يئاەنلا مدختسملل ADFS 2.0 عم Kerberos SAML SSO نيوكت لاثمل Jabber

المحتويات

<u>المقدمة</u> <u>المتطلبات الأساسية</u> <u>المكونات المستخدمة</u> معلومات أساسية <u>التحقق من الصحة</u> استكشاف الأخطاء واصلاحها

المقدمة

يصف هذا المستند كيفية تكوين Kerberos باستخدام خدمات إتحاد 2.0 Active Directory (ADFS).

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

يتطلب تكوين تسجيل الدخول الأحادي (SSO) الخاص ب تأكيد أمان المستخدم النهائي تكوين Kerberos للسماح للمستخدم النهائي SAML SSO ل Jabber بالعمل مع مصادقة المجال. عند تنفيذ SAML SSO باستخدام Kerberos، يقوم البروتوكول الخفيف للوصول إلى الدليل (LDAP) بمعالجة كل التخويل ومزامنة المستخدم، بينما يقوم Kerberos بإدارة المصادقة. Kerberos هو بروتوكول مصادقة تم إستخدامه بالاقتران مع المثيل الذي تم تمكين

LDAP به.

على أجهزة Microsoft Windows و Macintosh المرتبطة بمجال Active Directory، يمكن للمستخدمين تسجيل الدخول إلى Cisco Jabber بسلاسة دون الحاجة إلى إدخال اسم مستخدم أو كلمة مرور ولا يشاهدون حتى شاشة تسجيل دخول. لا يزال المستخدمون الذين لم يتم تسجيل دخولهم إلى المجال على أجهزة الكمبيوتر لديهم يرون نموذج تسجيل دخول قياسي.

نظرا لأن المصادقة تستخدم رمزا مميزا فرديا تم تمريره من أنظمة التشغيل، فلا حاجة لإعادة التوجيه. يتم التحقق من الرمز المميز مقابل وحدة التحكم بالمجال الأساسية (KDC) التي تم تكوينها، وإذا كان صحيحا، فيتم تسجيل دخول المستخدم.

التكوين

فيما يلي الإجراء لتكوين Kerberos باستخدام ADFS 2.0.

أضف هذا الجهاز إلى المجال الذي أنشأته في تثبيت ADDS.

.1	تثبيت Microsoft Windows Server 2008 R2 على جهاز.
.2	تثبيت خدمات مجال خدمة Active Directory (ADDS) و ADFS على نفس الجهاز.
.3	تثبيت "خدمات معلومات الإنترنت" (IIS) على الجهاز المثبت على Microsoft Windows Server 2008 R2.
.4	إنشاء شهادة موقعة ذاتيا ل IIS.
.5	قم باستيراد الشهادة الموقعة ذاتيا إلى IIS واستخدمها كشهادة خادم HTTPS.
.6	قم بتثبيت Microsoft Windows7 على جهاز آخر واستخدمه كعميل.
	قم بتغيير خادم اسم المجال (DNS) إلى الجهاز الذي قمت بتثبيت "إضافة" فيه.

انتقل إلى **البدء**.انقر بزر الماوس الأيمن على **الكمبيوتر**.انقر فوق **خصائص**.انقر على **تغيير الإعدادات** في الجانب الأيمن من النافذة.انقر على **علامة التبويب اسم الكمبيوتر**.طقطقة **تغير**.إضافة المجال الذي قمت بإنشائه.

							rashaikn	Star
System Properties		8	 User Management 	t 👻 Bulk Adr	ninistration +	Help 👻		
Computer Name/Domain C	Changes 🗾	ote						
You can change the name an	nd the membership of this	mputer						
Computer. Changes might affe More information	ect access to network resources.		-					83
			Security System		- 4	Search Cor	trol Panel	P
Computer name:		y's						. 0
Sabberch			asic information	about you	r compute	er -		
JabberPC1.mangolab.com			s edition					.
	More		lows 7 Professional					11
Member of		(ID	right © 2009 Microso	ft Corporation	. All rights re	eserved.		
Domain:			ce Pack 1					
mangolab.com		90	nore features with a ne	ew edition of V	Vindows 7			
O Workgroup:								
			L					•
			ıg:	System ratin	g is not avail	able		
	Cance		essor:	Intel(R) Xeon	n(R) CPU E7-	2870 @ 2.40GH	z 2.40 GHz	
	OK Cancel	Apply	lied memory (RAM):	2.00 GB 64-bit Opera	ting System			
		GPP7	and Touch:	No Pen or To	ouch Input is	available for th	is Display	
ut Cisco Unified Commun		Come	ter some demain and	workerson cet	tions			
Support please visit our]		Compt	mouter name, domain, and	labbarDC1	ungs		Change settings	
		Ful	l computer name:	JabberPC1.m	nangolab.cor	n	Change seconds	
		Co	mputer description:	JabberPC1	,			
	See also	Do	main:	mangolab.co	om			
	Action Center	Windo	ws activation					
	Windows Update	Wir	ndows is activated				and the	
	Performance Information and	Pro	duct ID: 00371-221-876	7124-86146	Change pro	duct key	genuine	
	Tools				- /	-	software	-
							Learn more online	

.7

تحقق ما إذا كانت خدمة Kerberos تقوم بتوليد على كلا الجهازين.

