Configurazione dell'installazione di SAML SSO con autenticazione Kerberos

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Configurazione Configurare ADFS Configura browser Microsoft Internet Explorer Mozilla Firefox Verifica Risoluzione dei problemi

Introduzione

In questo documento viene descritto come configurare Active Directory e Active Directory Federation Service (ADFS) versione 2.0 in modo da consentire l'utilizzo dell'autenticazione Kerberos da parte dei client Jabber (solo Microsoft Windows), che consente agli utenti di eseguire l'accesso con l'accesso a Microsoft Windows senza che vengano richieste le credenziali.

Attenzione: Questo documento si basa su un ambiente lab e presuppone che l'utente sia a conoscenza dell'impatto delle modifiche apportate. Per comprendere l'impatto delle modifiche apportate, consultare la documentazione del prodotto in uso.

Prerequisiti

Requisiti

Cisco raccomanda:

- AD FS versione 2.0 installato e configurato con i prodotti Cisco Collaboration come attendibilità componente
- Prodotti per la collaborazione come Cisco Unified Communications Manager (CUCM), IM e Presenza, Cisco Unity Connection (UCXN) e CUCM abilitati per l'utilizzo di SAML (Security Assertion Markup Language) Single Sign-On (SSO)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Active Directory 2008 (nome host: ADFS1.ciscolive.com)
- AD FS versione 2.0 (nome host: ADFS1.ciscolive.com)
- CUCM (nome host: CUCM1.ciscolive.com)
- Microsoft Internet Explorer versione 10
- Mozilla Firefox versione 34
- Telerik Fiddler versione 4

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Configurare ADFS

1. Configurare AD FS versione 2.0 con il nome dell'entità servizio (SPN) per consentire al computer client in cui è installato Jabber di richiedere i ticket, che a sua volta consente al computer client di comunicare con un servizio AD FS.



Per ulteriori informazioni, fare riferimento al documento <u>ADFS 2.0: Come configurare l'SPN</u> (servicePrincipalName) per l'account del servizio per ulteriori informazioni.

 Verificare che la configurazione di autenticazione predefinita per il servizio AD FS (in C:\inetpub\adfs\ls\web.config) sia Autenticazione integrata di Windows. Verificare che non sia stata modificata in Autenticazione basata su form.

<pre><microsoft.identityserver.web> <localauthenticationtypes> <add name="Integrated" page="auth/integrated/"></add></localauthenticationtypes></microsoft.identityserver.web></pre>

<add name="fischent" page="auth/ssichent/"></add>
<add name="Basic" page="auth/basic/"></add>
<commondomaincookie reader="" writer=""></commondomaincookie>
<context hidden="true"></context>
<error page="Error.aspx"></error>
<pre><acceptedfederationprotocols saml="true" wsfederation="true"></acceptedfederationprotocols></pre>
<pre><homerealmdiscovery page="HomeRealmDiscovery.aspx"></homerealmdiscovery></pre>
<pre><pre><pre><pre>sistIdentityProviderInformation enabled="true" lifetimeInDays="30" /></pre></pre></pre></pre>
<pre><singlesignon_enabled="true"></singlesignon_enabled="true"></pre>

 Selezionare Autenticazione di Windows e fare clic su Impostazioni avanzate nel riquadro di destra. In Impostazioni avanzate, deselezionare Abilita autenticazione in modalità kernel, accertarsi che la protezione estesa sia disattivata e fare clic su OK.



4. Verificare che AD FS versione 2.0 supporti sia il protocollo Kerberos che il protocollo NTLM (NT LAN Manager), poiché tutti i client non Windows non possono utilizzare Kerberos e si basano su NTLM.

Nel riquadro di destra, selezionare **Provider** e assicurarsi che **Negotiate** e **NTLM** siano presenti in Provider abilitati:



Nota: ADFS passa l'intestazione di sicurezza Negotiate quando viene utilizzata l'autenticazione integrata di Windows per autenticare le richieste client. L'intestazione Negotiate consente ai client di scegliere tra l'autenticazione Kerberos e l'autenticazione NTLM. Il processo Negotiate seleziona l'autenticazione Kerberos a meno che non si verifichi una delle seguenti condizioni:

- Uno dei sistemi coinvolti nell'autenticazione non può utilizzare l'autenticazione Kerberos.

- L'applicazione chiamante non fornisce informazioni sufficienti per utilizzare l'autenticazione Kerberos.

- Per consentire al processo Negotiate di selezionare il protocollo Kerberos per l'autenticazione di rete, l'applicazione client deve fornire un nome SPN, un nome dell'entità utente (UPN) o un nome account NetBIOS (Network Basic Input/Output System) come nome della destinazione. In caso contrario, il processo Negotiate seleziona sempre il protocollo NTLM come metodo di autenticazione preferito.

Configura browser

Microsoft Internet Explorer

1. Verificare che Internet Explorer > Avanzate > Abilita autenticazione integrata di Windows sia selezionato.

Internet Options					
General Security Privacy Content Connections Programs Advanced					
Settings					
 Do not submit unknown addresses to your auto-search province 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 					
 Check for signatures on downloaded programs Do not save encrypted pages to disk Empty Temporary Internet Files folder when browser is dc 					
 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. Aggiungere l'URL ADFS in **Protezione >Aree Intranet > Siti**.

