Jabber 컨피그레이션을 위한 최종 사용자 SAML SSO용 ADFS 2.0이 포함된 Kerberos 예

목차

<u>소개</u> <u>사전 요구 사항</u> <u>요구 사항</u> <u>사용되는 구성 요소</u> <u>배경 정보</u> <u>구성</u> <u>다음을 확인합니다.</u> <u>문제 해결</u>

소개

이 문서에서는 ADFS(Active Directory Federation Services) 2.0을 사용하여 Kerberos를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

SAML(End User Security Assertion Markup Language) SSO(Single Sign On) 구성을 사용하려면 Jabber용 최종 사용자 SAML SSO가 도메인 인증과 작동하도록 Kerberos를 구성해야 합니다 .SAML SSO가 Kerberos와 함께 구현되면 LDAP(Lightweight Directory Access Protocol)는 모든 권 한 부여 및 사용자 동기화를 처리하며 Kerberos는 인증을 관리합니다.Kerberos는 LDAP 지원 인스 턴스와 함께 사용할 인증 프로토콜입니다.

Active Directory 도메인에 가입된 Microsoft Windows 및 Macintosh 시스템에서 사용자는 사용자 이 름 또는 비밀번호를 입력하지 않고도 Cisco Jabber에 원활하게 로그인할 수 있으며 로그인 화면도 볼 수 없습니다.컴퓨터의 도메인에 로그인하지 않은 사용자도 표준 로그인 양식을 볼 수 있습니다.

인증은 운영 체제에서 전달된 단일 토큰을 사용하므로 리디렉션이 필요하지 않습니다.구성된 KDC(Key Domain Controller)에 대해 토큰이 확인되며, 유효한 경우 사용자가 로그인됩니다.

구성

다음은 ADFS 2.0으로 Kerberos를 구성하는 절차입니다.

- 1. 컴퓨터에 Microsoft Windows Server 2008 R2를 설치합니다.
- 2. ADDS(Active Directory Domain Services) 및 ADFS를 동일한 컴퓨터에 설치합니다.
- 3. Microsoft Windows Server 2008 R2 설치 컴퓨터에 IIS(인터넷 정보 서비스)를 설치합니다.
- 4. IIS용 자체 서명 인증서를 만듭니다.
- 5. 자체 서명 인증서를 IIS로 가져와 HTTPS 서버 인증서로 사용합니다.
- 6. 다른 컴퓨터에 Microsoft Windows7을 설치하고 클라이언트로 사용합니다.

DNS(Domain Name Server)를 ADDS를 설치한 시스템으로 변경합니다.

ADDS 설치에서 만든 도메인에 이 컴퓨터를 추가합니다.

시작으로 **이동합니다.컴퓨터**를 마우스 오른쪽 단추로 클릭합니다.속성**을 클릭합니다**.창 오른 쪽에서 Change Settings를 클릭합니다.**컴퓨터 이름 탭**을 클릭합니다.**변경**을 **클릭합니다**.생성 한 도메인을 추가합니다.

					the second s	rasnalki Scarc
System Properties		8	User Management	t + Bulk Administration +	Help 👻	
Computer Name/Domain Cl	hanges 🗾	ote				
You can change the name an computer. Changes might affer More information	d the membership of this ct access to network resources.	mputer				
Computer name:			Security System	• •	Search Control Pan	el P
JabberPC1			asis information	about your computer		• • • •
Full computer name: JabberPC1.mangolab.com			s edition	about your computer		
Member of © Domain: mangolab.com © Workgroup:	More	: ID	Iows 7 Professional rright © 2009 Microso ce Pack 1 nore features with a n	ft Corporation. All rights rese ew edition of Windows 7	rved.	<i>**</i>
	OK Cancel		ig: essor: lied memory (RAM):	System rating is not availab Intel(R) Xeon(R) CPU E7- 28 2 00 GB	ie 70 @ 2.40GHz 2.40 0	iHz E
	OK Cancel	Apply	em type:	64-bit Operating System		
		5	and Touch:	No Pen or Touch Input is a	ailable for this Displa	y III
out Cisco Unified Commun		Comm	ter name domain and	workeroup cattings		
Support please visit our		Compt	mer name, domain, and	labbarDC1		Change settings
		Ful	computer name:	JabberPC1 mangolab.com		Change settings
		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	e Pro	duct ID: 00371-221-876	7124-86146 Change produ	ct key	Genuine

7. Kerberos 서비스가 두 컴퓨터에서 생성되는지 확인합니다.

서버 시스템에서 관리자로 로그인하고 명령 프롬프트를 엽니다.그런 다음 다음 명령을 실행합니다.

cd \windows\System32Klist 티켓

C:\Users\Administrator.WIN2K8>cd \windows\System32					
C:∖Windo	C:\Windows\System32>Klist tickets				
Current	LogonId is 0:0x3d6072				
Cached 1	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 4:06:04 (local) Renew Time: 12/17/2014 18:06:04 (local) Session Key Type: AES-256-CTS-HMAC-SHA1-96				

클라이언트 시스템에서 도메인 사용자로 로그인하고 동일한 명령을 실행합니다.

