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

本文档介绍如何使用Microsoft Windows Active Directory(AD)单点登录(SSO)来配置和排除思科网络准入控制(NAC)设备(以前称为思科Clean Access(CCA))的故障。

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（标准或企业版）SP1或Windows 2003 R2。不支持不带SP1的Windows 2003。
- 确保仅在AD环境中支持Windows SSO。不支持Windows NT环境。需要Clean Access Agent。
- 按照《思科NAC设备 — Clean Access Server安装和配置指南，版本4.1(2)》中所述设置Clean Access Server(CAS)帐户。

使用的组件

本文档中的信息基于NAC设备软件版本4.x或更高版本。

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。

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

本节中的信息介绍如何配置本文档中介绍的功能。

设置AD SSO提供程序

- 无法对AD SSO提供程序或VPN SSO执行身份验证测试。
- 仅当用户要为AD SSO执行映射规则时，才需要LDAP查找服务器，以便在AD SSO之后，用户将基于AD属性被置于角色中。这不是使基本SSO正常运行（无角色映射）所必需的。

在直流电源上运行KTPass

KTPass是Windows 2000/2003支持工具的一部分。有关详细信息，请参阅Cisco NAC设备 — Clean Access服务器安装和配置指南4.1(2)版。

运行KTPass时，必须注意，始终介于“/”和“@”之间的计算机名称与DC名称匹配，因为DC上的“控制面板”>“系统”>“计算机名称”>“完整计算机名称”下会显示该名称。

此外，请确保在@突出显示后显示的领域名称始终为大写字母。

```
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.
```

要支持Windows 7，必须运行KTPASS，如本示例所示：

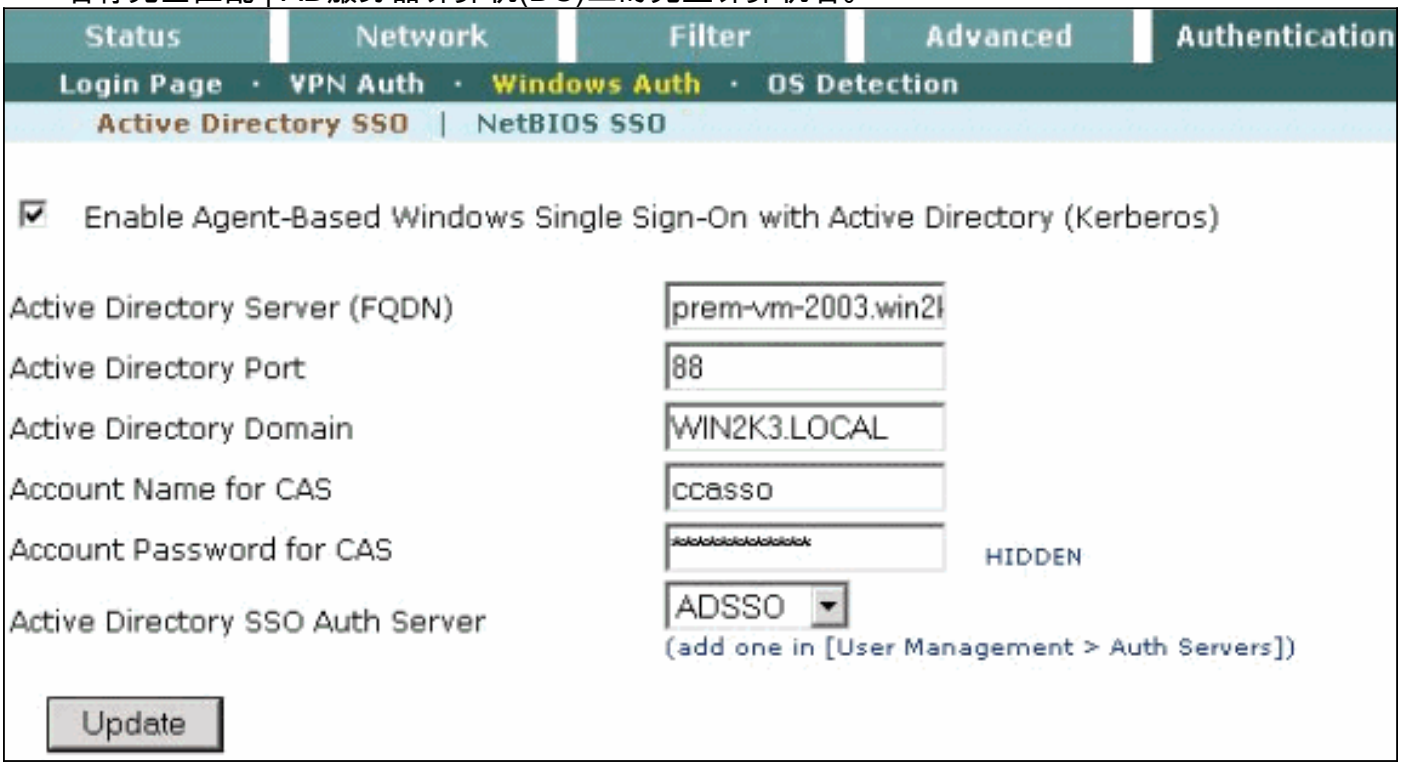
```
C:\Program Files\Support Tools>KTPASS.EXE -princ
newadsso/[adserver.]domain.com@DOMAIN.COM -mapuser newadsso
-pass PasswordText -out c:\newadsso.keytab -ptype KRB5_NT_PRINCIPAL
```

