Ejemplo de Configuración de Kerberos con ADFS 2.0 para el Usuario Final SAML SSO para Jabber

Contenido

Introducción Prerequisites Requirements Componentes Utilizados Antecedentes Configuración Verificación Troubleshoot

Introducción

Este documento describe cómo configurar Kerberos con los Servicios de federación de Active Directory (ADFS) 2.0.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

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.

Antecedentes

La configuración de Lenguaje de marcado de aserción de usuario final (SAML) de inicio de sesión único (SSO) requiere la configuración de Kerberos para permitir que el SSO de usuario final SAML para Jabber funcione con la autenticación de dominio. Cuando se implementa SAML SSO con Kerberos, el protocolo ligero de acceso a directorios (LDAP) controla toda la autorización y la sincronización de usuarios, mientras que Kerberos administra la autenticación. Kerberos es un protocolo de autenticación que se pretende utilizar junto con una instancia habilitada para LDAP.

En los equipos Microsoft Windows y Macintosh que se unen a un dominio de Active Directory, los usuarios pueden iniciar sesión de forma fluida en Cisco Jabber sin necesidad de introducir un nombre de usuario o una contraseña y ni siquiera ven una pantalla de inicio de sesión. Los usuarios que no han iniciado sesión en el dominio de sus equipos siguen viendo un formulario de inicio de sesión estándar.

Debido a que la autenticación utiliza un único token pasado desde los sistemas operativos, no se requiere redirección. El token se verifica con el controlador de dominio de clave (KDC) configurado y, si es válido, el usuario inicia sesión.

Configuración

Este es el procedimiento para configurar Kerberos con ADFS 2.0.

- 1. Instale Microsoft Windows Server 2008 R2 en un equipo.
- 2. Instale Active Directory Domain Services (ADDS) y ADFS en el mismo equipo.
- 3. Instale Internet Information Services (IIS) en el equipo instalado en Microsoft Windows Server 2008 R2.
- 4. Cree un certificado autofirmado para IIS.
- 5. Importe el certificado autofirmado en IIS y utilícelo como certificado de servidor HTTPS.
- 6. Instale Microsoft Windows7 en otro equipo y utilícelo como cliente.

Cambie el servidor de nombres de dominio (DNS) a la máquina en la que instaló ADDS.

Agregue esta máquina al dominio que creó en la instalación de ADDS.

Vaya a **Inicio**.Haga clic con el botón derecho del ratón en **Equipo**.Haga clic en Properties (Propiedades).Haga clic en **Cambiar configuración** en el lado derecho de la ventana.Haga clic en la **ficha Nombre del equipo**.Haga clic en **Cambiar**.Agregue el dominio que creó.

		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. Compruebe si el servicio Kerberos se genera en ambos equipos.

Inicie sesión como administrador en el equipo servidor y abra el símbolo del sistema. A continuación, ejecute estos comandos:

cd \windows\System32Entradas de Klist

C:\Users\Administrator.WIN2K8>cd \windows\System32				
C:\Windo	C:\Windows\System32>Klist tickets			
Current	LogonId is 0:0x3d6072			
Cached I	ickets: (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 18:06:04 (local) Renew Time: 12/17/2014 18:06:04 (local) Session Key Type: AES-256-CTS-HMAC-SHA1-96			

Inicie sesión como usuario de dominio en el equipo cliente y ejecute los mismos comandos.

C:\Users\rashaikh>cd \windows\System32
C:\Windows\System32>Klist tickets
Current LogonId is 0:0x558ba
Cached Tickets: <5>
#8> Client: rashaikh @ MANGOLAB.COM Server: krbtgt/MANGOLAB.COM @ MANGOLAB.COM KerbIicket Encryption Type: AES-256-CIS-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-CIS-HMAC-SHA1-96
11> 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_dele
ate 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
43> Client: rashaikh @ MANGOLAB.COM Server: HITP/win2k8.mangolab.com @ MANGOLAB.COM KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96 Ticket Flags Øx40a40000 -> forwardable renewable pre_authent ok_as_dele
Ate 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
44> 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_dele
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-CIS-HMAC-SHA1-96
C:\Windows\System32>

8. Cree la identidad ADFS Kerberos en el equipo donde instaló ADDS.

El administrador de Microsoft Windows inició sesión en el dominio de Microsoft Windows (como <domainname>\administrator), por ejemplo en el controlador de dominio de Microsoft Windows, crea la identidad ADFS Kerberos. El servicio ADFS HTTP debe tener una identidad Kerberos denominada nombre principal de servicio (SPN) con este formato: HTTP/DNS_name_of_ADFS_server.

