ةقداصم مادختساب SAML SSO دادعإ نيوكت Kerberos

المحتويات

<u>المقدمة</u> <u>المتطلبات الأساسية</u> <u>المكونات المستخدمة</u> <u>التكوين</u> <u>AD FS تهيئة AD FS</u> <u>يرنامج AD FS Microsoft Internet Explorer يرنامج Microsoft Internet Explorer <u>التحقق من الصحة</u> <u>استكشاف الأخطاء وإصلاحها</u></u>

المقدمة

يوضح هذا المستند كيفية تكوين الإصدار 2.0 من خدمة إتحاد خدمة Active Directory (AD FS) و Active Directory لتمكينها من إستخدام مصادقة Kerberos بواسطة عملاء Jabber (في Microsoft Windows فقط)، والتي تتيح للمستخدمين تسجيل الدخول باستخدام تسجيل الدخول إلى Microsoft Windows وعدم مطالبتهم ببيانات الاعتماد.

تحذير: يستند هذا المستند إلى بيئة معملية ويفترض أنك على دراية بتأثير التغييرات التي تقوم بها. ارجع إلى وثائق المنتج ذات الصلة لفهم تأثير التغييرات التي تقوم بها.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن يكون لديك:

- AD FS الإصدار 2.0 المثبت والمهيئة باستخدام منتجات التعاون من Cisco كثقة جهة معتمدة
- منتجات التعاون مثل المراسلة الفورية Cisco Unified Communications Manager (CUCM) IM and (UCXN و CUCN الممكنة من أجل إستخدام لغة تمييز تأكيد الأمان (Presence، Cisco Unity Connection (UCXN) تسجيل الدخول الأحادي (SSO)

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- Active Directory 2008 (اسم المضيف: ADFS1.ciscolive.com)
 - AD FS الإصدار 2.0 (اسم المضيف: ADFS1.ciscolive.com)
 - CUCM (اسم المضيف: CUCM (اسم المضيف: CUCM1.ciscolive.com)
 - Microsoft Internet Explorer، الإصدار 10
 - موزيلا فايرفوكس الإصدار 34
 - تيليريك فيدلر الإصدار 4

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.

التكوين

تهيئة AD FS

قم بتكوين AD FS الإصدار 2.0 باستخدام اسم الخدمة الأساسي (SPN) لتمكين كمبيوتر العميل المثبت عليه 1. Jabber لطلب التذاكر، مما يمكن كمبيوتر العميل بدوره من الاتصال بخدمة AD FS.



راجع AD FS 2.0: <u>كيفية تكوين SPN (servicePrincipalName) لحساب الخدمة</u> للحصول على مزيد من المعلومات.

تأكد من أن تكوين المصادقة الافتراضي لخدمة AD FS (في **C:\inetpub\adfs\ls\web.config**) هو **مصادقة**2. Windows المدمجة. تأكد من أنه لم يتم تغييره إلى **مصادقة مستندة إلى نموذج**.

3. حدد **مصادقة Windows** وانقر فوق **إعدادات متقدمة** أسفل الجزء الأيمن. في الإعدادات المتقدمة، قم بإلغاء

تحديد **تمكين مصادقة وضع kernel**، وتأكد من **إيقاف تشغيل الحماية الموسعة**، ثم انقر على **موافق**.



تأكد من أن AD FS الإصدار 2.0 يدعم كلا من بروتوكول Kerberos وبروتوكول مدير شبكة MAN NT (NTLM). لأن جميع العملاء بخلاف Windows لا يمكنهم إستخدام Kerberos والاعتماد على NTLM.