C:\Users\rashaikh>cd \windows\System32
C:\Windows\System32>Klist tickets
Current LogonId is 0:0x558ba
Cached Tickets: <5>
#0> 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
42> Client: rashaikh @ MANGOLAB.COM Server: LDAP/win2k8.mangolab.com/mangolab.com @ MANGOLAB.COM KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96 Ticket Flags @x40a4000 -> forwardable renewable pre authent ok as deleg
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
#3> 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_deleg ate
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 0x40a40000 -> forwardable renewable pre_authent ok_as_deleg
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
C:\Windows\System32>

8. ADDS를 설치한 컴퓨터에 ADFS Kerberos ID를 만듭니다.

Microsoft Windows 도메인(예: Microsoft Windows 도메인 컨트롤러)에 로그인한 Microsoft Windows 관리자는 ADFS Kerberos ID를 생성합니다.ADFS HTTP 서비스에는 다음 형식의 SPN(서비스 사용자 이름)이라는 Kerberos ID가 있어야 합니다 .**HTTP/DNS_name_of_ADFS_server**.

이 이름은 ADFS HTTP 서버 인스턴스를 나타내는 Active Directory 사용자에게 매핑되어야 합 니다.Microsoft Windows 2008 Server에서 기본적으로 사용할 수 있는 Microsoft Windows setspn 유틸리티를 사용합니다.

절차 ADFS 서버의 SPN을 등록합니다.Active Directory 도메인 컨트롤러에서 setspn 명령을 실행합니다.

예를 들어 ADFS 호스트가 adfs01.us.renoverations.**com이고** Active Directory 도메인이 US.REFRESH.COM인 경우 명령은 다음과 같습니다.

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

SPN의 HTTP/부분은 HTTPS인 SSL(Secure Sockets Layer)에서 일반적으로 ADFS 서버에 액 세스하지만 적용됩니다.

setspn 명령을 사용하여 ADFS 서버의 SPN이 제대로 만들어졌는지 확인하고 출력을 봅니다.

setspn -L



9. Microsoft Windows 클라이언트의 브라우저 설정을 구성합니다.

통합 Windows 인증을 **활성화하려면 Tools > InternetOptions > Advanced**로 이동합니다.

Enable Integrated Windows Authentication 확인란을 선택합니다.

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 Integrated Windows Authentication* Enable native XMLHTTP support Enable SmartScreen Filter *Takes effect after you restart Internet Explorer
Destore advanced celtings
Reset Internet Explorer settings Resets Internet Explorer's settings to their default Reset You should only use this if your browser is in an unusable state.
OK Cancel Apply

인트라넷 영역에서 자동 로그온만을 선택하려면 도구 > 인터넷 옵션 > 보안 > 로컬 인트라넷 > 사용자 지정 수준으로 이동합니다.

Internet Options	
General Security Privacy Content Connections Programs Advanced Select a zone to view or change security settings. Internet Incal intranet Trusted sites Restricted sites Internet Local intranet Trusted sites Restricted sites Internet Local intranet Trusted sites Restricted sites Image: Content intranet Trusted sites Sites Image: Content intranet Sites Sites Image: Content intranet Sites Sites Image: Content intranet Sites Sites Image: Content view of this zone Alowed levels for this zone: All Image: Content will be run without prompting you Image: Content will be run without prompting you Image: Content will be run without prompting you Image: Content will be run without prompting you Image: Content will be run without prompting you Image: Content will be run without prompting you Image: Content will be run without prompting you Image: Content will be run without prompting you Image: Content will be run without prompting you Image: Content will be run without prompting you Image: Content will be run without prompting you Image: Content will be run without prompting you	************************************

Tools(**툴**) > Internet Options(인터넷 옵션) > Security(보안) > Local intranet(로컬 인트라넷) > Sites(사이트) > Advanced(고급)로 이동하여 IDP(Intrusion Detection & Prevention) URL을 로 컬 인트라넷 사이트에 추가합니다.

참고:로컬 인트라넷 대화 상자에서 모든 확인란을 선택하고 **고급 탭**을 클릭합니다.

General Security Privacy Content Connections Programs Advances	
Select a zone to view or change security settings. Internet Internet Local intranet Trusted sites Local intranet Sites This zone is for all websites that are found on your intranet. Sites	Local intranet 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)
Security level for this zone Allowed levels for this zone: All Medium-low Appropriate for websites on your local network Most content will be run without prompting you 	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

CUCM 호스트 이름**을 신뢰할 수 있는 사이트에** 추가하려면 Tools(툴) > Security(보안) > Trusted sites(신뢰할 수 있는 사이트) > Sites(사이트)로 이동합니다.