Este nombre debe asignarse al usuario de Active Directory que representa la instancia del

servidor HTTP de ADFS. Utilice la utilidad **setspan** de Microsoft Windows, que debe estar disponible de forma predeterminada en un servidor de Microsoft Windows 2008.

Procedimiento Registre los SPN para el servidor ADFS. En el controlador de dominio de Active Directory, ejecute el comando **setspan**.

Por ejemplo, cuando el host ADFS es **adfs01.us.renovations.com** y el dominio de Active Directory es **US.RENOVATIONS.COM**, el comando es:

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

Se aplica la parte **HTTP**/ del SPN, aunque el servidor ADFS suele tener acceso a través de Secure Sockets Layer (SSL), que es HTTPS.

Verifique que los SPNs para el servidor ADFS se crean correctamente con el comando **setspan** y vea el resultado.

```
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
    IERMSRU/WIN2K8
    TERMSRU/WIN2K8
    TERMSRU/WIN2K8.mangolab.com
    Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EB04/win2k8.mangolab.com
    Dfs/win2k8.mangolab.com/mangolab.com
    RestrictedKrbHost/WIN2K8
    HOSI/WIN2K8.mangolab.com/MANGOLAB
    HOSI/WIN2K8.mangolab.com/MANGOLAB
    HOSI/WIN2k8.mangolab.com
    HOSI/WIN2k8.mangolab.com
    RestrictedKrbHost/WIN2K8
    HOSI/WIN2k8.mangolab.com
    HoSI/WIN2k8.mangolab.com/mangolab.com
    HoSI/WIN2k8.mangolab.com/mangolab.com
    HoSI/WIN2k8.mangolab.com/mangolab.com
    HoSI/WIN2k8.mangolab.com/mangolab.com
    HoSI/WIN2k8.mangolab.com/mangolab.com
    HoSI/WIN2k8.mangolab.com/mangolab.com
    HoSI/WIN2k8.mangolab.com/mangolab.com
    HoSI/WIN2k8.mangolab.com
    HoSI/WIN2k8.mangolab.com/mangolab.com
    HoSI/WIN2k8.mangolab.com/mangolab.com
    HoSI/WIN2k8.mangolab.com/mangolab.com
    HoSI/WIN2k8.mangolab.com
    HoSI/WIN2k8.mangolab.c
```

9. Configure los parámetros del explorador del cliente de Microsoft Windows.

Navegue hasta **Herramientas > Opciones de Internet > Avanzadas** para habilitar la autenticación integrada de Windows.

Marque la casilla de verificación Habilitar autenticación integrada de 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 server 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 Storage Enable Integrated Windows Authentication* Enable memory protection to help mitigate online attacks* Enable native XMLHTTP support Enable SmartScreen Filter 				
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				

Vaya a Herramientas > Opciones de Internet > Seguridad > Intranet local > Nivel personalizado... para seleccionar Inicio de sesión automático solamente en la zona Intranet.

