Kerberos認証を使用したSAML SSOセットアップの設定

内容

<u>概要</u> <u>前提条件</u> <u>要件</u> <u>使用するコンポーネント</u> <u>設定</u> <u>AD FS の設定</u> <u>ブラウザの設定</u> <u>Microsoft Internet Explorer</u> <u>Mozilla Firefox</u> <u>確認</u> <u>トラブルシュート</u>

概要

このドキュメントでは、Jabber クライアントによる Kerberos 認証(Microsoft Windows のみ)を使用するために Active Directory および Active Directory Federation Service (AD FS)バー ジョン 2.0 を有効にする方法を説明します。これにより、ユーザは Microsoft Windows ログオン でログインし、クレデンシャルの入力を求められません。

注意:このドキュメントは、ラボ環境に基づいており、前提として、変更を実行したことに よる影響を認識しておいてください。実行した変更の影響を理解するために、関連する製品 ドキュメントを参照してください。

前提条件

要件

Cisco では次の前提を満たす推奨しています。

- AD FS バージョン 2.0 がインストールされ、シスコ コラボレーション製品を使用して信頼で きるパーティとして設定している
- Security Assertion Markup Language (SAML)シングル サインオン(SSO)を使用するために、Cisco Unified Communications Manager (CUCM) IM および Presence、Cisco Unity Connection (UCXN)、CUCM が有効化されている

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Active Directory 2008 (ホスト名: ADFS1.ciscolive.com)
- AD FS バージョン 2.0 (ホスト名: ADFS1.ciscolive.com)
- CUCM (ホスト名: CUCM1.ciscolive.com)
- Microsoft Internet Explorer $\mathcal{N} \mathcal{V} \exists \mathcal{V} \exists \mathcal{V}$
- Mozilla Firefox バージョン 34
- Telerik Fiddler バージョン 4

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。

設定

AD FS の設定

1. Jabber がインストールされているクライアントコンピュータを有効化してチケットをリク エストし、AD FS サービスと通信するためのクライアント コンピュータを有効化するため に、Service Principal Name (SPN)を使用して AD FS バージョン 2.0 を設定します。

📾 Administrator: Command Prompt	
Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation. All rights reserved.	^
C:\Users\Administrator>setspn —a HTTP/adfs1 ciscolive\sso Registering ServicePrincipalNames for CN=Saml SSO,CN=Users,DC=ciscolive,DC=c HTTP/adfs1 Updated object	:OM
C:\Users\Administrator>	

詳細については、「<u>AD FS 2.0:サービスアカウント用に SPN (servicePrincipalName)を</u> <u>設定する方法」を参照してください。</u>

2. AD FS サービス用のデフォルトの認証設定(C:\inetpub\adfs\ls\web.config に含まれる)が 統合 Windows 認証であることを確認します。それがフォームベース認証に変更されていな いことを確認します。



3. [Windows Authentication] を選択し、右ペインにある [Advanced Settings] をクリックします 。[Advanced Settings] で、[Enable Kernel-mode authentication] をオフにし、[Extended Protection] が [Off] であることを確認し、[OK] をクリックします。



4. Windows 以外のすべてのクライアントは、Kerberos を使用できず、NTLM に依存するため 、AD FS バージョン 2.0 が Kerberos プロトコルと NT LAN Manager (NTLM)プロトコル の両方をサポートすることを確認します。

右ペインで [Providers] を選択し、[Enabled Providers] の下に [Negotiate] と [NTLM] が存在 することを確認します。



注:統合 Windows 認証を使用すると、AD FS は、クライアントの要求を認証するためにネ ゴシエート セキュリティ ヘッダーを渡します。ネゴシエート セキュリティ ヘッダーは、ク ライアントが Kerberos 認証と NTLM 認証のいずれかを選択できるようにします。次のいず れかの条件に該当する場合を除き、ネゴシエート プロセスは Kerberos 認証を選択します。