في الجزء الأيمن، حدد **الموفرين** وتأكد من وجود **التفاوض** وNTLM ضمن الموفرين الذين تم تمكينهم:

Linternet Information Services (IIS) Manager					
ADFS1 ► Sites	Default Web Site Adfs Is		🖬 🖂 🚹 I 😰 🕶		
File View Help					
File View Hep Connections Start Page Start Page ADFS1 (CISCOLIVE\Administrato Application Pools Sites Optication Pools Sites Select a proviate NTLM Select a proviation: localhost Available Prov	Authentication Group by: No Grouping Name Anonymous Authentication ASP.NET Impersonation Forms Authentication Windows Authentication ders: der from the list of available providers to add it to the enabled providers.	Status Enabled Disabled Prosbled ? X Move Up ove Down Remove	Alerts		
	ок	Cancel	- L ::		

ملاحظة: يمرر AD FS رأس أمان التفاوض عند إستخدام مصادقة Windows المتكاملة لمصادقة طلبات العميل. يتيح رأس أمان التفاوض للعملاء إمكانية التحديد بين مصادقة Kerberos ومصادقة NTLM. تحدد عملية التفاوض مصادقة Kerberos ما لم يكن أحد هذه الشروط صحيحا:

- يتعذر على أحد الأنظمة المشاركة في المصادقة إستخدام مصادقة Kerberos.
 - لا يوفر تطبيق الاتصال معلومات كافية لاستخدام مصادقة Kerberos.

- لتمكين عملية التفاوض لتحديد بروتوكول Kerberos لمصادقة الشبكة، يجب أن يوفر تطبيق العميل اسم SPN أو اسم مستخدم أساسي (UPN) أو اسم حساب نظام الإدخال/الإخراج الأساسي للشبكة (NetBIOS) كاسم هدف. وإلا، فتقوم عملية التفاوض دائما بتحديد بروتوكول NTLM كطريقة المصادقة المفضلة.

تكوين المستعرض

برنامج Microsoft Internet Explorer

تأكد من أن Internet Explorer > **متقدم>تمكين المصادقة المتكاملة ل Windows** تم التحقق. .1

Internet Options
General Security Privacy Content Connections Programs Advanced
Settings
 Empty Temporary Internet Files folder when browser is clc Enable DOM Storage Enable Integrated Windows Authentication* Enable memory protection to help mitigate online attacks*
*Takes effect after you restart Internet Explorer
Restore advanced 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

إضافة عنوان URL ل AD FS تحت **الأمان >مناطق إنترانت > المواقع**.

Internet Options
General Security Privacy Content Connections Programs Advanced
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
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)
What are intranet settings? Advanced OK Cancel
Local intranet
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:
adfs1.ciscolive.com Remove

إضافة أسماء مضيفي CUCM و IMP و Unity إلى **الأمان >المواقع الموثوق بها**.

Internet Options	? 🔀
General Security Privacy Content Connections Progr	rams Advanced
Select a zone to view or change security settings.	
🥥 🔩 🗸 🚫	
Internet Local intranet Trusted sites Restricted sites	1
Trusted sites	Sites
Trusted sites	
You can add and remove websites from this zone this zone will use the zone's security settings. Add this website to the zone:	e. All websites in
	Add
Websites:	
cucm1.ciscolive.com	Remove
ucxn1.ciscolive.com	
Require server verification (https:) for all sites in this z	one
	Close

تأكد من أن Internet Exporer > **أمان > إنترانت المحلية > إعدادات الأمان>**مصادقة المستخدم - تم تكوين 4. **تسجيل الدخول** لاستخدام بيانات الاعتماد التي تم تسجيل الدخول لمواقع إنترانت.

Internet Options	8 23
General Security Privacy Content Connections	s Programs Advanced
	Security Settings - Local Intranet Zone
Select a zone to view or change security settings. Network of the security settings. Network of the security level in the security level for this zone Allowed levels for this zone Allowed levels for this zone: All 	Sectings Settings Settings
ОК	OK Cancel

Mozilla Firefox

.1

.2

افتح Firefox وأدخل **حول:config** في شريط العناوين.