General Security Privacy Connections Programs Advanced Select a zone to view or change security settings. Internet Security is settings Image: Security Setings Image: Security Settings Image:	Internet Options	- = ≥ C × 🗰 Cisco Unified Serviceability ×
OK Cancel Apply OK Cancel	General Security Privacy Content Connections Programs Advanced Select a zone to view or change security settings. Image: Security and the security settings. Internet Local intranet Trusted sites Restricted sites Internet Local intranet Trusted sites Restricted sites Image: Content will be security level for this zone Stes Stes Security level for this zone Alowed levels for this zone Stes Alowed levels for this zone: Alowed levels for this zone: Stes Security level for this zone Alowed levels for this zone: Stes Image: Alowed levels for this zone: Alowed levels for this zone: Stes Image: Alowed level for this zone: Alowed levels for this zone: Stes Image: Alowed level for this zone: Alowed level for this zone: Stes Image: Alowed level for this zone: Alowed level for this zone: Stes Image: Alowed level for this zone: Alowed level for this zone: Alowed level for this zone: Image: Alowed level for this zone: Alowed level for this zone: Alowed level for this zone: Image: Alowed level for this zone: S	Image: Cisco Unified Serviceability X Recurity Settings - Local Intranet Zone Image: Cisco Unified Serviceability Settings Disable Enable Enable Enable Enable Sorpting of Java applets Disable Disable Enable Sorpting of Java applets Disable Enable Prompt User Authentication Logon Automatic logon only in Intranet zone Automatic logon only in Intranet zone Automatic logon with current user name and password Image: Ciscobility Takes effect after you restart Internet Explorer Reset custom settings Reset to: Medum-low (default) Reset OK Cancel

Navegue hasta Herramientas > Opciones de Internet > Seguridad > Intranet local > Sitios > Avanzado para agregar la URL de Detección y Prevención de Intrusiones (IDP) a sitios de Intranet local.

Nota: Marque todas las casillas de verificación del cuadro de diálogo Intranet local y haga clic en la **ficha Avanzadas**.

General Security Privacy Content Connections Programs Advanced
Select a zone to view or change security settings. Internet Internet Internet Local intranet Internet Coll intranet Internet Coll intranet Internet Restricted sites Internet Stes Intranet Stes Include all local (intranet) sites not listed in other zones Include all sites that bypass the proxy server Include all network paths (LNCs) What are intranet settings? Advanced OK Include all network paths (INCs) What are intranet settings? Add this website to the zone's security settings. Include all zones to default level Reset all zones to default level Internet Add Include server verification (https:) for all sites in this zone
Close

Navegue hasta Herramientas > Seguridad > Sitios de confianza > Sitios para agregar los

nombres de host de CUCM a sitios de confianza:

Internet Options	
General Security Privacy Content Connections Programs Advanced	
Select a zone to view or change security settings.	Trusted sites
Internet Local intranet Trusted sites Restricted	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	Add
your files.	Webstes:
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	
Content Content Unsigned ActiveX controls will not be downloaded	Require server verification (https:) for all sites in this zone
	Chse
Enable Protected Mode (requires restarting Internet Explorer)	
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 c
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	

Verificación

Esta sección explica cómo verificar qué autenticación (Kerberos o NT LAN Manager (NTLM)) se utiliza.

- 1. Descargue la herramienta Fiddler en su equipo cliente e instálela.
- 2. Cierre todas las ventanas de Internet Explorer.
- 3. Ejecute la herramienta Fiddler y verifique que la opción **Capturar tráfico** esté habilitada en el menú Archivo.

Fiddler funciona como proxy de paso entre el equipo cliente y el servidor y escucha todo el tráfico, lo que establece temporalmente los parámetros de Internet Explorer de la siguiente manera:

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 setti	erver a proxy serve up or VPN con ings	r for your LAN (These settings will not nections).	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 v >	with:	*		

- 4. Abra Internet Explorer, busque la URL del servidor de gestión de relaciones con el cliente (CRM) y haga clic en algunos enlaces para generar tráfico.
- 5. Vuelva a la ventana principal de Fiddler y elija una de las tramas donde el resultado es 200 (correcto):

