NAC设备(CCA) ：活动目录Windows选择签订合同(SSO)配置和故障排除

目录

简介

本文描述如何使用Microsoft Windows激活目录(AD)单个符号(SSO)为了配置和排除故障思科网络准入控制(美洲台)设备，以前叫作思科Clean Access (CCA)。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 确保DC运行Windows 2000 SP4或Windows 2003年(英文虎报或企业) SP1或Windows 2003个R2。2003年不支持没有SP1的Windows。
- 确保Windows SSO仅AD环境支持。不支持Windows NT环境。Clean Access代理程序要求。
- 设置Clean Access服务器(CAS)帐户正如Cisco NAC设备所描述- Clean Access服务器安装和配置指南，版本4.1(2)。

使用的组件

本文档中的信息根据NAC设备软件版本4.x或以上。

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Windows SSO

在此部分的信息描述如何配置在本文提交的功能。

设置AD SSO供应商

- 您不可执行验证测验到AD SSO供应商或VPN SSO。
- LDAP查找服务器必要，只有当用户要执行AD SSO的映射规则，因此在AD SSO以后，用户在根据AD属性的角色将安置。这不是需要的获得基本SSO工作(没有角色映射)。

运行在DC的KTPass

KTPass是工具联机作为Windows的部分2000/2003支持工具。参考的Cisco NAC设备- Clean Access服务器安装和配置指南，发布4.1(2)欲知更多信息。

当您运行KTPass时，请注意总是下跌在"/"之间的计算机名称和"@"匹配DC的名称，因为将看起来在控制面板>System >计算机名称下>在DC的全双工计算机名称。

并且，请确保在那以后出现@的领域名突出显示了总是在大写字母。

```
C:\Program Files\Support Tools>ktpass -princ
 ccasso/prem-vm-2003.win2k3.local@WIN2K3.LOCAL -mapuser ccasso -pass Cisco123 -out
c:\test.keytab -ptype KRB5_NT_PRINCIPAL +DesOnly Using legacy password setting method //confirms
ccasso acct is mapped Successfully mapped ccasso/prem-vm-2003.win2k3.local to ccasso. Key
created. Output keytab to c:\test.keytab Keytab version: 0x502 keysize 80 ccasso/prem-vm-
2003.win2k3.local@WIN2K3.LOCAL ptype 1 (KRB5_NT_PRINCIPAL) vno 3 etype 0x17 (RC4-HMAC) keylength
16 (0xf2e787d376cbf6d6dd3600132e9c215d) Account ccasso has been set for DES-only encryption.
```

如此示例所显示，为了支持Windows 7，您必须运行KTPASS ：

```
C:\Program Files\Support Tools>KTPASS.EXE -princ
newadsso/[adserver.]domain.com@DOMAIN.COM -mapuser newadsso -pass PasswordText -out
c:\newadsso.keytab -ptype KRB5_NT_PRINCIPAL
```

并且，请确保在那以后出现@的领域名突出显示了总是在大写字母。

配置在CAS的SSO

选择**CCA服务器>管理>验证> Windows验证>活动目录SSO**为了打开AD窗口，并且验证这些项目：

- 活动目录域：Kerberos领域name=需要大写。
- 激活目录服务器(FQDN) ：确保CAS能通过DNS解析此名称。此字段不可以是IP地址。使用在本例中的值，您能登录到CAS通过安全壳SSH，并且执行“nslookup prem-vm-2003.win2k3.local”。然后，请确保它成功地解决。
- 确保FQDN完全照原样匹配AD服务器(DC)的名称在控制面板>System >计算机名称下|在AD服务器设备(DC)的全双工计算机名称。

验证SSO服务开始

完成这些步骤：

1. 去**CCA服务器>管理>状态**为了验证SSO服务开始。
2. 运行此命令为了验证CAS在TCP 8910当前侦听(用于Windows SSO)。`[root@cs-ccas02 ~]#netstat -a | grep 8910 tcp 0 0 *:8910 *:* LISTEN`

