SAML SSO设置Kerberos认证配置示例

目录

简介

本文描述如何配置活动目录和活动目录联邦服务(AD FS)版本2.0为了使它由Jabber客户端(仅Microsoft Windows使用Kerberos认证)，允许用户登陆与他们的Microsoft Windows登录和不提示输入凭证。

> **警告：**本文根据实验室环境并且假设，您知道您做变动的影响。参考相关产品文档为了了解您做变动的影响。

先决条件

要求

Cisco 建议您：

- AD用Cisco协作产品安装和配置的FS版本2.0作为取决于Party信任
- 协作产品例如Cisco Unified Communications Manager (CUCM) IM和在线状态、启用的Cisco Unity Connection (UCXN)和CUCM为了使用安全断言标记语言(SAML)单一登录(SSO)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 活动目录2008年(主机名：ADFS1.ciscolive.com)

- AD FS版本2.0 (主机名：ADFS1.ciscolive.com)
- CUCM (主机名：CUCM1.ciscolive.com)
- 微软Internet Explorer版本10
- Mozilla Firefox版本34
- Telerik提琴手版本4

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。

配置

配置AD FS

1. 配置AD与服务主体名称(SPN)的FS版本2.0为了启用Jabber安装请求票，反过来使客户端计算机与AD FS服务联络的客户端计算机。

   参考AD FS 2.0 ：如何配置SPN (servicePrincipalName)服务帐户的欲知更多信息。

2. 保证AD FS服务的默认验证配置(在**C:\inetpub\adfs\ls\web.config**)是**集成的Windows验证**。保证它未更改对**基于表的验证**。

3. 选择**Windows验证**并且单击**先进的设置**在右窗格下。在先进的设置，请不选定**Enable (event)内核模式验证**，确保延长的保护关掉，并且点击OK键。

4. 保证AD FS版本2.0支持Kerberos协议和NT LAN Manager (NTLM)协议，因为所有非Windows客户端在NTLM不能使用Kerberos和取决于。

   在右窗格中，请选择**供应商**并且确保**协商，**并且**NTLM**是存在已启用供应商下：

   注意：当集成Windows验证用于为了验证客户端的要求时， AD FS传递协商安全报头。协商安全报头让客户端精选在Kerberos认证和NTLM验证之间。除非这些情况之一是真的，协商进程选择Kerberos认证：

   -在验证涉及的其中一个系统不能使用Kerberos认证。

   -呼叫的应用程序不提供充足的信息使用Kerberos认证。

   -为了使协商进程选择网络验证的Kerberos协议，客户端应用必须提供SPN、用户主体名称

(UPN)，或者网络基本输入/输出系统(NetBIOS)帐户名作为目标名称。否则，协商进程总是选择NTLM协议作为首选的认证方法。

配置浏览器

Microsoft Internet Explorer

1. 保证**Internet Explorer** >Advanced >enable**集成的Windows验证**被检查。

2. 添加AD FS URL在**安全>Intranet区域>站点下**。

3. 添加CUCM、IMP和Unity主机名到**安全>Trusted站点**。

4. 保证**互联网Exporer** > Security **>本地内联网>** Security**设置>**用户认证**-登录**配置为了使用记录在凭证内联网站点。

Mozilla Firefox

1. 打开Firefox并且输入：**配置**在地址栏。

2. 点击**我小心，我承诺!**

3. 双击首选名称network.negotiate auth.allow非**FQDN对真和network.negotiate-auth.trusted-uris对ciscolive.com,adfs1.ciscolive.com为了**修改。

4. 结束Firefox并且重新打开。

验证

为了检查AD FS服务器的SPNs适当地创建，请输入**setspn**命令并且查看输出。

检查客户端机器是否有Kerberos票：

完成验证的这些步骤为了验证(Kerberos或NTLM验证)是在使用中的。

1. 下载提琴手工具到您的客户端机器并且安装它。

2. 关上所有微软Internet Explorer windows。

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。

4. 打开微软Internet Explorer，浏览到您的CUCM，并且点击一些链路为了生成流量。

5. 参考回到提琴手主窗口并且选择的其中一帧结果是**200** (成功)，并且您能看到Kerberos作为认证机制

6. 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

如果所有配置和验证步骤完成正如本文所描述，并且仍然有登录问题，则您必须咨询Microsoft Windows活动目录/AD FS管理员。