A 54	dia di fata in f	hungar			
V Flor	aler web t	rebugger			
Pile	Edit Ruli	es Tools	View Help GET /E	oook 🔝 GeoEdge	
Q fg	Replay 2	X - 🕨 Go	🛛 🏶 Stream 🦉 Deci	ode 🔰 Keep: All sessions 🔹 🕀 Any Proce	ss 👬 Find 🔣 Save 🎼 🧑 🌽 Browse 🔹 🅀 Clear Cache 🎢 TextWizard 🕼 Tearoff 🛛 MSDN Search 👘
	Result	Protocol	Host	URL	🕐 Statistics 🔀 Inspectors of AutoBessonder 📝 Composer 🔲 Filters 🗉 Log 🚍 Tasine
0	200	HTTP	same defenderener	Date of Web aids 10000 means frame 1207	Headers TectVess WebForms HexVess Auth Cookies Rev 350N XNL
02	200	HTTP	www.defailt.cear	Dokt-1763.ok-10098-me-never-1907	The former of the second
(f) a	200	HTTP	Tunnelito	vis-rm35.ssp-44.rom/443	No Proxy-Ruthorization Header is present.
04	200	HTTPS	vos-cm35.ssp-44.com		Ruthorization Header (Negotiate) appears to contain a Kerberos tickets
N 5	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 +.
16	302	HTTPS	vos-cm35.sso-14.com	issosp/samillogin?relayurl=%2Fccmadmir	01 02 02 06 09 2A 86 48 86 F7 12 01 02 02 06 0A* H + 28 06 01 04 01 82 37 02 02 1E 06 0A 28 06 01 04 +
曲7	200	HTTP	Tunnel to	vos-cm44.sso-44.com/443	01 82 37 02 02 0A A2 82 05 CD 04 82 05 C9 60 82 . 74 .1E
58	302	HTTPS	vos-cm44.sso-44.com	/adfs/is/?SAMLRequest=nVLLbtswELznKy	82 05 84 30 82 05 80 A0 03 02 01 05 A1 03 02 01 . 0.*
2 9	401	HTTPS	unsicred-4, sso-44, com	ladisikia thintegrated 25AM Request-	0E A2 07 03 05 00 20 00 00 00 A3 82 04 3E 61 82
10	200	HTTPS	vos-cm44.sso-44.com	/adfs/k/auth/integrated/?SAMLRequest/	53 4F 20 34 34 2E 43 4F 4D A2 26 30 24 A0 03 02 90-44.COM440\$
(1) 11	200	HTTP	Tunnel to	vos-cm35.sso-44.com:8443	01 02 A1 10 30 18 18 04 48 54 54 50 18 13 76 6P
212	302	HTTPS	vos-cm35.sso-44.c	/ssosp/saml/S50/alias/vos-cm35.sso-44.c	60 A3 82 03 F7 30 82 03 F3 A0 03 02 01 17 A1 03 md .+0 .0
5 13	302	HTTPS	vos-cm35.sso-44.c	(ssosp(relay	44 12 nd 46 27 94 ng 62 65 64 62 65 51 40 65 56 1.11 14 16 16 100
4314	200	HTTPS	vos-cm35.sso-44.c	(conedmin/showhome.do	Get SyntaxView Transformer Headers TextView InaceView HexView WebView Auth Caching
凸 15	200	HTTP	Tunnel to	vos-cm35.sso-44.com/8443	Contine Days 19200 VM
尚 16	200	HTTP	Tunnel to	vos-cm35.sso-44.com/8443	Cookies Kaiv John APE
曲 17	200	HTTP	Tunnel to	vos-cm35.sso-44.com:8443	Response Headers (Haw) Header Detrators)
們 18	200	HTTP	Tunnel to	vos-cm35.eso-44.com:8443	HTTP/1.1 200 0K
(f) 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: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
4	300	UTTR	Tunnelin	ine en3E con 64 com/9442	Expres: -1
DUCIE	escl ALT+0	0 > type HEI	P		×
Will com				the star and an it was to be to	
≘ge Cap	cuning	T AI Proce	sses 1/30	nttps://vos-cn44.sso-44.com/adfs/is/a	utryintegratedy/s4MLHequest=mitLbtsweLankinTeP-vgWoEue2d/DHEdRA2IR/20Nva3gMEXBBUU57d%28RLh6wW8OHngguh7MEs7

Si el tipo de autenticación es NTLM, verá **Negotiate - NTLMSSP** al principio de la trama, como se muestra aquí:

🕑 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 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 HXX
68 00 00 00 00 00 00 A8 00 00 05 82 88 A2 h ¢
05 01 28 0A 00 00 0F 49 00 4E 00 54 00 57 00(I.N.T.W.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.