为NAC客户服务器配置活动目录单一登录

目录

简介

在客户端的Web浏览器和Cisco NAC访客服务器之间的活动目录单一登录(AD SSO)功能用途Kerberos为了利用活动目录域控制器自动地验证访客。

注意： 为本文的目的， NTP和DNS服务器也在DC，但是这可能不是在您的环境的实际情形。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 必须配置DNS和在Cisco NAC访客服务器的工作。
- 必须配置DNS和在域控制器的工作。
- 必须定义Cisco NAC访客服务器的DNS条目： 一个记录*PTR*记录
- 必须定义域控制器的DNS条目： 一个记录*PTR*记录
- 必须与活动目录域同步Cisco NAC访客服务器时间设定。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 美洲台访客服务器2.0
- 有Internet Explorer的6.0 Microsoft Windows XP

- Windows服务器2003年

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。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

本文档使用以下网络设置：

配置

本文使用这些IP地址：

- 域控制器— 172.23.117.46 (w2k3-server.cca.cisco.com)
- 美洲台访客服务器— 172.23.117.42 (ngs.cca.cisco.com)
- 赞助商计算机— 172.23.117.45

完成这些步骤：

1. 访问NGS Admin接口。从浏览器，请去**http://172.23.117.42/admin**
2. **NGS网络配置**选择**Server>网络设置**。主机名- ngs域— cca.cisco.com主要的DNS — 172.23.117.46
3. **NTP设置**在**Server>日期/时间**，请配置Ntp server对DC IP **172.23.117.46**。
4. **AD SSO设置**在您配置SSO部分前，请确保A和PTR记录为域控制器和美洲台访客服务器存在。在AuthServer >验证SSO部分，配置此：如果配置是成功的，您应该看到成功消息。
5. **验证SSO功能**从用户计算机，请登录域。在本例中，此计算机是cca域的一部分。仅Internet Explorer为SSO功能支持。您需要确保，美洲台访客服务器是本地内联网的一部分，并且自动登录打开。**注意：** 请使用FQDN访客服务器为了测试从浏览器的SSO。例如，IP地址不工作。验证网络浏览器设置：从Web浏览器，请去**http://ngs.cca.cisco.com**。您应该自动地登陆到与域凭证的ngs。**注意：** 如果配置在admin模式的美洲台与用户凭证，链路**http://ngs.cca.cisco.com**只将运作。在美洲台访客服务器审计日志下，您能看到用户Niall登录默认组：
6. **与AD SSO的用户组映射(可选)***除默认组之外，在此部分您将学习映射SSO用户对一特定组。*要映射有ADSSO的用户组，您需要配置激活目录服务器作为认证服务器然后映射有赞助商用户组的AD组。选择**NGS (http://172.23.117.42/admin)认证>赞助>激活目录服务器**。添加一个新域控制器。测试连接连接选项在故障排除方便的NGS 2.0介绍。它分辨您您是否正确地配置DC。**配置用户组**添加一个新用户组名**— tme**。在本例中，您选择**没有**为了变大块帐户创建。这样您立即知道用户是否被放置了给tme组*或*默认组。在活动目录映射，测试用户niall已经作为域管理员的部分。

验证

使用本部分可确认配置能否正常运行。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

验证ADSSO用户组映射

为了访问赞助商计算机，请打开一个新的浏览器并且去http://ngs.cca.cisco.com。

Niall应该在tme组中安置没有访问变大块帐户创建。

如果查看审计日志，您能验证赞助商被放置到正确角色。

故障排除

本部分提供的信息可用于对配置进行故障排除。

这些是在日志的错误消息。Kerberos错误导致这些错误之一：

- /FQDNIP域在一个正确格式未被输入(应该是表CCA.CISCO.COM)。
- FQDNIP美洲台访客服务器的主机名不可以是即它必须是完全限定域名nac.cca.cisco.com的IP地址。
- IP有DNS配置问题。
- DNS有DNS配置问题。
- DNS A有DNS配置问题。
- DNSIPPTR有DNS配置问题。
- DNSIPPTR有DNS配置问题。
- .。查看应用程序日志发现错误的全面的详细信息。
- /管理员用户名/密码不正确。
- DC有在AD服务器的一DNS问题。
- 保证服务器时间匹配，它推荐您使用NTP同步服务器时间。
- DCDNS confiugration有在您的AD服务器的DNS配置问题。

相关信息

- 技术支持和文档 - Cisco Systems