此外，请确保在@突出显示后显示的领域名称始终为大写字母。

在CAS上配置SSO

选择**CCA Servers > Manage > Authentication > Windows Auth > Active Directory SSO**以打开AD窗口，并验证以下项：

- Active Directory域：Kerberos领域名称=需要大写。
- Active Directory服务器(FQDN):确保CAS可以通过DNS解析此名称。此字段不能是IP地址。使用本示例中的值，您可以通过安全外壳(SSH)登录到CAS，并执行“nslookup prem-vm-2003.win2k3.local”。然后，确保成功解析。
- 确保FQDN与AD服务器(DC)的名称完全匹配，与其在“控制面板”>“系统”>“计算机名称”下显示的名称完全匹配 | AD服务器计算机(DC)上的完整计算机名。



验证SSO服务是否已启动

请完成以下步骤：

1. 转到**CCA Servers > Manage > Status**以验证SSO服务是否已启动。

2. 运行此命令以验证CAS现在是否在TCP 8910上侦听（用于Windows SSO）。

```
[root@cs-ccas02 ~]#netstat -a | grep 8910
   tcp        0      0 *:8910                      *:*
   LISTEN
```

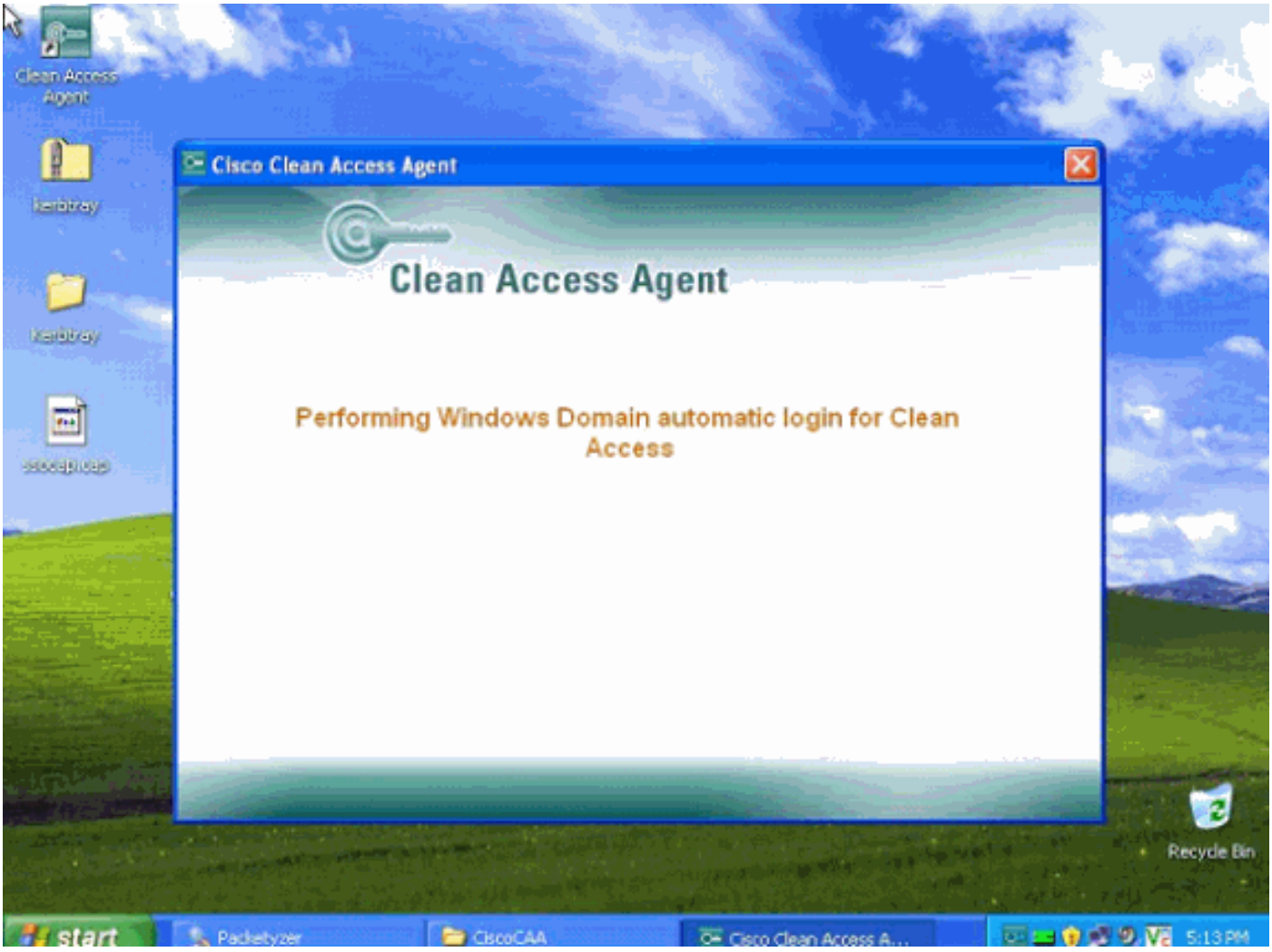
打开DC端口

要向DC打开适当的端口，请完成以下步骤：

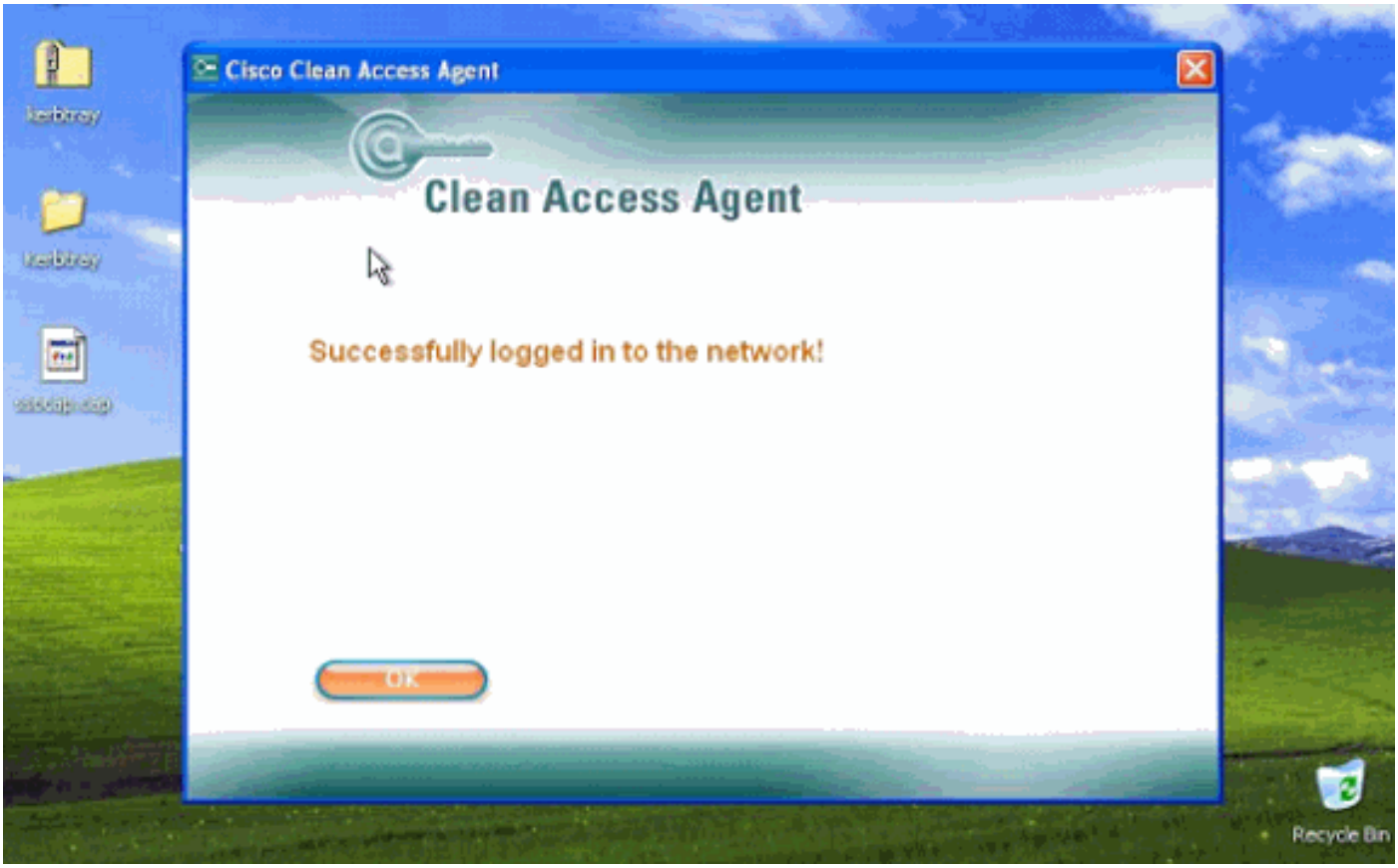
注意：要进行测试，请始终打开对DC的完全访问。然后，一旦SSO工作，您就可以将其绑定到特定端口。

1. 确保在Active Directory的不受信任的角色中允许以下端口：TCP:88、135、445、389/636、1025、1026**UDP**:88 、389**注意**： *TCP端口445必*须打开，Windows密码重置才能正常工作。
2. 确保客户端运行CCA代理4.0.0.1或更高版本。
3. 使用Windows域凭证登录PC。**注意**：确保您登录到域而不是本地帐户。