- 認証に関与するシステムのいずれかが Kerberos 認証を使用できない。

- 発信側のアプリケーションが、Kerberos 認証を使用するための十分な情報を提供しない。

- ネットワーク認証に Kerberos プロトコルを選択するように、ネゴシエート プロセスを有 効化する目的で、クライアント アプリケーションが SPN、ユーザ プリンシパル名 (UPN)、または Network Basic Input/Output System (NetBIOS)アカウント名をターゲ ット名として提供する必要がある。そうしないと、ネゴシエート プロセスは、優先認証方 法として NTLM プロトコルを常に選択します。

ブラウザの設定

Microsoft Internet Explorer

1. [Internet Explorer] > [Advanced] > [Enable Integrated Windows Authentication] がオンになっ ていることを確認します。

Internet Options									
General Security Privacy Content Connections Programs Advanced									
Settings									
 Do not submit unknown addresses to your auto-search provention Just display the results in the main window Security 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 invi 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 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									
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									

2. [Security] > [Intranet zones] > [sites] に AD FS の URL を追加します。

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									

3. CUCM、IMP、および Unity のホスト名を [Security] > [Trusted sites] に追加します。

Internet Options	8 🕺								
General Security Privacy Content Connections Prog	rams Advanced								
Select a zone to view or change security settings.									
🛛 🔮 🔩 🗸 🚫									
Internet Local intranet Trusted sites Restricte sites	d								
Trusted sites	Sites								
Tructed sites	Sites								
Trusted sites									
You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.									
	Add								
Websites:									
cucm1.ciscolive.com	Remove								
imp1.ciscolive.com									
ucxn1.ciscolive.com									
Require server verification (https:) for all sites in this	zone								
	Close								

4. イントラネット サイト用にログイン クレデンシャルを使用するために、[Internet Exporer] > [security] > [Local Intranet] > [Security Settings] > [User Authentication - Logon] が設定され ていることを確認します。

Internet Options	83
General Security Privacy Content Connection	s Programs Advanced
	Security Settings - Local Intranet Zone
Select a zone to view or change security settings.	Settings
🔮 👒 🗸	O Disable
Internet Local intranet Trusted sites	Enable Enable XSS filter
Local intranet	Disable
This zone is for all websites that are	Enable Scripting of Java applets
Select a zone to view or change security settings Internet Local intranet Trusted sites Local intranet Local intranet Trusted sites Local intranet Trusted sites Local intranet Security level for this zone Allowed levels for this zone: All Allowed levels for this zone: All Appropriate for websites on you (intranet) Anst content will be run without Same as Medium level without pu Enable Protected Mode (requires restarti Custom level	 Disable
	Enable
Security level for this zone	Prompt
Allowed levels for this zone: All	& Logon
- Medium-low	Anonymous logon
 Appropriate for websites on your (intranet) 	Automatic logon only in Intranet zone
- Most content will be run without p	Automatic logon with current user name and password Prompt for user name and password
Internet Security Privacy Content Connection Select a zone to view or change security settings. Internet Internet </td <td>· · · · · · · · · · · · · · · · · · ·</td>	· · · · · · · · · · · · · · · · · · ·
Enable Protected Mode (requires restartin	*Takes effect after you restart Internet Evilorer
Custom level	Takes effect and you restart internet explorer
	Reset custom settings
Reset all zo	Reset to: Medium-low (default) Reset
	OK Cancel
OK	

Mozilla Firefox

1. Firefoxを開き、アドレ**スバーに**about:configと入力します。



2. [I'll be careful, I promise!] をクリックします。

<u> </u>	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!				