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 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)				
What are intranet settings? Advanced OK Cancel				
Local intranet 💌	Γ			
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:				
Remove				

3. Aggiungere i nomi host CUCM, IMP e Unity a Sicurezza >Siti attendibili.

Internet Options	8 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			
Trusted sites				
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:				
Websites:				
cucm1.ciscolive.com	Remove			
imp1.ciscolive.com				
ucxn1.ciscolive.com				
Require server verification (https:) for all sites in this	zone			
	Close			

4. Verificare che Internet Explorer > protezione > Intranet locale > Impostazioni protezione > Autenticazione utente - Accesso sia configurato per utilizzare le credenziali di accesso per i siti Intranet.

Internet Options	83
General Security Privacy Content Connections	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
found on your intranet.	 Disable
	Enable
Security level for this zone	O Prompt
Allowed levels for this zone: All	Set Logon
- Medium-low	Anonymous logon
Appropriate for websites on your	Automatic logon only in Intranet zone
- Most content will be run without p	Automatic logon with current user name and password
- Unsigned ActiveX controls will not	Prompt for user name and password T
- Same as Medium level without pro	< •
Enable Protected Mode (requires restartin	*Takes effect after you restart Internet Explorer
Custom level	Reset custom settings
Reset all zo	Reset to: Medium-low (default) Reset
ОК	OK Cancel

Mozilla Firefox

1. Aprire Firefox e immettere **about:config** nella barra degli indirizzi.



2. Clicca su Attenzione, te lo prometto!

	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!

 Fare doppio clic sul nome della preferenza network.negotiation-auth.allow-non-fqdn su true e network.negotiation-auth.trusted-uris su ciscolive.com,adfs1.ciscolive.com per apportare modifiche.

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-Im-response	default	boolean	false

4. Chiudere Firefox e riaprire.

Verifica

Per verificare che gli SPN per il server AD FS siano stati creati correttamente, immettere il comando **setspn** e visualizzare l'output.



Verificare se i computer client dispongono di ticket 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>	

Completare questa procedura per verificare quale autenticazione (Kerberos o NTLM) è in uso.

- 1. Scaricare lo strumento Fiddler sul computer client e installarlo.
- 2. Chiudere tutte le finestre di Microsoft Internet Explorer.
- 3. Eseguire lo strumento Trova e verificare che l'opzione **Cattura traffico** sia attivata nel menu File. Fiddler funge da proxy pass-through tra il computer client e il server ed è in ascolto di tutto il traffico.
- 4. Aprire Microsoft Internet Explorer, sfogliare il CUCM e fare clic su alcuni collegamenti per generare traffico.
- Fare riferimento alla finestra principale del Finder e scegliere uno dei Frame in cui il risultato è 200 (operazione riuscita); è possibile visualizzare Kerberos come meccanismo di autenticazione



6. Se il tipo di autenticazione è NTLM, all'inizio del frame viene visualizzato **Negotiate - NTLMSSP**, come mostrato di seguito.

🚸 Fiddl	er Web C	ebugger			
File Ed	it Rules	Tools Vie	ew Help GET/bo	ok 🔛 GeoEdge	
Q fy P	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	5, No Denni Authorization Handra in constant
23	200	HTTP	cucm.ciscolive	/ciscologo.gif	NO Proxy-Authorization Header is present.
= 4	200	HTTP	cucm.ciscolive	/favicon.ico	1, Authorization Header is present: NTLM
N 5	302	HTTP	cucm.ciscolive	/ccmadmin/showHome.do	58 00 00 00 00 00 00 058 00 00 00 00 00 00 00 00 00 00 00 00 00
<u>6 (11)</u>	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	нттр	www.downloa	/msdownload/update/v3/s	06 01 81 1D 00 00 00 0F 4E 84 C3 AA 0D D1 81 34
58	302	HTTPS	cucm.ciscolive	/comadmin/showHome.do	78 AA CE A9 41 F3 D1 31 Xº18AÓÑ1
59	302	HTTPS	cucm.ciscolive	/ssosp/saml/login?relayurl	
10	200	HTTP	Tunnel to	adfs1.ciscolive.com:443	-[NTLM Type3: Authentication]
5 11	302	HTTPS	adfs1.ciscoliv	/adfs/ls/?5AMLRequest=n	Cat Controlling Transformer Distant Textiling Impaction Hading Webling
12 12	401	HTTPS	adfs1.ciscoliv	/adfs/ls/auth/integrated/?	6, Get Syntaxvew Transformer Treaders Textvew Imageview Hexvew Vietovew
13	401	HTTPS	adfs1.ciscoliv	/adfs/ls/auth/integrated/?	7, Auth Caching Cookies Raw JSON XML
<> 14	200	HTTPS	adfs1.ciscoliv	/adfs/ls/auth/integrated/?	9/ Response Headers [Raw] [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
[Quid:Exe	ec] ALT+C) > type HE	LP		
Tie Capb	uring	Al Proce	sses	1 / 19 https://adfs1.ciscol	olive.com/adfs/(s/auth/integrated/7SAMLRequest=nVLLbtswELznKw/ebYryIwphGXBsFDWQNErk9NDbl/4BCR55VJp%28%

Risoluzione dei problemi

Se tutte le operazioni di configurazione e verifica vengono completate come descritto in questo documento e si verificano ancora problemi di accesso, è necessario rivolgersi a un amministratore di Microsoft Windows Active Directory o AD FS.