Esempio di configurazione di Kerberos con ADFS 2.0 per l'utente finale SAML SSO per Jabber

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Premesse Configurazione Verifica Risoluzione dei problemi

Introduzione

In questo documento viene descritto come configurare Kerberos con Active Directory Federation Services (ADFS) 2.0.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

La configurazione di Single Sign-On (SSO) SAML (End User Security Assertion Markup Language) richiede la configurazione di Kerberos per consentire a Jabber di utilizzare l'SSO SAML utente finale per l'autenticazione del dominio. Quando SAML SSO viene implementato con Kerberos, il protocollo LDAP (Lightweight Directory Access Protocol) gestisce tutte le autorizzazioni e la sincronizzazione degli utenti, mentre Kerberos gestisce l'autenticazione. Kerberos è un protocollo di autenticazione da utilizzare in combinazione con un'istanza abilitata per LDAP.

Sui computer Microsoft Windows e Macintosh che fanno parte di un dominio di Active Directory, gli utenti possono accedere senza problemi a Cisco Jabber senza dover immettere un nome utente o una password e non visualizzano neanche una schermata di accesso. Gli utenti che non hanno effettuato l'accesso al dominio sui propri computer continuano a visualizzare un modulo di accesso standard.

Poiché l'autenticazione utilizza un singolo token passato dai sistemi operativi, non è necessario alcun reindirizzamento. Il token viene verificato rispetto al controller di dominio chiave (KDC) configurato e, se è valido, l'utente ha eseguito l'accesso.

Configurazione

Di seguito viene riportata la procedura per configurare Kerberos con ADFS 2.0.

- 1. Installare Microsoft Windows Server 2008 R2 in un computer.
- 2. Installare Servizi di dominio Active Directory (ADDS) e ADFS nello stesso computer.
- 3. Installare Internet Information Services (IIS) nel computer in cui è installato Microsoft Windows Server 2008 R2.
- 4. Creare un certificato autofirmato per IIS.
- 5. Importare il certificato autofirmato in IIS e utilizzarlo come certificato del server HTTPS.
- 6. Installare Microsoft Windows7 in un altro computer e utilizzarlo come client.

Modificare il DNS (Domain Name Server) nel computer in cui è stato installato ADDS.

Aggiungere il computer al dominio creato durante l'installazione di ADDS.

Vai a **Start**.Fare clic con il pulsante destro del mouse su **Computer**.Fare clic su **Proprietà**.Fare clic su **Cambia impostazioni** sul lato destro della finestra.Fare clic sulla **scheda Nome computer**.Fare clic su **Cambia**.Aggiungere il dominio creato.

		Pashalkit Sc
System Properties		User Management Bulk Administration Help
Computer Name/Domain Changes	exe ote	
You can change the name and the membership of the computer. Changes might affect access to network More information	resources.	
Computer name:	n/s	Security System Security Securit
JabberPC1		
Full computer name: JabberPC1.mangolab.com	More	s edition lows 7 Professional
Member of © Domain: mangolab.com © Workgroup:	20	rright © 2009 Microsoft Corporation. All rights reserved. ce Pack 1 nore features with a new edition of Windows 7
ок (Cancel Apply	g: System rating is not available essor: Intel(R) Xeon(R) CPU E7- 2870 @ 2.40GHz led memory (RAM): 2.00 GB m type: 64-bit Operating System and Touch: No Pen or Touch logit is available for this Display.
Cisco Unified Commun		
upport please visit our]	Co	mputer name, domain, and workgroup settings
		Computer name: JabberPC1 Change settings
		Full computer name: JabberPCL mangolab.com
		Computer description: Jabber/CI
See also		Domain: mangolab.com
Action Center	Wi	ndows activation
Windows Updat	te	Windows is activated
Performance In Tools	formation and	Product ID: 00371-221-8767124-86146 Change product key

7. Verificare se il servizio Kerberos viene generato in entrambi i computer.

Accedere come amministratore sul computer server e aprire il prompt dei comandi. Eseguire quindi i seguenti comandi:

cd \windows\System32Biglietti Klist



Accedere come utente di dominio sul computer client ed eseguire gli stessi comandi.

C:\Users\rashaikh>cd \windows\System32
::\Windows\System32>Klist tickets
Current LogonId is 0:0x558ba
Cached Tickets: <5>
#0> Client: rashaikh @ MANGOLAB.COM Server: krbtgt/MANGOLAB.COM @ MANGOLAB.COM KerbTicket 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
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 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
te 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
t4> 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_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. Creare l'identità Kerberos ADFS nel computer in cui è installato ADDS.