3. 変更するには、プリファレンス名network.negotiate-auth.allow-non-fqdnをtrueに、 network.negotiate-auth.trusted-urisをciscolive.com,adfs1.ciscolive.comにダブルクリックし ます。

Seagch: 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.ntim.send-im-response	default	boolean	false

4. Firefox を閉じ、再度開きます。

確認

AD FS サーバの SPN が正しく作成されたことを確認するために、setspn コマンドを入力し、出力を表示します。



クライアント マシンが Kerberos チケットを持っているかどうか確認します。

C:\Windows\system32\cmd.exe	
C:\Users\user1.CISCOLIVE>Klist tickets	*
Current LogonId is 0:0xabc6d	
Cached Tickets: <2>	
#0> Client: user1 @ CISCOLIUE.COM Server: krbtgt/CISCOLIUE.COM @ CISCOLIUE.COM KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96 Ticket Flags 0x40e00000 -> 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	
#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>	

これらの手順を完了し、どの認証(Kerberos または NTLM 認証)が使用されているか検証します。

- 1. クライアント マシンに Fiddler ツールをダウンロードしてインストールします。
- 2. すべての Microsoft Internet Explorer ウィンドウを閉じます。
- 3. Fiddler ツールを実行し、[File] メニューの [Capture Traffic] オプションが有効であることを 確認します。Fiddler は、クライアント マシンとサーバ間でパススループロキシとして動作 し、すべてのトラフィックをリッスンします。
- 4. Microsoft Internet Explorer を開いてから CUCM を参照し、リンクをいくつかクリックして トラフィックを生成します。
- 5. Fiddler のメイン ウィンドウに戻り、結果が 200 (成功)であるいずれかのフレームを選択 すると、Kerberos が認証メカニズムであることがわかります。

🚸 Fi	ddler Web I	Debugger				
File	Edit Rules	Tools Vie	ew Help GET /bo	ok 🔛 GeoEdge		
Q 4	PReplay	X • 🕨 😡	ا 🏶 Stream 🚻 🕻	Decode Keep: All sessions	() Any	ıy Process 🏦 Find 😡 Save 🗟 🕐 🏉 Browse 🔹 🕀 Clear Cache 🎢 TextWizard 🛃 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	cucm.ciscolive	/favicon.ico	1	the Desire to the second of the second
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:
1≤6	302	HTTPS	cucm.ciscolive	/ccmadmin/showHome.do		4D 53 53 50 00 03 00 00 00 00 00 00 00 58 00 00 MSSPX.
57	302	HTTPS	cucm.ciscolive	/ssosp/saml/login?relayurl		00 00 00 00 00 58 00 00 00 00 00 00 58 00 00XX
1 8	200	HTTP	Tunnel to	adfs1.ciscolive.com:443		00 00 00 00 00 58 00 00 00 15 C2 88 E2 06 01 B1X
59	302	HTTPS	adfs1.ciscoliv	/adfs/ls/?SAMLRequest=n		1D 00 00 00 0F 7E AF 60 90 3B D7 F3 E2 F4 5E 84~ ;x080^
2 1	0 401	HTTPS	adfs1.ciscoliv	/adfs/ls/auth/integrated/?	- E	50 2D 22 9A 84 00 00 00 00 P-"
21	1 401	HTTPS	adfs1.ciscoliv	/adfs/ls/auth/integrated/?	- 7	
<۵1	2 200	HTTPS	adfs1.ciscoliv	/adfs/ls/auth/integrated/?		Cat Contaution Transformer Handers Tauthien Imagelian Hanitan Wahilian
01	3 502	HTTP	www.downioa	/msdownload/update/v3/s		decisivitative inalisionen neues rettiew inageview netwew viewew
1 1	4 401	HTTPS	adfs1.ciscoliv	/favicon.ico	- E	Auth Cadhing 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 Kerbergs reply:
21	7 403	HTTPS	cucm.ciscolive	/ssosp/relay	- 1	A1 18 30 19 A0 03 0A 01 00 A3 12 04 10 01 00 00 i.0
11	8 200	HTTPS	cucm.ciscolive	/ciscologo.gif		00 43 87 E0 88 C1 36 E3 A9 00 00 00 00 00 .C a A6d0
Ø	9 502	HTTP	www.downloa	/msdownload/update/v3/s		
02	0 502	HTTP	www.downloa	/msdownload/update/v3/s	_	
					. A	
					<u> </u>	
Quid	(Exec] ALT+(Q > type HE	LP			P
₩, C	apturing	👻 All Proce	5965	1 / 20 Download Progress	: 0 byter	s. Ht F5 to refresh.

