与ADFS 2.0的Kerberos最终用户Jabber配置示例的SAML SSO的

目录

简介

本文描述如何配置与活动目录联邦服务(ADFS)的Kerberos 2.0。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

在(SSO)配置的最终用户安全断言标记语言(SAML)单个符号要求将配置的Kerberos为了允许最终用户SAML SSO Jabber与域认证一起使用。当SAML SSO实现与Kerberos时，轻量级目录访问协议(LDAP)处理所有授权和用户同步，而Kerberos管理验证。Kerberos是被认为与一个支持LDAP的实例一道使用的认证协议。

在加入对活动目录域的Microsoft Windows和麦金塔机器上，用户能无缝地登录思科Jabber，不用需求输入用户名或密码和他们没有均等看到登录画面。仍然没有登录在他们的计算机的域的用户看到一标准的登录表。

由于验证使用从操作系统通过的单个标记，重定向没有要求。标记验证已配置的关键域控制器(KDC)，并且，如果有效，用户登陆。

配置

这是配置与ADFS 2.0的Kerberos的步骤。

1. 安装MS Windows服务器在计算机的2008个R2。

2. 安装活动目录域在同样计算机的服务(添加)和ADFS。

3. 安装互联网信息服务(IIS)在MS Windows服务器2008 R2-installed计算机。

4. 创建IIS的一自签名证书。

5. 导入自签名证书到IIS并且请使用它作为HTTPS服务器证书。

6. 安装在另一计算机的Microsoft Windows7并且请使用它作为客户端。

   更改域名服务器(DNS)对您安装添加的计算机。

   添加此计算机到您在ADDS的安装中创建的域。

   去**开始**。用鼠标右键单击**计算机**。单击 **Properties**。点击在窗口右边的**崔凡吉莱设置**。单击 **Computer Name** 选项卡。单击 **Change**。添加您创建的域。

7. 证实Kerberos服务是否在两台机器生成。

   登陆作为服务器设备的管理员并且打开prompt命令。然后请执行这些命令：

   cd \windows\System32Klist票

   登陆作为客户端机器的域用户并且执行同样命令。

8. 创建在您安装添加的计算机的ADFS Kerberos标识。

   Microsoft Windows管理员登录Microsoft Windows域(作为<domainname> \管理员)，例如在

Microsoft Windows域控制器，创建ADFS Kerberos标识。ADFS HTTP服务必须有呼叫一服务主体名称的Kerberos标识(SPN)在此格式：**HTTP/DNS_name_of_ADFS_server**.

必须映射此名称对代表ADFS HTTP服务器实例的活动目录用户。请使用Microsoft Windows **setspn**工具，默认情况下应该取得到在Microsoft Windows 2008服务器。

步骤 注册ADFS服务器的SPNs。在活动目录域控制器上，请运行**setspn**命令。

例如，当ADFS主机是**adfs01.us.renovations.com时**和活动目录域是**US.RENOVATIONS.COM，命令是：**

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

SPN的**HTTP**部分应用，即使ADFS服务器由安全套接字协议层(SSL)典型地访问，是HTTPS。

检查ADFS服务器的SPNs用**setspn**命令适当地创建并且查看输出。

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

9. 配置Microsoft Windows客户机的浏览器设置。

导航对**Tools> InternetOptions >Advanced**为了启用集成Windows验证。

检查**Enable (event)集成的Windows Authentication复选框**：

导航对**工具> Internet选项> Security >本地级内联网>的自定义…**为了选择仅**自动登录在内联网区域**。

导航对**工具> Internet选项> Security >本地内联网>站点>Advanced**为了添加入侵检测&预防(IDP) URL到本地内联网站点。

Note:检查所有在本地内联网对话框的复选框并且点击**高级选项卡**。

导航到**Tools > Security >可信的站点>站点**为了添加CUCM主机名到可信的站点：

验证

验证的此部分说明如何验证(Kerberos或NT LAN Manager (NTLM)验证)使用。

1. 下载提琴手工具到您的客户端机器并且安装它。

2. 关闭所有 Internet Explorer 窗口。

3. 运行提琴手工具并且检查**捕获流量**选项启用在文件菜单下。

   提琴手工作作为在客户端机器和服务器之间的转接代理并且听所有流量，临时地设您的象这样的Internet Explorer设置：

4. 打开Internet Explorer，浏览到您的用户关系管理(CRM)服务器URL，并且点击一些条链路为了生成流量。

5. 参考回到提琴手主窗口并且选择结果是200的其中一帧(成功) ：

   如果认证类型是NTLM，则您看到**协商- NTLMSSP**在帧的开头部分，如显示此处：

故障排除

目前没有针对此配置的故障排除信息。