Cloud Web安全：配置ADFS在验证时包括特定组

目录

简介

本文描述如何配置Microsoft Active Directory联盟的服务(ADFS)作为标识供应商(IdP)，发送特定组详细信息对思科Cloud Web安全(CWS)服务，而不是组成员详尽列表。

先决条件

要求

Cisco 建议您了解以下主题：

- Cloud与ScanCenter门户的Web安全配置
- 安全断言标记语言(SAML)验证
- Microsoft ADFS服务器的管理

使用的组件

本文档中的信息根据Microsoft ADFS版本2.0，在Windows服务器2008 R2的该运行。

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

当在客户端浏览器之间的认证过程发生， ADFS服务器(IdP)和CWS (服务提供商(SP))所有信息加密并且被添加到在客户端浏览器的URL字串。这意味着URL字串更加长，当更多信息发送对CWS时。

当您配置SAML验证(与Microsoft ADFS)时为了用在CWS服务上，您应该配置一取决于的Party托拉斯提供用户名和分组信息。Cloud Web安全：配置与PingFederate和ADFS的用户/组属性，曾经SAML较详细地描述此步骤。

用户被添加对组的数量增加URL大小。如果用户属于很大数量的激活目录(AD)组， URL成长为大小

，藉以浏览器实施URL限制被到达，并且认证过程发生故障。

每个浏览器也许定义他们自己的最大数量允许的URL长度。RFC 2616不指定一个最大长度，但是浏览器供应商实施实际限制。

> **Note**:因为组没有字符，固定数量的明确地定义组最大是不可能的。例如， GroupA比Test_Group_A有较少字符。要定义在URL限制之下坚持的很多组取决于域名+组名的字符计数。

配置

您在认证过程能配置Microsoft ADFS服务器包括特定组。典型地您会选择用于CWS Web过滤规则的仅组。当您运行存在策略时的审计，帮助确定已经是在使用中的组。

已经存在的两个新建的和部署应该跟随提供这些好处的最佳实践配置：

- 保持URL大小到最低
- 加速在IdP (ADFS)和SP (CWS)之间的认证过程
- 保存在每认证请求的带宽

最佳实践配置

公开主张供应商信任和创建两个接受转换规则：

请使用声明规则模板发送LDAP属性作为要求

属性存储：AD;

LDAP属性：标记组-不够资格的名称;

流出的声明类型：组

请使用声明规则模板发送LDAP属性作为要求

属性存储：AD;

LDAP属性：SAM帐户NAME;

流出的声明类型：名称

通过打开取决于的部分信任和创建两个转换规则创建出版物转换规则：

请使用转换一个流入声明模板

流入声明类型：名称

格式：未指定

流出的声明类型：命名ID

格式：未指定

选择穿过所有声明值

请使用Passthrough或过滤一流入声明

流入声明类型：组

选择穿过从一个特定值开始仅的声明值：

指定您的AD组名

验证

使用本部分可确认配置能否正常运行。

- 当登陆作为最终用户时，请浏览对http://whoami.scansafe.net。
- 输出应该列出在以前被提及的步骤指定的仅组，而不是组成员详尽列表。

故障排除

目前没有针对此配置的故障排除信息。