŏ	58	õõ	õõ	õõ	10	õõ	10	õõ	Ĥ		.x.					
68	00	00	00	00	00	00	00	A8	00	00	00	05	82	88	AZ	h		· _ ·			¢		
105	01	28	0A	00	00	00	OF	49	00	4E	00	54	00	57	00	(.1.	N. 1	.w.	•		

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.