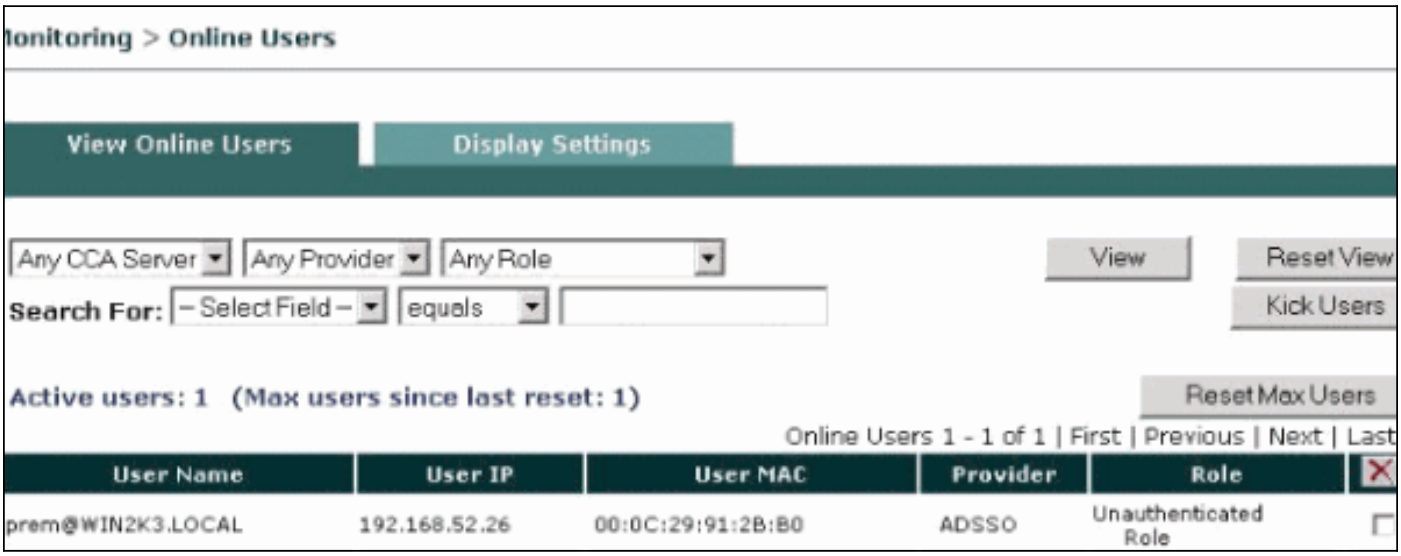
客户端看到代理执行SSO


Clean Access Agent
Cisco Clean Access Agent
Clean Access Agent
Performing Windows Domain automatic login for Clean Access
Recycle Bin
start
Packetyzer
CiscoCAA
Cisco Clean Access A...
5:13 PM

SSO已完成


Cisco Clean Access Agent
Clean Access Agent
Successfully logged in to the network!
OK
Recycle Bin

在线用户列表上看到的SSO用户



排除Windows SSO故障

Error:无法启动SSO服务。请检查配置。

问题

您收到以下错误：

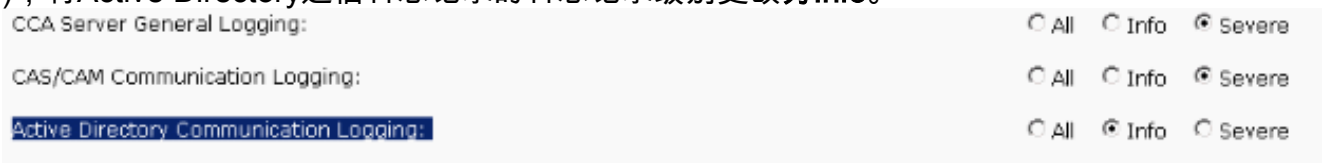
解决方案

要解决此问题，请完成以下步骤：

1. 检查以确保KTPass正确运行。检查幻灯片X中提到的字段非常重要。如果KTPass运行不正确，请删除该帐户，在AD上创建新帐户，然后再次运行KTPass。
2. 确保CAS上的时间与DC同步。通过将这两个服务器都指向同一时间服务器，可以执行此步骤。在实验设置中，将CAS指向DC本身一段时间（DC运行Windows时间）。 Kerberos对时钟敏感，偏差不能超过5分钟（300秒）。**注意：**当您尝试启动CAS的AD SSO服务时，时间同步NTP可能会出现问题。如果配置了NTP，且时钟未同步，则服务将无法工作。修复后，服务应能正常工作。
3. 确保Active Directory域为大写（领域），并且CAS可以解析DNS中的FQDN。对于实验设置

，您可以指向运行DNS的DC（AD至少需要一台DNS服务器）。

4. 直接以https://<*CAS-IP-address*>/admin身份登录CAS。然后，单击**Support Logs(支持日志)**，将Active Directory通信日志记录的日志记录级别更改**为Info**。



