Exemple de configuration de Kerberos avec ADFS 2.0 pour l'utilisateur final SAML SSO pour Jabber

Contenu

Introduction Conditions préalables Conditions requises Components Used Informations générales Configuration Vérification Dépannage

Introduction

Ce document décrit comment configurer Kerberos avec Active Directory Federation Services (ADFS) 2.0.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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.

Informations générales

La configuration SSO (Single Sign On) SAML (End User Security Assertion Markup Language)

nécessite la configuration de Kerberos afin de permettre à l'utilisateur final SAML SSO pour Jabber de fonctionner avec l'authentification de domaine. Lorsque SAML SSO est implémenté avec Kerberos, le protocole LDAP (Lightweight Directory Access Protocol) gère toutes les autorisations et la synchronisation utilisateur, tandis que Kerberos gère l'authentification. Kerberos est un protocole d'authentification qui est destiné à être utilisé conjointement avec une instance compatible LDAP.

Sur les machines Microsoft Windows et Macintosh qui sont jointes à un domaine Active Directory, les utilisateurs peuvent se connecter de manière transparente à Cisco Jabber sans avoir à entrer un nom d'utilisateur ou un mot de passe et ils ne voient même pas d'écran de connexion. Les utilisateurs qui ne sont pas connectés au domaine sur leurs ordinateurs voient toujours un formulaire de connexion standard.

Étant donné que l'authentification utilise un jeton unique transmis par les systèmes d'exploitation, aucune redirection n'est requise. Le jeton est vérifié par rapport au contrôleur de domaine de clé (KDC) configuré et, s'il est valide, l'utilisateur est connecté.

Configuration

Voici la procédure à suivre pour configurer Kerberos avec ADFS 2.0.

- 1. Installez Microsoft Windows Server 2008 R2 sur une machine.
- 2. Installez les services de domaine Active Directory (ADDS) et ADFS sur le même ordinateur.
- 3. Installez Internet Information Services (IIS) sur l'ordinateur Microsoft Windows Server 2008 R2 installé.
- 4. Créez un certificat auto-signé pour IIS.
- 5. Importez le certificat auto-signé dans IIS et utilisez-le comme certificat de serveur HTTPS.
- 6. Installez Microsoft Windows7 sur un autre ordinateur et utilisez-le comme client.

Remplacez le serveur de noms de domaine (DNS) par l'ordinateur sur lequel vous avez installé ADDS.

Ajoutez cet ordinateur au domaine que vous avez créé lors de l'installation d'ADDS.

Allez à **Démarrer**.Cliquez avec le bouton droit sur **Ordinateur**.Cliquez sur **Properties**.Cliquez sur **Modifier les paramètres** à droite de la fenêtre.Cliquez sur l'onglet **Computer Name.**Cliquez sur **Change**.Ajoutez le domaine que vous avez créé.

	8	 User Management 	t 👻 Bulk Administration 👻 Hel	¢ ▼
nges 🗾	ote			
You can change the name and the membership of this computer. Onanges might affect access to network resources.				
	V's	Security System	• • • • S	earch Control Panel
				•
		s edition	about your computer	
More	t ID	rright © 2009 Microso ce Pack 1 nore features with a n	ft Corporation. All rights reserve ew edition of Windows 7	
OK Cancel		ig: essor: lled memory (RAM):	System rating is not available Intel(R) Xeon(R) CPU E7- 2870 2.00 GB	@ 2.40GHz 2.40 GHz
OK Cancel	Apply	em type:	64-bit Operating System	
		and Touch:	No Pen or Touch Input is availa	able for this Display
	Compu	uter name, domain, and	workproup settings	
	Co	mputer name:	JabberPC1	Change settings
	Ful	computer name:	JabberPC1.mangolab.com	• • •
	Cor	mputer description:	JabberPC1	
See also	Dor	main:	mangolab.com	
Action Center	Window	ws activation		
Windows Update	Wir	ndows is activated		ask for .
Performance Information and Tools	d Pro	oduct ID: 00371-221-876	7124-86146 Change product k	genuine C. Microsoft
	nges	nges ote he membership of this access to network resources. More Provider Pe.	nges ste he membership of this access to network resources. mputer y's ssic information sedition Nore sID gi ssori le nore features with a	ges ote he membership of this access to network resources y's asic information about your computer s edition lows 7 Professional right © 2009 Microsoft Corporation. All rights reserve c Pack 1 nore features with a new edition of Windows 7 g: System rating is not available essor: Intel(R) Xeon(R) CPU E7- 2870 Ied memory (RAM): 2.00 G8 m type: 64-bit Operating System and Touch: No Pen or Touch Input is available See also Computer name: JabberPC1 Action Center Windows activation Windows activation Windows Update Product ID: 00371-221-8767124-86145 Change product if