انقر **سأكون حذرا، أعدك!**

	Here be dragons!		
•	Changing these advanced settings can be harmful to the stability, security, and performance of this application. You should only continue if you are sure of what you are doing.		
	Show this warning next time		
	I'll be careful, I promise!		

انقر نقرا مزدوجا على اسم التفضيل network.negotiate-auth.allow non-fqdn إلى true وriscolive.com،adfs1.ciscolive.com إلى ciscolive.com،adfs1.ciscolive.com من أجل التعديل.

Search: network.n						
Preference Name	Status	Туре	Value			
network.negotiate-auth.allow-insecure-ntlm-v1	default	boolean	false			
network.negotiate-auth.allow-insecure-ntlm-v1-https	default	boolean	true			
network.negotiate-auth-allow-non-fqdn	user set	boolean	true			
network.negotiate-auth.allow-proxies	default	boolean	true			
network.negotiate-auth.delegation-uris	default	string				
network.negotiate-auth.gsslib	default	string				
network.negotiate-auth.trusted-uris	user set	string	adfs1.adfs1.ciscolive.com.ciscolive.com			
network.negotiate-auth.using-native-gsslib	default	boolean	true			
network.ntlm.send-lm-response	default	boolean	false			

4. إغلاق Firefox وإعادة فتحه.

التحقق من الصحة

للتحقق من إنشاء SPNs لخادم AD FS بشكل صحيح، أدخل أمر **setSPN** وعرض المخرجات.

🖬 Administrator: Command Prompt	l ×
Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation. All rights reserved.	-
C:\Users\Administrator>setspn -L sso Registered ServicePrincipalNames for CN=Saml SSO,CN=Users,DC=ciscolive,DC=com: HTTP/adfs1	
C:\Users\Administrator>	

تحقق مما إذا كانت أجهزة العميل تحتوي على تذاكر Kerberos:

C:\Windows\system32\cmd.exe	×
C:\Users\user1.CISCOLIVE>Klist tickets	-
Current LogonId is 0:0xabc6d	
Cached Tickets: <2>	
#0> Client: user1 @ CISCOLIVE.COM Server: krbtgt/CISCOLIVE.COM @ CISCOLIVE.COM KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96 Ticket Flags 0x40e0000 -> forwardable renewable initial pre_authent Start Time: 1/17/2015 20:52:47 (local) End Time: 1/18/2015 6:52:47 (local) Renew Time: 1/24/2015 20:52:47 (local) Session Key Type: AES-256-CTS-HMAC-SHA1-96	Ш
#1> Client: user1 @ CISCOLIVE.COM Server: host/pc1.ciscolive.com @ CISCOLIVE.COM KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96 Ticket Flags 0x40a00000 -> forwardable renewable pre_authent Start Time: 1/17/2015 20:52:47 (local) End Time: 1/18/2015 6:52:47 (local) Renew Time: 1/24/2015 20:52:47 (local) Session Key Type: AES-256-CTS-HMAC-SHA1-96	
C:\Users\user1.CISCOLIVE>_	

أكمل هذه الخطوات للتحقق من المصادقة (مصادقة Kerberos أو NTLM) قيد الاستخدام.

إغلاق كافة نوافذ Microsoft Internet Explorer.

قم بتشغيل أداة fiddler وتحقق من أن **خيار التقاط حركة مرور** يكون مكنت تحت القائمة ملف. يعمل Fiddler. كوكيل مرور بين جهاز العميل والخادم ويستمع إلى كل حركة مرور.

افتح Microsoft Internet Explorer، واستعرض إلى CUCM، وانقر فوق بعض الارتباطات لإنشاء حركة مرور. البيانات.