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 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:
V trust not to damage your computer or your files. You have websites in this zone.	Webstes: https:// CUCM1.domainname.com
Security level for this zone	https:// CUCM2.domainname.com
Allowed levels for this zone: All Medium Prompts before downloading potentially unsafe Control of the second se	۲.5
- 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
	und at our <u>Export Compliance Product Rep</u> ur <u>Unified Communications System Docum</u> Loading, please
OK Cancel Apply	

다음을 확인합니다.

이 섹션에서는 어떤 인증(Kerberos 또는 NTLM(NT LAN Manager) 인증을 사용하는지 확인하는 방법에 대해 설명합니다.

- 1. 클라이언트 <u>컴퓨터에</u> Windows Media Player 도구를 다운로드하여 설치합니다.
- 2. 모든 Internet Explorer 창을 닫습니다.
- 3. File Tool을 실행하고 File 메뉴에서 Capture Traffic 옵션이 활성화되었는지 확인합니다.

Fiddler는 클라이언트 시스템과 서버 간의 통과 프록시 역할을 하며 모든 트래픽을 수신하며, 이 경우 Internet Explorer 설정을 다음과 같이 일시적으로 설정합니다.

Local Area	Network (L	AN) Settings	-	23
Automa Automa use of r Auto Use Ado	tic configurat atic configurat manual setting omatically det automatic co	tion tion may override manual settings. gs, disable automatic configuration. tect settings nfiguration script	To ensure	the
Proxy s Use dial-	a proxy serv up or VPN co ings	er for your LAN (These settings will nnections).	not apply	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	Po	rt 888 888
Exception	Do not use <-loopbac Use semicol	proxy server for addresses beginnink k>	ng with:	*

- 4. Internet Explorer를 열고 CRM(Customer Relationship Management) 서버 URL을 찾은 다음 링크를 클릭하여 트래픽을 생성합니다.
- 5. Windows Media Player 기본 창을 다시 참조하고 Frames(프레임) 중 하나를 선택합니다(성공).

A Da	aller Mich I	Debugger				
V Fig	Citer web t	repugger	March 11 - OFT O			^
Pile	Edit Rul	es Tools	View Help GET /2	oook Eva GeoEdge		
24	Replay 7	X - 🕨 Go	🗣 Stream 🌆 Deci	ode 🔰 Keep: All sessions 👻 🕀 Any Proce	as 👬 Find 🔣 Save 1 🎼 🕐 🏉 Browse 🔹 🕀 Clear Cache 🎢 TextWizard 🛛 🔛 Tearoff 🛛 MSDN Search	E.
	Result	Protocol	Host	URL A	🕐 Statistics 🚟 Inspectors 🥖 AutoResponder 🧭 Composer 🔲 Niters 🗈 Log 🚍 Timeline	
01	200	HTTP	www.default-searc	Psid=476baid=1000itype=n6wer=1307;	Headers TextWew WebForms HexWew Auth Cookies Raw 350N XML	
432	200	HTTP	www.default-searc	/rsid=476baid=1008itype=r6wer=1307:	No Proxy-Authorization Header is present.	
(f) 3	200	HTTP	Tunnel to	vos-cm35.sso-44.com:443	buthorization wester (Menotiate) annearr to contain a Merheror ticket:	51
434	200	HTTPS	vos-cm35.sso-44.com	/	worder raation Header (Negotiate) appears to contain a kerberos cickeci	-
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/samil/ogin?relayurl=%2Fcomadmir	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	
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	HTTPS	uncirretti, sso-tti com	ladisik/authintensatedi?SAM Requester	GE 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.COM460\$	
00.11	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	
2 12	302	HTTPS	vos-cm35.sso-44.c	/ssosp/sami/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	da 12 nd al 3/ 9a na 62 88 de 68 no 87 en na et 1 1 8 th ha	-
4314	200	HTTPS	vos-cm35.sso-44.c	(conadmin/showhlome.do	Get SyntaxView Transformer Headers TextView ImageView HexView WebView Auth Cachin	
凸 15	200	HTTP	Tunnel to	vos-cm35.sso-44.com/8443	Contries Days 15/61 Vie	1
16	200	HTTP	Tunnel to	vos-cm35.sso-44.com/8443		-1
曲 17	200	HTTP	Tunnel to	vos-cm35.sso-44.com:8443	Response Headers (Haw) Header Definition	
們 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	*
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	UTTO	Tunnellan	une en 36 een 44 een 9445	Expres: -1	•
The second	Sector Tal	n s biss alfi	D		t II.	
111						_
El Ca	sturing	T Al Proces	sses 1/30	https://vos-cm44.sso-44.com/adfs/is/a	.atvintegrated(?SAMLRequest=nkLLbtswELznkiwTeFVqWbEuE2cONEdRA2IR20Nva3qVEX80Uu57d%284Lh6wW80Hrgguh7Mz	6 ₁₁

인증 유형이 NTLM인 경우 프레임 시작**에 협상 - NTLMSSP**가 표시됩니다(아래 참조).

🕐 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 00 0F 49 00 4E 00 54 00 57 00(I.N.T.W.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.