Kerberos with ADFS 2.0 for End User SAML SSO for Jabber Configuration Example

Contents

Introduction
Prerequisites
Requirements
Components Used
Background Information
Configuration
Verify
Troubleshoot

Introduction

This document describes how to configure Kerberos with Active Directory Federation Services (ADFS) 2.0.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

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.

Background Information

End User Security Assertion Markup Language (SAML) Single Sign On (SSO) configuration requires Kerberos to be configured in order to allow End User SAML SSO for Jabber to work with domain authentication. When SAML SSO is implemented with Kerberos, Lightweight Directory
Access Protocol (LDAP) handles all the authorization and user synchronization, while Kerberos manages authentication. Kerberos is an authentication protocol that is meant to be used in conjunction with an LDAP-enabled instance.

On Microsoft Windows and Macintosh machines that are joined to an Active Directory domain, users can seamlessly log into Cisco Jabber without the requirement to enter a username or password and they do not even see a login screen. Users who are not logged into the domain on their computers still see a standard login form.

Because authentication uses a single token passed from the operating systems, no redirect is required. The token is verified against the configured Key Domain Controller (KDC), and if it is valid, the user is logged in.

Configuration

Here is the procedure to configure Kerberos with ADFS 2.0.

1. Install Microsoft Windows Server 2008 R2 on a machine.

2. Install Active Directory Domain Services (ADDS) and ADFS on the same machine.

3. Install Internet Information Services (IIS) on the Microsoft Windows Server 2008 R2-installed machine.

4. Create a self-signed certificate for IIS.

5. Import the self-signed certificate into IIS and use it as the HTTPS server certificate.

6. Install Microsoft Windows7 on another machine and use it as a client.

   Change the Domain Name Server (DNS) to the machine where you installed ADDS.

   Add this machine to the domain you created in the installation of ADDS.

   Go to Start. Right-click Computer. Click Properties. Click Change Settings on the right-hand side of window. Click the Computer Name tab. Click Change. Add the domain you created.
7. Check whether the Kerberos service generates on both machines.

Log in as administrator on the server machine and open the command prompt. Then execute these commands:

```
cd \windows\System32\Klist tickets
```

```
C:\Users\Administrator.WIN2K8>cd \windows\System32
C:\Windows\System32>Klist tickets
Current LogonId is 0:0x3d6072
Cached Tickets: <1>

#0>  Client: Administrator@MANGOLAB.COM
     Server: krbtgt/MANGOLAB.COM@MANGOLAB.COM
     KerbTicket Encryption Type: AES-256-CBC-HMAC-SHA1-96
     Ticket Flags 0x40000000 -> forwardable renewable initial pre_authent
     Start Time: 12/10/2014 18:06:04 (local)
     End Time: 12/11/2014 4:06:04 (local)
     Renew Time: 12/17/2014 18:06:04 (local)
     Session Key Type: AES-256-CBC-HMAC-SHA1-96
```

Log in as domain user on the client machine and execute the same commands.
8. Create the ADFS Kerberos identity on the machine where you installed ADDS.

The Microsoft Windows administrator logged into the Microsoft Windows domain (as <domainname>\administrator), for example on the Microsoft Windows domain controller, creates the ADFS Kerberos identity. The ADFS HTTP service must have a Kerberos identity called a Service Principal Name (SPN) in this format: HTTP/DNS_name_of_ADFS_server.

This name must be mapped to the Active Directory user that represents the ADFS HTTP server instance. Use the Microsoft Windows setspn utility, which should be available by
default on a Microsoft Windows 2008 Server.

Procedure Register the SPNs for the ADFS server. On the Active Directory domain controller, run the `setspn` command.

For example, when the ADFS host is `adfs01.us.renovations.com`, and the Active Directory domain is `US.RENOVATIONS.COM`, the command is:

```
setspn -a HTTP/adfs01.us.renovations.com <ActiveDirectory user>
setspn -a HTTP/adfs01 <ActiveDirectory user>
```

The `HTTP/` portion of the SPN applies, even though the ADFS server is typically accessed by Secure Sockets Layer (SSL), which is HTTPS.

Check that the SPNs for the ADFS server are properly created with the `setspn` command and view the output.

```
setspn -L <ActiveDirectory user>
```

![Registered ServicePrincipalNames for CN=WIN2K8,OU=Domain Controllers,DC=mangolab]  
Registered ServicePrincipalNames for CN=WIN2K8,OU=Domain Controllers,DC=mangolab:  
HTTP/win2k8.mangolab.com  
ldap/win2k8.mangolab.com/ForestDnsZones.mangolab.com  
ldap/win2k8.mangolab.com/DomaiDnsZones.mangolab.com  
TERMSRU/WIN2K8  
TERMSRU/win2k8.mangolab.com  
Dns/win2k8.mangolab.com  
CC/win2k8.mangolab.com/Mangolab.com  
RestrictedKrbHost/win2k8.mangolab.com  
RestrictedKrbHost/WIN2K8  
HOST/WIN2K8/MANGOLAB  
HOST/win2k8.mangolab.com/MANGOLAB  
HOST/WIN2K8  
HOST/win2k8.mangolab.com  
E3514235-48DB-11D1-AD04-00C04FC2C0E2/df771b0f-5bf5-4dc3-b472-562f92383774  
Mangolab.com  

9. Configure the browser settings of the Microsoft Windows Client.

Navigate to **Tools > InternetOptions > Advanced** in order to enable Integrated Windows Authentication.

Check the **Enable Integrated Windows Authentication check box**:
Navigate to **Tools > Internet Options > Security > Local intranet > Custom level...** in order to select **Automatic logon only in Intranet zone.**
Navigate to Tools > Internet Options > Security > Local intranet > Sites > Advanced in order to add the Intrusion Detection & Prevention (IDP) URL to Local intranet sites.

**Note:** Check all of the check boxes in the Local intranet dialog box and click the Advanced tab.

Navigate to Tools > Security > Trusted sites > Sites in order to add the CUCM hostnames to Trusted sites:
Verify

This section explains how to verify which authentication (Kerberos or NT LAN Manager (NTLM) authentication) is used.

1. Download the Fiddler Tool to your client machine and install it.

2. Close all Internet Explorer windows.

3. Run the Fiddler Tool and check that the **Capture Traffic** option is enabled under the File menu.

   Fiddler works as a pass-through proxy between the client machine and the server and listens to all traffic, which temporarily sets your Internet Explorer Settings like this:
4. Open Internet Explorer, browse into your Customer Relationship Management (CRM) Server URL, and click a few links in order to generate traffic.

5. Refer back to the Fiddler main window and choose one of the Frames where the Result is 200 (success):
If the Authentication type is NTLM, then you see **Negotiate - NTLMSSP** in the beginning of the frame, as shown here:

**Troubleshoot**

There is currently no specific troubleshooting information available for this configuration.