قم بتسجيل الدخول كمسؤول على جهاز الخادم وافتح موجه الأوامر. بعد ذلك قم بتنفيذ هذه الأوامر:

القرص المضغوط \Windows\System32 تذاكر قائمة

C:\User	s\Administrator.WIN2K8>cd \windows\System32
C:\Vind	ows\System32>Klist tickets
Current	LogonId is 0:0x3d6072
Cached 🕻	Tickets: <1>
#0>	Client: Administrator @ 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 18:06:04 (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

قم بتسجيل الدخول كمستخدم مجال على جهاز العميل وقم بتنفيذ الأوامر نفسها.

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 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
f1> 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_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
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_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-CTS-HMAC-SHA1-96
14> 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
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
C:\Windows\System32>

8. قم بإنشاء هوية ADFS Kerberos على الجهاز حيث قمت بتثبيت ADDS.

قام مسؤول Microsoft Windows بتسجيل الدخول إلى مجال Microsoft Windows (باسم <Administrator>\administrator)، على سبيل المثال على وحدة التحكم بالمجال ل Microsoft Windows، بإنشاء هوية ADFS Kerberos. يجب أن تحتوي خدمة ADFS HTTP على هوية Kerberos تسمى اسم الخدمة الأساسي (SPN) بهذا التنسيق: HTTP/DNS_name_of_ADFS_server.

يجب تعيين هذا الاسم لمستخدم Active Directory الذي يمثل مثيل خادم ADFS HTTP. أستخدم الأداة المساعدة ل Microsoft Windows **SetSPN**، والتي يجب أن تكون متوفرة بشكل افتراضي على خادم

.Microsoft Windows 2008

الإجراء قم بتسجيل SPNs لخادم ADFS. على وحدة التحكم بمجال Active Directory، قم بتشغيل الأمر setSPN.

على سبيل المثال، عندما يكون مضيف ADFS هو adfs01.us.renovations.com، ويكون مجال Active وDirective هو Directors هو Directory هو US.RENOVATIONS.COM، فإن الأمر هو:

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

يتم تطبيق جزء **HTTP/** من SPN، حتى وإن كان خادم ADFS يتم الوصول إليه عادة من خلال طبقة مآخذ التوصيل الآمنة (SSL)، والتي هي HTTPS.

تحقق من أن SPNs لخادم ADFS تم إنشائها بشكل صحيح باستخدام أمر setSPN وعرض المخرجات.

setspn -L



انتقل إلى **أدوات > InternetOptions > متقدمة** لتمكين المصادقة المتكاملة ل Windows.

حدد خانة الاختيار **تمكين مصادقة Windows المتكاملة**:

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 sortware to run or install even in the signature is inv.						
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						
Finable DOM Storage						
Enable Integrated Windows Authentication*						
Enable memory protection to help mitigate online attacks*						
Enable native XMLHTTP support						
Enable Smartscreen Filter						
*Takes affect after you restart Internet Evoluter						
Takes effect arter you restart internet Explorer						
Restore advanced settings						
Reset Internet Explorer settings						
Resets Internet Explorer's settings to their default Reset						
condition.						
You should only use this if your browser is in an unusable state.						
Cancer Apply						

انتقل إلى **أدوات > خيارات الإنترنت > الأمان > إنترانت المحلية > مستوى مخصص.**. لتحديد **تسجيل الدخول** التلقائي فقط في منطقة إنترانت.

Internet Options P E3 General Security Privacy Content Connections Programs Advanced	←
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 Sites Internet Local intranet Sites Internet This zone is for all websites that are found on your intranet. Sites Security level for this zone Allowed levels for this zone: All Image: Content will be run without prompting you Insigned ActiveX controls will not be downloaded Same as Medium level without prompting you Unsigned ActiveX controls will not be downloaded 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 Image: Content will be run without prompting you Image: Content will be run without prompting you Image: Content will be run without prompting Image: Content will be run without prompting Image: Content will be run Image: Content will be run Image: Content will be run Image: Content will be run <	Security Settings - Local Intranet Zone Settings Disable Enable XSS filter Disable Enable Sorpting of Java applets Disable Enable Frompt User Authentication Automatic logon only in Intranet zone Automatic logon With Current User Hame and password Prompt for user name and password Prompt for user name and password Reset custom settings Reset to: Medium-low (default) OK Cancel

انتقل إلى **أدوات > خيارات الإنترنت > الأمان > إنترانت المحلية > المواقع > خيارات متقدمة** لإضافة عنوان URL لاكتشاف التسلل ومنعه (IDP) إلى مواقع إنترانت المحلية.

ملاحظة: تحقق من كافة خانات الاختيار الموجودة في شاشة إنترانت المحلية وانقر فوق **علامة التبويب خيارات متقدمة**.