DC的开放端口

为了打开适当的端口到DC，请完成这些步骤：

注意： 对于测试，总是请打开对DC的完整访问。然后，一旦SSO工作，您能附加它向下到特定端口。

1. 确保以下端口允许在对活动目录的不信任角色：**TCP** ：88， 135， 445， 389/636， 1025， 1026**UDP** ：88， 389**注意：** *TCP端口445*一定是开放的为了Windows密码重设能正确地运作。
2. 保证客户端运行CCA代理程序4.0.0.1或以上。
3. 登陆到有Windows域凭证的PC。**注意：** 确保您登录域而不是本地帐户。

客户端看到代理程序执行的SSO

完成的SSO

在线用户用户列表看到的SSO用户

排除故障Windows SSO

Error:不能开始SSO服务。请检查配置。

问题

您收到此错误：

解决方案

要解决此问题，请完成以下步骤：

1. 检查正确地确保KTPass运行。检查字段按照幻灯片X.所述是重要的。如果KTPass不正确地运行了，请删除帐户并且创建在AD的一新帐户并且再运行KTPass。
2. 确保在CAS的时间与DC同步。此步骤可以通过指向他们执行两个同一时间服务器。在实验室设置，请指向CAS时间的DC (DC运行Windows时间)。Kerberos是敏感的计时，并且反称性比5分钟(300秒)不可以极大。**注意：** 当您设法开始CAS的AD SSO服务时，问题也许发生在时间syncronization， NTP。如果NTP配置，并且时钟不是已同步的，服务不会工作。一旦修复服务应该工作。
3. 确保活动目录域以大写(领域)，并且CAS能解决在DNS的FQDN。对于实验室设置，运行DNS的您能指向DC (AD要求在租期一DNS服务器)。
4. 登录CAS直接地作为https:// <CAS-IP-address>/admin。然后，请点击**支持日志**并且改变记录对**资讯台的**活动目录通信的日志级别。
5. 再现问题并且下载支持日志。

客户端验证不工作

问题

AD SSO服务开始，但是客户端验证不工作。

解决方案

UDP端口不是开放的在未经鉴定的角色。在您添加这些端口到数据流策略后，验证应该工作。

无法运行在windows 7 PC的SSO

问题

SSO不为运行Windows 7操作系统的机器工作。

解决方案 1

为了解决此问题，运行Windows 7操作系统在计算机的enable (event) DES加密，然后重新运行KTPass。完成这些步骤为了启用在Windows 7 PC:的DES

1. 登陆到Windows 7客户端机器作为管理员。
2. 去**启动>控制面板>System和安全>Administrative Tools>本地安全策略>本地策略/安全>选项。**
3. 选择**网络安全>配置允许的加密类型。**
4. 在本地安全设置选项卡，请检查复选框启用所有选项，除了将来加密类型选项。

解决方案 2

(如果需要支持Windows 7)，为了解决此问题，请运行此on命令Windows 2003服务器：

```
C:\Program Files\Support Tools> ktpass.exe -princ
casuser/cca-eng-domain.cisco.com@CCA-ENG-DOMAIN.CISCO.COM-mapusercasuser -pass
Cisco123 -out c:\casuser.keytab -ptype KRB5_NT_PRINCIPAL
```

欲知更多信息，参考配置在Windows 7环境的AD SSO。

无法配置用户的Linux客户端支持美洲台环境的

问题

无法配置一个用户的Linux客户端支持美洲台环境的。

解决方案

Linux不支持Web代理程序或代理程序。美洲台与仅Web洛金的支持Linux没有任何状态评估。一旦计算机通过Web洛金验证，用户应该分配到您配置的一个最终用户角色。用户根据用户角色的数据流策略然后将访问。参考Cisco Bug CSCti54517 (仅限注册用户)欲知更多信息。

SSO服务开始，但是客户端不执行SSO

这通常归结于某个通信问题在DC/client PC之间或在客户端PC和CAS之间。

这是验证的一些工作：

- 客户端有Kerberos密钥。
- 端口是开放的对DC，因此客户端能连接，接收代理程序日志，并且接收注册CAS。
- 时间或时钟在客户端PC与DC同步。
- 确认CAS在端口8910侦听。在客户端PC的嗅探器跟踪也将帮助。
- CCA代理程序是4.0.0.1或以后。
- 使用本地帐户，用户实际上登陆使用域帐户和不。