L'amministratore di Microsoft Windows ha eseguito l'accesso al dominio di Microsoft Windows (come <nomedominio>\amministratore), ad esempio nel controller di dominio di Microsoft Windows, e crea l'identità Kerberos ADFS. Il servizio HTTP ADFS deve disporre di un'identità Kerberos denominata nome dell'entità servizio (SPN) nel formato seguente: HTTP/nome_DNS_del_server_ADFS.

Questo nome deve essere mappato all'utente di Active Directory che rappresenta l'istanza

del server HTTP ADFS. Utilizzare l'utilità **setspn di** Microsoft Windows, che dovrebbe essere disponibile per impostazione predefinita in un server Microsoft Windows 2008.

Procedura Registrare gli SPN per il server ADFS. Eseguire il comando **setspn** nel controller di dominio Active Directory.

Ad esempio, quando l'host ADFS è **adfs01.us.renovations.com** e il dominio di Active Directory è **US.RENOVATIONS.COM**, il comando è:

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

Viene applicata la parte HTTP/SPN, anche se al server ADFS si accede in genere tramite SSL (Secure Sockets Layer), ovvero HTTPS.

Verificare che gli SPN per il server ADFS siano stati creati correttamente con il comando **setspn** e visualizzare l'output.

```
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.mangol
```

9. Configurare le impostazioni del browser del client di Microsoft Windows.

Per abilitare l'autenticazione integrata di Windows, selezionare **Strumenti > Opzioni Internet > Avanzate**.

Selezionare la casella di controllo Abilita autenticazione integrata di 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 DON Storage 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

Selezionare Strumenti > Opzioni Internet > Protezione > Intranet locale > Livello personalizzato per selezionare Accesso automatico solo nell'area Intranet.

Internet Options Internet Options Image: Content I Connections Image: Connections <th< th=""><th>→ 을 클 Ĉ × 🗰 Cisco Unified Serviceability ×</th></th<>	→ 을 클 Ĉ × 🗰 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. Select a zone to view or change security settings. Image: Content view or change security settings. Internet Cocal intranet Trusted sites Restricted sites Internet Local intranet Trusted sites Restricted sites Internet Local intranet Trusted sites Restricted sites Internet Local intranet Trusted sites Sites Internet Local intranet Trusted sites Restricted sites Internet Local intranet Trusted sites Rest al zones to default level Internet Local intranet Trusted sites Sites Internet Image: Cocal intranet Sites Sites Security level for this zone Allowed levels for this zone: All Image: Cocal intranet Sites Image: Cocal intranet Image: Cocal intranet Ima	Image: Construction of the service ability X Security Settings - Local Intranet Zone Image: Construction of the service ability Settings Disable Image: Construction of the service ability Image: Construction of the service ability Settings Disable Image: Construction of the service ability Image: Construction of the service ability Image: Construction of the service ability Image: Construction of the service ability Image: Construction of the service ability Image: Construction of the service ability Image: Construction of the service ability Image: Construction of the service ability Image: Construction of the service ability Image: Construction of the service ability Image: Construction of the service ability
OK Cancel Apply	OK Cancel

Selezionare **Strumenti > Opzioni Internet > Sicurezza > Intranet locale > Siti > Avanzate** per aggiungere l'URL di Rilevamento e prevenzione intrusioni (IDP) ai siti Intranet locali.

Nota: Selezionare tutte le caselle di controllo nella finestra di dialogo Intranet locale e fare clic sulla **scheda Avanzate**.

Internet Options 2 2 General Security Privacy Content Connections Programs Advanced	
Select a zone to view or change security settings.	Local intranet E3
Security level for this zone Allowed levels for this zone: All Meclium-low 	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

Per aggiungere i nomi host CUCM ai siti attendibili, selezionare **Strumenti > Protezione > Siti** attendibili > Siti:

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	You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.
Trusted sites This zone contains websites that you Sites	Add this website to the zone:
 trust not to damage your computer or your files. You have websites in this zone. 	Websites:
Security level for this zone	https:// CUCM1.domainname.com https:// CUCM2.domainname.com
Allowed levels for this zone: All	2.5
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	

Verifica

Questa sezione spiega come verificare quale autenticazione (Kerberos o NTLM) viene utilizzata.

- 1. Scaricare lo strumento Finder sul computer client e installarlo.
- 2. Chiudere tutte le finestre di Internet Explorer.
- 3. Eseguire lo strumento Trova e verificare che l'opzione **Cattura traffico** sia attivata nel menu File.