7. Vérifiez si le service Kerberos génère sur les deux machines.

Connectez-vous en tant qu'administrateur sur l'ordinateur serveur et ouvrez l'invite de commandes. Exécutez ensuite ces commandes :

cd \windows\System32Billets Klist

C:\Users\Administrator.WIN2K8>cd \windows\System32 C:\Windows\System32>Klist tickets Current LogonId is 0:0x3d6072 Cached Tickets: (1) 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) #0> 2014 4:06:04 (local) 4 local) 17/ 201 18:06:0 Time: 96 Session Key Type: **AES** -256 HA1-

Connectez-vous en tant qu'utilisateur de domaine sur l'ordinateur client et exécutez les mêmes commandes.

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. Créez l'identité Kerberos ADFS sur l'ordinateur sur lequel vous avez installé ADDS.

L'administrateur Microsoft Windows connecté au domaine Microsoft Windows (en tant que <nom du domaine>\administrateur), par exemple sur le contrôleur de domaine Microsoft Windows, crée l'identité Kerberos ADFS. Le service HTTP ADFS doit avoir une identité Kerberos appelée SPN (Service Principal Name) au format suivant : HTTP/DNS_name_of_ADFS_server.

Ce nom doit être mappé à l'utilisateur Active Directory qui représente l'instance du serveur

HTTP ADFS. Utilisez l'utilitaire **setspn** Microsoft Windows, qui doit être disponible par défaut sur un serveur Microsoft Windows 2008.

Procédure Enregistrez les SPN pour le serveur ADFS. Sur le contrôleur de domaine Active Directory, exécutez la commande **setspn**.

Par exemple, lorsque l'hôte ADFS est **adfs01.us.renovations.com** et que le domaine Active Directory est **US.RENOVATIONS.COM**, la commande est :

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

La partie **HTTP**/du SPN s'applique, même si le serveur ADFS est généralement accessible par SSL (Secure Sockets Layer), qui est HTTPS.

Vérifiez que les SPN du serveur ADFS sont correctement créés à l'aide de la commande **setspn** et affichez le résultat.

```
setspn -L
```

```
:\Windows\System32>setspn -L win2k8
Yegistered ServicePrincipalNames for CN=WIN2K8,0U=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-12P9A27C-BP97-4787-9364-D31B6C55EB04/win2k8.mangolab.com
    Dfsr-12P9A27C-BP97-4787-9364-D31B6C55EB04/win2k8.mangolab.com
    Dfsr-12P9A27C-BP97-4787-9364-D31B6C55EB04/win2k8.mangolab.com
    Dfsr-izP9A27C-BP97-4787-9364-D31B6C55EB04/win2k8.mangolab.com
    Dfsr-izP9A27C-BP97-4787-9364-D31B6C55EB04/win2k8.mangolab.com
    Dfsr-izP9A27C-BP97-4787-9364-D31B6C55EB04/win2k8.mangolab.com
    Dfsr-izP9A27C-BP97-4787-9364-D31B6C55EB04/win2k8.mangolab.com
    Dfsr-izP9A27C-BP97-4787-9364-D31B6C55EB04/win2k8.mangolab.com
    Dfsr-izP9A27C-BP97-4787-9364-D31B6C55EB04/win2k8.mangolab.com
    Dfsr-izP9A27C-BP97-4787-9364-D31B6C55EB04/win2k8.mangolab.com
    Dfsr-izP9A27C-BP97-4787-9364-D31B6C55EB04/win2k8.mangolab.com
    RestrictedKrbHost/WIN2K8
    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/MANGOLAB
    ldap/WIN2K8.mangolab.com/MANGOLAB
    ldap/WIN2K8.mangolab.com/MANGOLAB
    ldap/WIN2K8.mangolab.com/MANGOLAB
    ldap/WIN2K8
    ldap/win2k8.mangolab.com/MANGOLAB
    ldap/wIN2K8.mangolab.com/MANGOLAB
    ldap/wIN2K8.mangolab.com
    ldap/wIN2K8.mangolab.com/MANGOLAB
    ldap/wIN2K8.mangolab.com/MANGOLAB
    ldap/wIN2K8.mangolab.com
    ldap/wIN2K8.mangolab.com
    ldap/wIN2K8.mangolab.com
    ldap/wIN2K8.mangolab.com
    ldap/wIN2K8.mangolab.com
    ldap/wIN2K8.mangolab.com
    ldap/wIN2K8.mangolab.com
    ldap/wIN2K8.mangolab.com
    ldap/wIN2K8.mangolab.com
    ldap/wIN2K8.mangolab.com/mangolab.com
    ldap/wIN2K8.mangolab.com/mangolab.com
    ldap/wIN2K8.mangolab.com/mangolab.com
    ldap/wIN2K8.mangolab.com/mangolab.com
```

9. Configurez les paramètres du navigateur du client Microsoft Windows.

Accédez à **Outils > Options Internet > Avancé** afin d'activer l'authentification Windows intégrée.