ارجع إلى الإطار الرئيسي ل Fiddler واختر أحد الإطارات حيث تكون النتيجة **200** (نجاح) ويمكنك أن ترى 5. Kerberos كآلية مصادقة

🚸 F	🔋 Fiddler Web Debugger					
File	Edit Rules	Tools Vi	ew Help GET /bo	ok 🔛 GeoEdge		
Q ·	PReplay >	<- 🕨 Go	ا 🖶 Stream 👑 🛙	Decode Keep: All sessions *	Process 🌺 Find 😡 Save 🗟 🕐 🌈 Browse 🔹 🕀 Clear Cache 🎢 T	extWizard 🔛 Tearoff 🛛 💂
	Result	Protocol	Host	URL	🔿 Statistics 🛗 Inspectors 🖌 🐔 AutoResponder 🗖 Composer 🗍	Filters 🗐 🕒 Log 🔚 Timeline 🗍
2	200	HTTP	cucm.ciscolive	/ciscologo.gif	Headers TextView WebForms HexView Auth Cookies	Raw JSON XML
3	200	HTTP	cuan.ciscolive	/favicon.ico		
54	302	HTTP	cucm.ciscolive	/ccmadmin/showHome.do	No Proxy-Authorization Header is present.	
🖆 5	200	HTTP	Tunnel to	cucm.ciscolive.com:443	Authorization Header (Negotiate) appears to contain a	Kerberos ticket:
56	302	HTTPS	cucm.ciscolive	/ccmadmin/showHome.do	4D 53 53 50 00 03 00 00 00 00 00 00 00 58 00 00 MSSP	X
57	302	HTTPS	cucm.ciscolive	/ssosp/saml/login?relayurl	00 00 00 00 00 58 00 00 00 00 00 00 00 58 00 00	.xx
1 1	200	HTTP	Tunnel to	adfs1.ciscolive.com:443	00 00 00 00 00 58 00 00 00 15 C2 88 E2 06 01 B1	.xλ à±
59	302	HTTPS	adfs1.ciscoliv	/adfs/ls/75AMLRequest=n	1D 00 00 00 0F 7E AF 60 90 3B D7 F3 E2 F4 5E 84	.~ ;×680^
21	0 401	HTTPS	adfs1.ciscoliv	/adfs/ls/auth/integrated/?	50 2D 22 9A 84 00 00 00 00 P-"	
21	1 401	HTTPS	adfs1.ciscoliv	/adfs/ls/auth/integrated/?		
<>	2 200	HTTPS	adfs1.ciscoliv	/adfs/ls/auth/integrated/?	Cat Contavilians Transformer Manders Tavilians Imagelians	Machine Wahllow
Øı	3 502	HTTP	www.downioa	/msdownload/update/v3/s	decisimaxiew marsioner meases reaction inageven	HEATEN WEDVEN
1 1	4 401	HTTPS	adfs1.ciscoliv	/favicon.ico	Auth Caching Cookies Raw JSON XML	
台 1	5 200	HTTP	Tunnel to	cucm.ciscolive.com:8443	No Proxy-Authenticate Header is present.	
🛛 🔂 1	6 302	HTTPS	cucm.ciscolive	/ssosp/sami/SSO/alias/CU	WWW-Authenticate Header (Negotiate) appears to be a K	erberos reply:
1 1 1	7 403	HTTPS	cucm.ciscolive	/ssosp/relay	A1 18 30 19 A0 03 0A 01 00 A3 12 04 10 01 00 00 i.0.	1
1	8 200	HTTPS	cucm.ciscolive	/ciscologo.gif	00 43 87 E0 88 CI 36 E3 A9 00 00 00 00 .C a	A640
01	9 502	HTTP	www.downloa	/msdownload/update/v3/s		
02	0 502	HTTP	www.downloa	/msdownload/update/v3/s		
1						
Quk	(Exec] ALT+Q	2 > type HE	1P		h	
iii c	apturing	+ All Proce	sees	1 / 20 Download Progress:	Hit F5 to refresh.	1