Fiddler funge da proxy pass-through tra il computer client e il server ed è in ascolto di tutto il traffico, che imposta temporaneamente le impostazioni di Internet Explorer nel modo seguente:

Local Area	Network (LA	AN) Settings	-	23
Automa Automa use of r Auto Use Add	tic configuration tic configuration manual setting omatically deter automatic con	ion ion may override manual settings. To gs, disable automatic configuration. ect settings nfiguration script	ensu	re the
Proxy s Use dial-	erver a proxy serve up or VPN cor ings	er for your LAN (These settings will no nnections).	t app	ly to
Servers	Type HTTP: Secure: FTP: Socks:	Proxy address to use 127.0.0.1 127.0.0.1 same proxy server for all protocols		Port 8888 8888
Exception	Do not use p <-loopback	proxy server for addresses beginning k> ons (;) to separate entries.	with:	*

- 4. Aprire Internet Explorer, individuare l'URL del server CRM e fare clic su alcuni collegamenti per generare traffico.
- 5. Fate riferimento alla finestra principale del Finder e scegliete uno dei fotogrammi in cui il risultato è 200 (esito positivo):

O Ed	dier Weit 1	lehugger				
(1) (1)	Line Deal	Teele	Mana Hala OFT 6	and the second		
Pile	East Pul	es 10015	view Help OET /	ooos Buil Geoedge		
Q 4	Replay 7	X - 🕨 Go	🗣 Stream 🌆 Deci	ode 🔰 Keep: All sessions 👻 🕀 Any Proces	s 🌺 Find 🔜 Save 📲 🕐 🏉 Browse 🔹 🅀 Clear Cache 🎢 TextWizard 🕼 Tearoff 🛛 MSDN Search	
	Result	Protocol	Host	URL ^	🕐 Statistics 👫 Inspectors 🗲 AutoResponder 🧭 Composer 🔲 Niters 🗉 Log 🚍 Timeline	
01	200	HTTP	www.default-searc	Pad=476baid=1000type=ctwar=1307;	Headers TextMew WebForms HexNew Auth Cookies Raw JSON XNL	
492	200	HTTP	www.default-searc	/rsid=4768aid=1008itype=n6wer=1307:	No Proxy-Authorization Header is present.	
(ff) 3	200	HTTP	Tunnel to	vos-cm35.sso-44.com:443		5 H
\$24	200	HTTPS	vos-cm35.sso-44.com	1	Authorization Header (Negotiate) appears to contain a Kerberos ticketi	ē
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 .1E	
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	uncirretti.ssa-tti.com	ladisikia thintercatedi?SAM 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/ls/auth/integrated/?SAMLRequestr	53 4F 20 34 34 2E 43 4F 40 A2 26 30 24 A0 03 02 50-44.CON46.05	
(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-cm44.550-44.Co	
2 12	302	HTTPS	vos-cm35.sso-44.c	/ssosp/sami/S50/alias/vos-cm35.sso-44.c	60 A7 92 07 F7 70 92 07 F7 A0 07 02 01 17 A1 07 mt .+0 .0	
5 13	302	HTTPS	vos-cm35.sso-44.c	(ssosp(relay	aa 17 na ad 20 9a ne 67 ee dd 6e no eo en ne di 3 1 8 44 'Na	•
\$\$14	200	HTTPS	vos-cm35.sso-44.c	/conedmin/showttome.do	Get SyntaxWew Transformer Hooders TextView InageWew HexMew WebMew Auth Cachin-	-
曲 15	200	HTTP	Tunnel to	vos-cm35.sso-44.com/8443	Contries Days 1900 190	11
16	200	HTTP	Tunnel to	vos-cm35.sso-44.com/8443	Contrast Contrast and Contrast	-1
曲 17	200	HTTP	Tunnel to	vos-cm35.sso-44.com:8443	Response Headers (Raw) Header Detrotoria	
m 18	200	HTTP	Tunnel to	vos-cm35.sso-44.com:8443	HTTP/1.1 200 OK	
<u>m</u> 19	200	HITTP	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: Fit, 25 Jul 2014 13:07:58 GMT	
1 22	100	- UTTIN	Tunnelin	100 m36 m 44 m 9443	Express •1	-
DUCK	esc] ALT+I	0 > type HEI	P		۲ <u>ا</u>	
Mile of				Alternations and any of some table to be		-
E Cap	curing	T Al Proce	sses 1/30	netps://vos-cm44.sso-44.com/adfs/ls/ac	anymoograadog vseval noquest – nivillatiswellanikin teP vojwaleuezachie drikaziin zahvaa over Baluus 7d%28s0.hSwiw90Hingguh7Masi	11

Se il tipo di autenticazione è NTLM, all'inizio del frame viene visualizzato **Negotiate - NTLMSSP**, come mostrato di seguito:

🕑 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.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.