Internet Options	
Select a zone to view or change security settings. Select a zone to view or change security settings. Internet Local intranet Trusted sites Restricted Sites Local intranet This zone is for all websites that are found on your intranet.	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 (Intranet) Most content will be run without prompting you 	What are intranet settings? Advanced OK Cancel Local intranet Image: Concel Ima

انتقل إلى **أدوات > التأمين > المواقع الموثوق بها > المواقع** لإضافة أسماء مضيف CUCM إلى المواقع الموثوق بها:

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 Stee	Add this website to the zone:
This zone contains websites that you trust not to damage your computer or your files.	Webstes:
You have websites in this zone.	https:// CUCM1.domainname.com Remove
Allowed levels for this zone: All	https:// CUCM2.domainname.com
	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 al zones to derault level	und at our <u>Export Compliance Product Rep</u> ur <u>Unified Communications System Docum</u> Loading, please
OK Cancel Apply	

التحقق من الصحة

يشرح هذا القسم كيفية التحقق من المصادقة (مصادقة Kerberos أو مصادقة مدير شبكة NTLM) (NTLM) المستخدمة.

.1	قم بتنزيل <u>أداة Fiddler</u> إلى جهاز العميل وقم بتثبيتها.
.2	إغلاق كافة نوافذ Internet Explorer.
.3	قم بتشغيل أداة الفواصل وتحقق من أن خيار التقاط حركة مرور متاح تحت قائمة الملف.

يعمل Fiddler كوكيل مرور بين جهاز العميل والخادم ويستمع إلى كل حركة مرور، والتي تقوم مؤقتا بتعيين إعدادات Internet Explorer مثل:

Local Area	Network (LAI	N) Settings	-	23			
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 server Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).							
		and the factor of the second					
Servers	Туре	Proxy address to use	I	Port			
	HTTP:	127.0.0.1	:	8888			
	Secure:	127.0.0.1	:	8888			
	FTP:		:				
	Socks:		:				
	Use the sa	ame proxy server for all protocols					
Exceptio	ons						
	Do not use pr	roxy server for addresses beginning v	with:				
	<-loopback:	>		4 4			
	Use semicolor	ns (;) to separate entries.					

افتح Internet Explorer، واستعرض عنوان URL لخادم إدارة علاقات العملاء (CRM)، وانقر فوق بعض 4. الارتباطات لإنشاء حركة مرور البيانات.

ارجع إلى نافذة Fiddler الرئيسية واختر أحد الإطارات حيث تكون النتيجة 200 (نجاح):

🔷 Fide	ller Web D	ebugger			
File	idit Rule	s Tools	View Help GET /b	oook 🔛 GeoEdge	
Q 4	Replay >	K- 🕨 Go	🗣 Stream 🌉 Deco	ode Keep: All sessions = 🕀 Any Proce	ess 🌺 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	/?sid=476baid=1000itype=n6wer=1307;	Headers TextWew WebForms HexWew Auth Cookies Raw JSON XNL
432	200	HTTP	www.default-searc	/hsid=4768aid=1008itype=n6wer=1307:	No Proxy-Authorization Header is present.
(f) 3	200	HTTP	Tunnel to	vos-cm35.sso-44.com:443	suthorization weater (wennetista) annearr to contain a Perheror ticket:
<24	200	HTTPS	vos-cm35.sso-44.com	/	to be us to be to be of the of the of the of the of the of the terms of terms o
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 + 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 +
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	vos-m44.ssp-44.com	ladisikia thintercated 250M Benuest-	04 3A 30 02 04 36 A0 03 02 01 05 A1 0C 18 0A 53 .:0 .6
10	200	HT1P5	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 90-44.COM4405
70.11	200	HTTP	Turnel 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/sami/S50/alias/vos-cm35.sso-44.c	60 A3 82 03 F7 70 82 03 F3 A0 03 02 01 17 A1 03 m£ .+0 .0
5 13	302	HTTPS	vos-cn35.sso-44.c	(ssosp(relay	aa 13 na ad 30 sa na 63 an de 68 n5 a7 en na et 3 't 8 fe 'ha
<>14	200	HTTPS	vos-cm35.sso-44.c	/comadmin/showHome.do	Get SyntaxWew Transformer Headers TextView ImageWew HexNew WebWew Auth Caching
曲 15	200	HTTP	Tunnel to	vos-cm35.sso-44.com/8443	Confiles Dave NON 1994
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 Octivitions
m 18	200	HTTP	Tunnel to	vos-cm35.sso-44.com:8443	NTTP/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: Fit, 25 Jul 2014 13:07:58 GMT
1 22	300	UTTO	Turned in	une em 36 con 44 com 9443	Expres: -1
The second s	escl ALT+C	s Nov HE	P		4
🕸 Cap	turing *	 Al Proces 	i / 30	https://vos-cm44.sso-44.com/adfs/is/a	uth/integrated(?SAMLRequest=nMLbtswELznKwTeFVqWbEUEZcONEdRA2iR20Nva3qVEXBUUu57d%28ALh5wW8OHngguh7Mbs/

إذا كان نوع المصادقة NTLM، فأنت ترى **التفاوض - NTLMSSP** في بداية الإطار، كما هو موضح هنا:

🕑 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 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.

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما