Configurar SAML SSO com autenticação Kerberos

Contents

Introduction Prerequisites Requirements Componentes Utilizados Configurar Configurar o AD FS Configurar navegador Microsoft Internet Explorer Mozilla FireFox Verificar Troubleshoot

Introduction

Este documento descreve como configurar o Ative Diretory e o Ative Diretory Federation Service (AD FS) Versão 2.0 para permitir que ele use a autenticação Kerberos por clientes Jabber (Microsoft Windows apenas), que permite que os usuários façam login com seu login do Microsoft Windows e não sejam solicitados a fornecer credenciais.

Caution: Este documento é baseado em um ambiente de laboratório e pressupõe que você está ciente do impacto das alterações feitas. Consulte a documentação relevante do produto para entender o impacto das alterações feitas.

Prerequisites

Requirements

A Cisco recomenda que você:

- O AD FS Versão 2.0 foi instalado e configurado com os produtos Cisco Collaboration como Confiança de terceira parte confiável
- Produtos de colaboração como Cisco Unified Communications Manager (CUCM) IM and Presence, Cisco Unity Connection (UCXN) e CUCM habilitados para usar o Security Assertion Markup Language (SAML) Single Sign-on (SSO)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Ative Diretory 2008 (nome de host: ADFS1.ciscolive.com)
- AD FS Versão 2.0 (Nome do host: ADFS1.ciscolive.com)
- CUCM (nome de host: CUCM1.ciscolive.com)
- Microsoft Internet Explorer versão 10
- Mozilla Firefox versão 34
- Telerik Fiddler versão 4

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.

Configurar

Configurar o AD FS

1. Configure o AD FS Versão 2.0 com Service Principal Name (SPN) para habilitar o computador cliente no qual o Jabber está instalado para solicitar tíquetes, o que, por sua vez, permite que o computador cliente se comunique com um serviço do AD FS.



Consulte o <u>AD FS 2.0: Como configurar o SPN (servicePrincipalName) para a conta de</u> <u>serviço</u> para obter mais informações.

 Certifique-se de que a configuração de autenticação predefinida para o serviço AD FS (em C:\inetpub\adfs\ls\web.config) é Autenticação Integrada do Windows. Verifique se ele não foi alterado para Autenticação baseada em formulário.

<pre><microsoft.identityserver.web> <localauthenticationtypes> <add name="Integrated" page="auth/integrated/"></add></localauthenticationtypes></microsoft.identityserver.web></pre>
<add name="Forms" page="FormsSignIn.aspx"></add>
<add name="TlsClient" page="auth/sslclient/"></add>
<add name="Basic" page="auth/basic/"></add>
<commondomaincookie reader="" writer=""></commondomaincookie>
<context hidden="true"></context>
<pre><error page="Error.aspx"></error></pre>
<pre><acceptedfederationprotocols saml="true" wsfederation="true"></acceptedfederationprotocols></pre>
<pre><homerealmdiscovery page="HomeRealmDiscovery.aspx"></homerealmdiscovery></pre>
<pre><persistidentityproviderinformation enabled="true" lifetimeindays="30"></persistidentityproviderinformation></pre>
<pre><singlesignon enabled="true"></singlesignon></pre>

 Selecione Autenticação do Windows e clique em Configurações avançadas no painel direito. Em Advanced Settings (Configurações avançadas), desmarque Enable Kernel-mode authentication, verifique se Extended Protection está desativado e clique em OK.



 Certifique-se de que o AD FS Versão 2.0 suporta o protocolo Kerberos e o protocolo NT LAN Manager (NTLM) porque todos os clientes não Windows não podem usar Kerberos e dependem do NTLM.

No painel direito, selecione **Provedores** e verifique se **Negociar** e **NTLM** estão presentes em Provedores Habilitados:



Note: O AD FS passa o cabeçalho de segurança Negociar quando a autenticação integrada do Windows é usada para autenticar solicitações de clientes. O cabeçalho de segurança Negociar permite que os clientes selecionem entre a autenticação Kerberos e a autenticação NTLM. O processo Negociar seleciona a autenticação Kerberos, a menos que uma destas condições seja verdadeira:

- Um dos sistemas envolvidos na autenticação não pode usar a autenticação Kerberos.

- O aplicativo de chamada não fornece informações suficientes para usar a autenticação Kerberos.

 Para permitir que o processo de negociação selecione o protocolo Kerberos para autenticação de rede, o aplicativo cliente deve fornecer um SPN, um UPN (User Principal Name, nome principal do usuário) ou um NetBIOS (Network Basic Input/Output System, sistema básico de entradas e saídas) como o nome de destino. Caso contrário, o processo Negociar sempre seleciona o protocolo NTLM como o método de autenticação preferencial.

Configurar navegador

Microsoft Internet Explorer

1. Verifique se Internet Explorer > Advanced > Enable Integrated Windows Authentication está marcado.

Internet Options					
General Security Privacy Content Connections Programs Advanced					
Settings					
 Do not submit unknown addresses to your auto-search prove 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 dc Enable DOM Storage					
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. Adicione a URL do AD FS em **Segurança >Zonas de intranet > sites**.

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.
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

3. Adicione os nomes de host CUCM, IMP e Unity a Segurança >Sites confiáveis.

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						
Trusted 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						

 Certifique-se de que o Internet Explorer > segurança > Intranet local > Configurações de segurança > Autenticação do usuário - Logon esteja configurado para usar as credenciais de login para sites de intranet.

Internet Options	
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
found on your intranet.	 Disable
	Enable
Security level for this zone	Prompt
Allowed levels for this zone: All	& Logon
- Medium-low	C 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
- Unsigned ActiveX controls will not - Same as Medium level without pro	
Enable Protected Mode (requires restartin	* III P
Custom level	Takes effect after you restart internet explorer
	Reset custom settings
Reset all zo	Reset to: Medium-low (default) Reset
	OK Cancel
OK	

Mozilla FireFox

1. Abra o Firefox e digite **about:config** na barra de endereços.



2. Clique em Eu serei cuidadoso, prometo!

	Here be dragons!		
<u> </u>	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. Clique duas vezes no nome de preferência **network.negotiation-auth.allow-non-fqdn** para **true** e **network.negotiation-auth.trust-uris** para **ciscolive.com,adfs1.ciscolive.com** para modificar.

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. Feche o Firefox e reabra.

Verificar

Para verificar se os SPNs do servidor AD FS foram criados corretamente, insira o comando **setspn** e exiba a saída.



Verifique se as máquinas clientes têm tíquetes Kerberos:

C:\Win	ndows\system32\cmd.exe	d 🔀
C:\Users	s\user1.CISCOLIVE>Klist tickets	-
Current	LogonId is 0:0xabc6d	
Cached 1	Tickets: <2>	
#0>	Client: user1 @ CISCOLIUE.COM Server: krbtgt/CISCOLIUE.COM @ CISCOLIUE.COM KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96 Ticket Flags Øx40e00000 -> forwardable renewable initial pre_authen 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	t E
#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	s\user1.CISCOLIVE>_	

Conclua estes passos para verificar qual autenticação (autenticação Kerberos ou NTLM) está sendo usada.

- 1. Baixe a ferramenta Fiddler na sua máquina cliente e instale-a.
- 2. Feche todas as janelas do Microsoft Internet Explorer.
- 3. Execute a ferramenta Fiddler e verifique se a opção **Capture Traffic** está ativada no menu File (Arquivo). O Fiddler funciona como um proxy de passagem entre a máquina cliente e o servidor e escuta todo o tráfego.
- 4. Abra o Microsoft Internet Explorer, navegue até o CUCM e clique em alguns links para gerar tráfego.
- 5. Consulte a janela principal do Fiddler e escolha um dos Quadros em que o Resultado é **200** (sucesso) e você pode ver Kerberos como Mecanismo de Autenticação



6. Se o tipo de autenticação for NTLM, você verá **Negotiate - NTLMSSP** no início do quadro, como mostrado aqui.

🚸 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%

Troubleshoot

Se todas as etapas de configuração e verificação forem concluídas conforme descrito neste documento e você ainda tiver problemas de login, consulte um Administrador do Microsoft Windows Ative Diretory / AD FS.