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

🚸 Fidd	er Web (ebugger			× II.
File Ed	it Rules	Tools Vie	w Help GET /bo	ok 🔛 GeoEdge	
Q 🙀	Replay 🕻	<- 🕨 Go	🔹 Stream 👹	Decode Keep: All sessions *	🕀 Any Process 🌺 Find 🔜 Save 🛛 🔞 🕐 Browse 🔹 🅀 Clear Cache 🎢 TextWizard 🛛 🛃 Tearoff
	Result	Protocol	Host	URL	📴 🕅 Statistics 👫 Inspectors 🖉 AutoResponder 🏹 Composer 🔲 Filters 🗉 Log 💳 Timeline
Ø 1	502	HTTP	www.bing.com	/favicon.ico	Headers TextView WebForms HexView Auth Cookies Raw JSON XML
≼ ≱2	200	HTTP	cucm.ciscolive	1	S, manual tables in the second product and the second second second second second second second second second s
23	200	HTTP	cucm.ciscolive	/ciscologo.gif	No Proxy-Authorization Header is present.
Ξ4	200	HTTP	cucm.ciscolive	/favicon.ico	1, Authorization Header is present: NTLM
5 5	302	HTTP	cucm.ciscolive	/comadmin/showHome.do	4E 54 4C 40 53 53 50 00 03 00 00 00 00 00 00 00 00 NTLMSSP
<u>6</u> 6	200	HTTP	Tunnel to	cucm.ciscolive.com:443	58 00 00 00 00 00 00 58 00 00 00 00 00 00 00 XXX
07	502	HTTP	www.downloa	/msdownload/update/v3/s	06 01 61 1D 00 00 00 F 4E 64 C3 AA 00 D1 61 34± N Å*.N 4
58	302	HTTPS	cucm.ciscolive	/comadmin/showHome.do	78 AA CE A9 41 F3 D1 31 Xª18AÓÑ1
59	302	HTTPS	cucm.ciscolive	/ssosp/saml/login?relayurl	
⁽¹⁾	200	HTTP	Tunnel to	adfs1.ciscolive.com:443	-[NTLM Type3: Authentication]
5 11	302	HTTPS	adfs1.ciscoliv	/adfs/ls/?SAMLRequest=n	Colombulton Transforms (2000) Testion Insultan Uniter Utility
12 12	401	HTTPS	adfs1.ciscoliv	/adfs/ls/auth/integrated/?	6, Get Syntaxview Transformer THeaders TextView Imageview Hexview Viebview
1 13	401	HTTPS	adfs1.ciscoliv	/adfs//s/auth/integrated/?	7, Auth Caching Cookies Raw JSON XML
<>14	200	HTTPS	adfs1.ciscoliv	/adfs/ls/auth/integrated/?	9, Response Headers [Raw1 Header Definitions]
15	401	HTTPS	adfs1.ciscoliv	/favicon.ico	6, HTTP/1,1 200 OK
16	200	HTTP	Tunnel to	cucm.ciscolive.com:8443	Cache
17	302	HTTPS	cucm.ciscolive	/ssosp/sami/SSO/alias/CU	Cache-Control: no-cache
18	403	HTTPS	cucm.ciscolive	/ssosp/relay	2.: Date: Sat, 17 Jan 2015 20:05:06 GMT
2 19	200	HTTPS	cucm.ciscolive	/ciscologo.gif	Expires: -1
					Pragma: no-cache
•					Conkies / Lonin
[QuidEx	ec] ALT+C) > type HEL	.P		
Tig Capt	😤 Capturing 🔍 All Processes 1 / 19 https://adfs1.dscolive.com/adfs/s/auth/integrated/75AMLRequest=nVLLbtsvELznKwjebYrytwphGXBsFDWQNErk9NDbi4BCR55V1p%28%2				

.2

استكشاف الأخطاء وإصلاحها

إذا تم إكمال جميع خطوات التكوين والتحقق كما هو موضح في هذا المستند وكانت لا تزال لديك مشاكل في تسجيل الدخول، فيجب عليك مراجعة مسؤول Microsoft Windows Active Directory / AD FS.

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