5. 重新创建问题并下载支持日志。

客户端身份验证不工作

问题

AD SSO服务已启动，但客户端身份验证不起作用。

解决方案

UDP端口未在未通过身份验证的角色中打开。在将这些端口添加到流量策略后，身份验证应会起作用。

无法在Windows 7 PC上运行SSO

问题

SSO对运行Windows 7操作系统的计算机不起作用。

解决方案 1

要解决此问题，请在运行Windows 7操作系统的计算机上启用DES加密，然后重新运行KTPass。要在Windows 7 PC上启用DES，请完成以下步骤：

1. 以管理员身份登录到Windows 7客户端计算机。
2. 转至开**始>控制面板>系统和安全>管理工具>本地安全策略>本地策略/安全>选项**。
3. 选择**Network security > Configure encryption types allowed**。
4. 在Local Security Settings选项卡上，选中复选框以启用除Future encryption types选项外的所有选项。

解决方案 2

要解决此问题，请在Windows 2003 Server上运行此命令（如果还需要支持Windows 7）：

```
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
```

有关详细信息，请参阅在Windows 7环境中配置AD SSO。

无法在NAC环境中为用户配置linux客户端支持

问题

无法在NAC环境中为用户配置Linux客户端支持。

解决方案

Linux不支持Web代理或代理。NAC仅支持Linux和Web登录，无需任何状态评估。通过Web登录对计算机进行身份验证后，应将用户分配给您配置的最终用户角色。然后，用户将根据用户角色的流量策略拥有访问权限。有关详细信息，请参阅Cisco Bug CSCti54517(仅限注册客户)。

SSO服务已启动，但客户端不执行SSO

这通常是由于DC/客户端PC之间或客户端PC与CAS之间的某些通信问题。

以下是需要验证的几点：

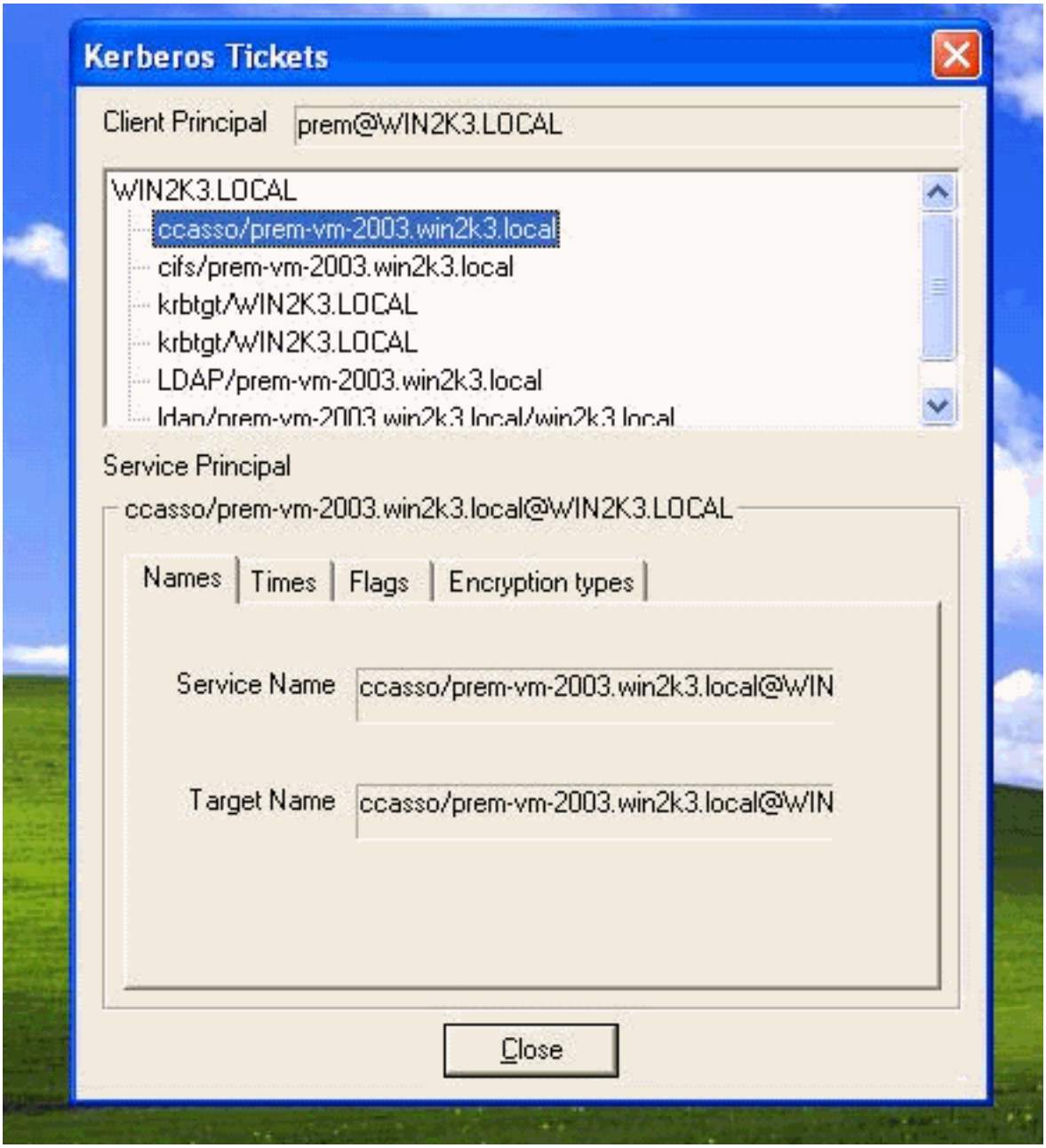
- 客户端有Kerberos密钥。
- 端口对DC开放，因此客户端可以连接、接收代理日志和接收CAS上的日志。
- 客户端PC上的时间或时钟与DC同步。
- 确认CAS正在侦听端口8910。客户端PC上的嗅探器跟踪也会有所帮助。
- CCA代理是4.0.0.1或更高版本。
- 用户实际上使用域帐户登录，而不使用本地帐户。