Cochez la case Activer l'authentification Windows intégrée :

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 Fnable DOM Storage Enable Integrated Windows Authentication* Enable native XMLHTTP support Enable SmartScreen Filter					
Restore advanced settings					
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					

Accédez à Outils > Options Internet > Sécurité > Intranet local > Niveau personnalisé... afin de sélectionner Connexion automatique uniquement dans la zone Intranet.

Internet Options P EX General Security Privacy Content Connections Provisions Advanced	- A B C X A Cisco Unified Serviceability X
General Security Privacy Content Connections Programs Advanced Select a zone to view or change security settings. Image: Content Image: Content	Image: Circle Unified Serviceability X Security Settings - Local Intranet Zone Image: Circle Unified Serviceability Settings Disable Image: Disable Enable Enable Enable Scripting of Java applets Disable Disable Enable Enable Enable Image: Circle Unified Service ability X Viser Authentication Enable Prompt User Authentication Image: Cogon Automatic logon only in Intranet zone Automatic logon only in Intranet zone Automatic logon only in Intranet zone Prompt for user name and password Image: Circle Authentication Takes effect after you restart Internet Explorer Image: Circle Authentication Reset custom settings Reset to: Medum-low (default) Reset
CK Cancel Apply	CK Cancel

Accédez à **Outils > Options Internet > Sécurité > Intranet local > Sites > Avancé** afin d'ajouter l'URL de détection et de prévention des intrusions (IDP) aux sites Intranet local.

Note: Cochez toutes les cases de la boîte de dialogue Intranet local et cliquez sur l**'onglet Avancé**.

Internet Options Total Total General Security Privacy Content Connections Programs Advances	SS - ● E C × dtb Cisco Unified Serviceability ×
Select a zone to view or change security settings.	Local intranet E3
Security level for this zone Allowed levels for this zone: All Medium-low Appropriate for websites on your local network 	What are intranet settings? Advanced OK Cancel Local intranet Image: Conceleration of the sone so
OK Cancel Apply	Require server verification (https:) for all sites in this zone

Accédez à **Outils > Sécurité > Sites de confiance > Sites** afin d'ajouter les noms d'hôte CUCM aux sites de confiance :

Internet Options	- ≙ ≅ ♂ × 0 330-44.com ×
Internet Options General Security Privacy Content Connections Programs Advanced 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 Trusted sites Trusted sites This zone contains websites that you trust not to damage your computer or where there	Add this website to the zone: Add
your files. You have websites in this zone. Security level for this zone Allowed levels for this zone: All - Medium - Prompts before downloading potentially unsafe content - Unsigned ActiveX controls will not be downloaded	Websites: https:// CUCM1.domainname.com Remove https:// CUCM2.domainname.com Image: Cucm2.domainname.com Image: Cucm2
Enable Protected Mode (requires restarting Internet Explorer) Custom level Default level Reset all zones to default level OK Cancel Apply	Close 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

Vérification

Cette section explique comment vérifier quelle authentification (authentification Kerberos ou NT LAN Manager (NTLM)) est utilisée.

- 1. Téléchargez l'<u>outil Fiddler</u> sur votre machine cliente et installez-le.
- 2. Fermez toutes les fenêtres Internet Explorer.
- 3. Exécutez l'outil Fiddler et vérifiez que l'option **Capture Traffic** est activée dans le menu Fichier.

Fiddler fonctionne comme un proxy de transfert entre l'ordinateur client et le serveur et écoute tout le trafic, qui définit temporairement vos paramètres Internet Explorer comme suit :

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 setting	erver a proxy serve up or VPN con ings	r for your LAN (These settings will no nections).	t 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 > ns (;) to separate entries.	with:	*	

- 4. Ouvrez Internet Explorer, accédez à l'URL de votre serveur de gestion de la relation client (CRM) et cliquez sur quelques liens pour générer du trafic.
- 5. Reportez-vous à la fenêtre principale de Fiddler et choisissez l'une des trames dont le résultat est 200 (réussite) :

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 Table in 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	https://vos-cn/44.sso-44.com/adfs/is/a	utryintegratedy/s4MLHequest=mitLbtsweLankinTeP-vgWoEue2d/DHEdRA2IR/20Nva3gMEXBBUU57d%28RLh6wW8OHngguh7MEs7

Si le type d'authentification est NTLM, **Negotiate - NTLMSSP** apparaît au début de la trame, comme indiqué ici :

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

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.