6. 認証タイプが NTLM の場合、次のようにフレームの先頭に [Negotiate - NTLMSSP] と表示 されます。

🚸 Fiddl	er Web D	ebugger					×
File Edi	t Rules	Tools Vie	ew Help GET/bo	ok 🔛 GeoEdge			
Q fy F	teplay >	<- 🕨 Go	🔹 Stream 👹	Decode Keep: All sessions *	🕀 Any F	Process 😤 Find 😹 Save 🛛 🎼 🕐 🏉 Browse 🔹 🕀 Clear Cache 🎢 TextWizard 🛛 🛃 Tearoff	Ŧ
	Result	Protocol	Host	URL	B	🔊 Statistics 📲 Inspectors 🖌 🐔 AutoResponder 🗐 🏹 Composer 🗍 🗖 Filters 🗍 🗉 Log 📜 💳 Timeline	1
Ø1	502	HTTP	www.bing.com	/favicon.ico	H	readers TextView WebForms HexView Auth Cookies Raw JSON XML	
≪≯2	200	HTTP	cucm.ciscolive	1	5,		_
2 3	200	HTTP	cucm.ciscolive	/ciscologo.gif		No Proxy-Authorization Header is present.	4
= 4	200	HTTP	cucm.ciscolive	/favicon.ico	1,	Authorization Header is present: NTLM	
N 5	302	HTTP	cucm.ciscolive	/comadmin/showHome.do		16 54 4C 40 53 53 50 00 03 00 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 XX.	
07	502	HTTP	www.downloa	/msdownload/update/v3/s		38 00 00 00 00 00 00 00 58 00 00 05 C2 88 A2 X	
58	302	HTTPS	cucm.ciscolive	/conadmin/showHome.do	7	78 AA CE A9 41 F3 D1 31 X°18AÓÑ1	
59	302	HTTPS	cucm.ciscolive	/ssosp/saml/login?relayurl			
一 10	200	HTTP	Tunnel to	adfs1.ciscolive.com:443		[NTLM Type3: Authentication]	•
5 11	302	HTTPS	adfs1.ciscoliv	/adfs/ls/?SAMLRequest=n			_
1 12	401	HTTPS	adfs1.ciscoliv	/adfs/ls/auth/integrated/?	6,1	et Syntaxview Transformer Headers Textview Imageview Hexview Webview	
1 13	401	HTTPS	adfs1.ciscoliv	/adfs/ls/auth/integrated/?	7, A	with Caching Cookies Raw JSON XML	
<≯14	200	HTTPS	adfs1.ciscoliv	/adfs/ls/auth/integrated/?	9,1	Response Headers [Rew1] Header Definition	
15	401	HTTPS	adfs1.ciscoliv	/favicon.ico	6,	TTP/1.1 200 OK	-
16	200	HTTP	Tunnel to	cucm.ciscolive.com:8443		Carthe	
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	-
19	200	HTTPS	cucm.ciscolive	/ciscologo.gif		Expires: -1	
						Pragma: no-cache	2,
4					<u> </u>	Condities / Lonin	-
[QuidExt	c] ALT+C	> type HE	LP		1	<u> </u>	
Tie Canh	ring	Al Proce	sses	1/19 https://adfs1.ciscol	e.com/e	dfs//s/auth/integrated/75AMLRequest=n/LLbtswELznKwiebYrvIwphGX8sFDWONErk9NDbi48CR55V1p%28%	2

トラブルシュート

このドキュメントの記載に従って、すべての設定手順および検証手順を完了してもまだログイン の問題が発生する場合は、Microsoft Windows の Active Directory / AD FS 管理者に相談する必要 があります。