Kerbtray

Kerbtray可以用于确认客户端获取Kerberos票(TGT和ST)。注意事项是为服务票(ST)，是为该CAS的帐户您创建在DC。

Kerbtray是从Microsoft支持工具的一自由工具可得到。它可能也用于清除在客户端机器的Kerberos票。

在系统托盘的一个绿色Kerbtray图标表明客户端有活动Kerberos票。然而，您需要验证票为CAS帐户是正确(有效)。

CAS日志–不能开始SSO服务

日志文件在CAS的利益是/perfigo/logs/perfigo-redirect-log0.log.0。

AD SSO服务在CAS不开始是CAS-DC通信问题：

1. `SEVERE: startServer - SSO Service authentication failed. Clock skew too great (37)` `Aug 3, 2006 7:52:48 PM com.perfigo.wlan.jmx.admin.GSSServer loginToKDC` 这意味着时钟没有同步在CAS和域控制器之间。
2. `Aug 21, 2006 3:39:11 PM com.perfigo.wlan.jmx.admin.GSSServer loginToKDC INFO: GSSServer - SPN : [ccass/PreM-vM-2003.win2k3public.local@WIN2K3PUBLIC.LOCAL] Aug 21, 2006 3:39:11 PM com.perfigo.wlan.jmx.admin.GSSServer loginToKDC SEVERE: startServer - SSO Service authentication failed. Client not found in Kerberos database (6) Aug 21, 2006 3:39:11 PM com.perfigo.wlan.jmx.admin.GSSServer startServer WARNING: GSSServer loginSubject could not be created.` 这意味着用户名不正确。注释错误用户名“ccass”，错误代码6和最后警告。
3. `Aug 21, 2006 3:40:26 PM com.perfigo.wlan.jmx.admin.GSSServer loginToKDC`

INFO: GSSServer - SPN : [ccasso/PreM-vM-2003.win2k3public.local@WIN2K3PUBLIC.LOCAL]
Aug 21, 2006 3:40:26 PM com.perfigo.wlan.jmx.admin.GSSServer loginToKDC
SEVERE: startServer - SSO Service authentication failed. Pre-authentication information was invalid (24) Aug 21, 2006 3:40:26 PM com.perfigo.wlan.jmx.admin.GSSServer startServer
WARNING: GSSServer loginSubject could not be created. 密码不正确或领域无效(不以大写？)。坏FQDN ？KTPass不正确地运行？注释错误24和最后警告。**注意：** 确保KTPass版本是5.2.3790.0。除非有KTPass一个坏版本，即使脚本适当地运行， SSO服务不会开始。

客户端– CAS通信问题：

Aug 3, 2006 10:03:05 AM com.perfigo.wlan.jmx.admin.GSSHandler run
SEVERE: GSS Error: Failure unspecified at GSS-API level (Mechanism level: Clock skew too great (37))
当客户端PC时间没有与DC时，同步此错误被看到。

注意： 在此错误和那个之间的区别CAS时间没有与DC的地方同步。

已知问题

- Cisco Bug ID CSCse64395 (仅限注册用户) — 4.0代理程序不解决Windows SSO的DNS。此问题在CCA代理程序4.0.0.1被解决。
- Cisco Bug ID CSCse46141 (仅限注册用户) —在启动期间，万一CAS不能到达AD服务器SSO发生故障。应急方案是去**CCA服务器>管理[CAS_IP]验证> Windows验证>活动目录SSO**，并且点击**更新**为了重新启动AD SSO服务。
- 进行在CAS的服务perfigo重新启动。有高速缓冲存储问题，当旧有凭证在CAS时被缓存，并且不使用新的，直到Tomcat重新启动。
- 您不能限制SSO的单个用户登录。这是SSO的正常行为，因为它是Kerberos协议，并且没有选项限制单个用户登录Kerberos协议。
- *Windows 7*和*Windows 2008*不支持SSO，当SSO使用Windows 7或Windows不支持2008年的**DES加密**。

相关信息

- Cisco NAC Appliance (Clean Access)支持页面
- 技术支持和文档 - Cisco Systems