克尔布特雷

Kerbtray可用于确认客户端已获得Kerberos票证（TGT和ST）。 问题出在服务票证(ST)上，该票证适用于您在数据中心上创建的CAS帐户。

Kerbtray是Microsoft支持工具中提供的免费工具。它还可用于清除客户端计算机上的Kerberos票证。

系统托盘上的绿色Kerbtray图标表示客户端具有活动的Kerberos票证。但是，您需要验证CAS帐户的票证是否正确（有效）。



CAS日志 — 无法启动SSO服务

CAS上关注的日志文件是/perfigo/logs/perfigo-redirect-log0.log.0。

AD SSO服务在CAS上不启动是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
```

这表示时钟在CAS和域控制器之间不同步。

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。注意用户名“ccass”错误、错误代码6和最后一个警告。

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（大写中不是？）。 FQDN错误？KTPass运行不正确？注意错误24和最后一个警告。**注意**：确保KTPass版本为5.2.3790.0。除非存在KTPass的错误版本，否则即使脚本运行正常，SSO服务也不会启动。

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时间未与DC同步时，会出现此错误。

注意：此错误与CAS时间未与DC同步的错误之间的区别。

已知问题

- Cisco Bug ID CSCse64395(仅注册客户)— 4.0代理不解析Windows SSO的DNS。此问题在CCA代理4.0.0.1中解决。
- Cisco Bug ID CSCse46141 (仅注册客户) — 在CAS在启动期间无法到达AD服务器时，SSO失败。解决方法是转到**CCA Servers > Manage [CAS_IP] Authentication > Windows Auth > Active Directory SSO**，然后单击**Update**以重新启动AD SSO服务。
- 在CAS上执行服务永久重启。当旧凭证在CAS上缓存并且在重新启动Tomcat之前不使用新凭证时，存在缓存问题。
- 您不能限制单个用户登录SSO。这是SSO的正常行为，因为它是kerberos协议，并且没有限制在kerberos协议中单用户登录的选项。
- *Windows 7*和*Windows 2008*不支持SSO，因为SSO使用Windows 7或Windows 2008不支持的DES加密。

相关信息

- 思科NAC设备(Clean Access)支持页
- 技术支持和文档 - Cisco Systems