Dispositivo NAC (CCA): Configuración y resolución de problemas de Windows Single Sign On (SSO) de Active Directory

Contenido

Introducción

Este documento describe cómo utilizar Microsoft Windows Active Directory (AD) Single Sign On (SSO) para configurar y resolver problemas del dispositivo Cisco Network Admission Control (NAC), anteriormente conocido como Cisco Clean Access (CCA).

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Asegúrese de que el DC ejecuta Windows 2000 SP4 o Windows 2003 (Standard o Enterprise) SP1 o Windows 2003 R2. Windows 2003 sin SP1 no es compatible.
- Asegúrese de que Windows SSO sólo se admite en un entorno AD. No se admite el entorno de Windows NT. Se necesita Clean Access Agent.
- Configure la cuenta de Clean Access Server (CAS) como se describe en la Guía de Instalación y Configuración de Cisco NAC Appliance - Clean Access Server, Versión 4.1(2).

Componentes Utilizados

La información en este documento se basa en la versión 4.x o posterior del software del dispositivo NAC.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos Técnicos Cisco para obtener más información sobre las convenciones del documento.

Configurar Windows SSO

La información de esta sección describe cómo configurar las funciones presentadas en este documento.

Configuración del proveedor de AD SSO

- No puede realizar una prueba de autenticación a un proveedor de AD SSO o a un SSO de VPN.
- El servidor de búsqueda LDAP sólo es necesario si los usuarios quieren hacer reglas de asignación para el AD SSO, de modo que después de AD SSO, los usuarios serán colocados en roles basados en atributos AD. Esto no es necesario para que funcione el SSO básico (sin asignación de funciones).

Ejecute KTPass en el DC

KTPass es una herramienta disponible como parte de las herramientas de soporte de Windows 2000/2003. Consulte Guía de Instalación y Configuración de Cisco NAC Appliance - Clean Access

Server, Versión 4.1(2) para obtener más información.

Cuando ejecute KTPass, es importante tener en cuenta que el nombre del equipo que siempre se encuentra entre "/" y "@" coincide con el nombre del DC, como aparecería en Panel de control > Sistema > Nombre del equipo > Nombre completo del equipo en el DC.

Además, asegúrese de que el nombre de rango que aparece después de @ resaltado siempre esté en mayúsculas.

```
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.
```

Para soportar Windows 7, debe ejecutar KTPASS como se muestra en este ejemplo:

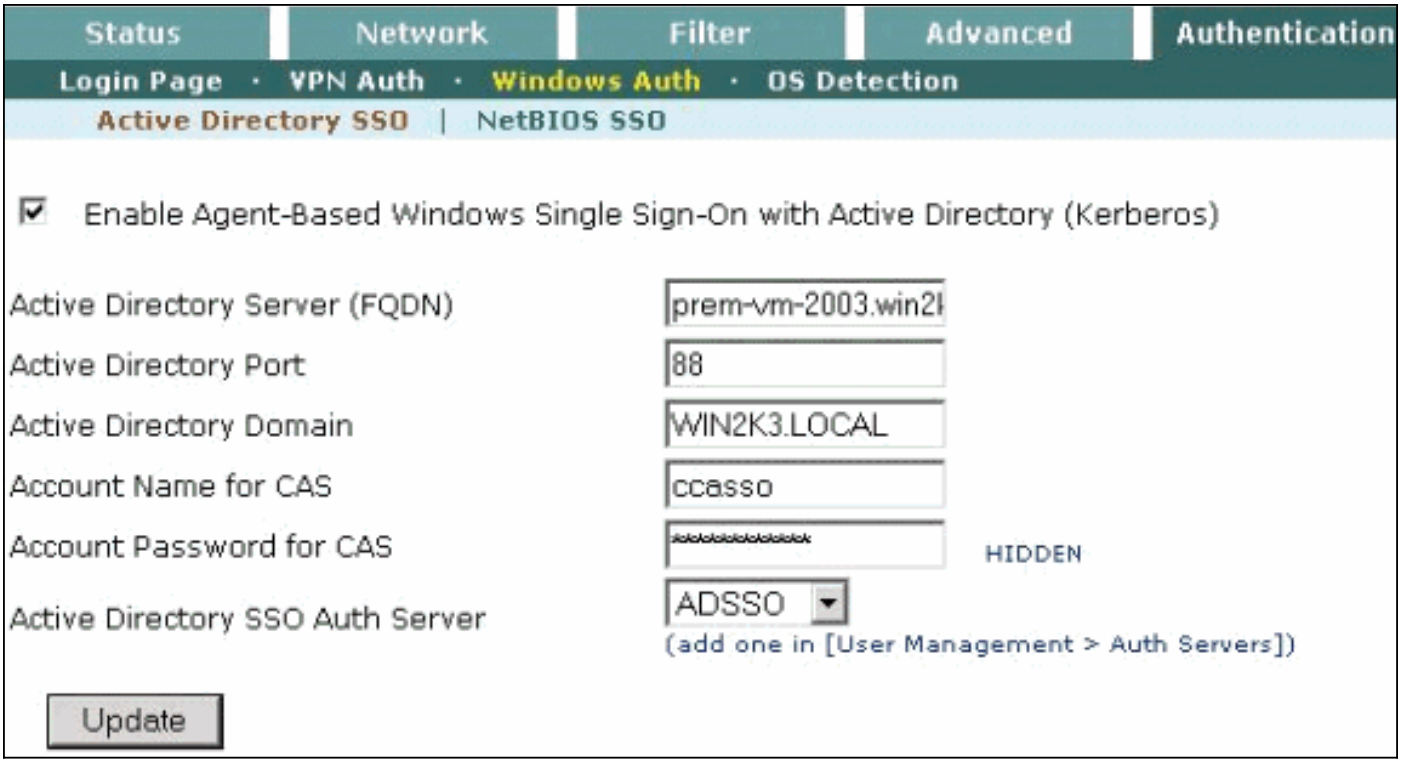
```
C:\Program Files\Support Tools>KTPASS.EXE -princ
newadsso/[adserver.]domain.com@DOMAIN.COM -mapuser newadsso
-pass PasswordText -out c:\newadsso.keytab -ptype KRB5_NT_PRINCIPAL
```

Además, asegúrese de que el nombre de rango que aparece después de @ resaltado siempre esté en mayúsculas.

Configuración de SSO en el CAS

Elija **CCA Servers > Manage > Authentication > Windows Auth > Active Directory SSO** para abrir la ventana AD, y verifique estos elementos:

- Dominio de Active Directory: Nombre de rango Kerberos = Necesita ser en mayúsculas.
- Servidor de directorio activo (FQDN): Asegúrese de que el CAS pueda resolver este nombre a través de DNS. Este campo no puede ser una dirección IP. Con los valores de este ejemplo, puede iniciar sesión en CAS a través de Secure Shell (SSH) y realizar "nslookup prem-vm-2003.win2k3.local". A continuación, asegúrese de que se resuelva correctamente.
- Asegúrese de que FQDN coincide con el nombre del servidor AD (DC) exactamente como aparece en Panel de control > Sistema > Nombre de equipo | Nombre completo del ordenador en el equipo servidor AD (DC).



Verifique que el Servicio SSO se Inició

Complete estos pasos:

1. Vaya a **CCA Servers > Manage > Status** para verificar que se haya iniciado el servicio SSO.

2. Ejecute este comando para verificar que el CAS ahora escucha en TCP 8910 (utilizado para Windows SSO).

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

Puertos abiertos al DC

Para abrir los puertos apropiados al DC, complete estos pasos:

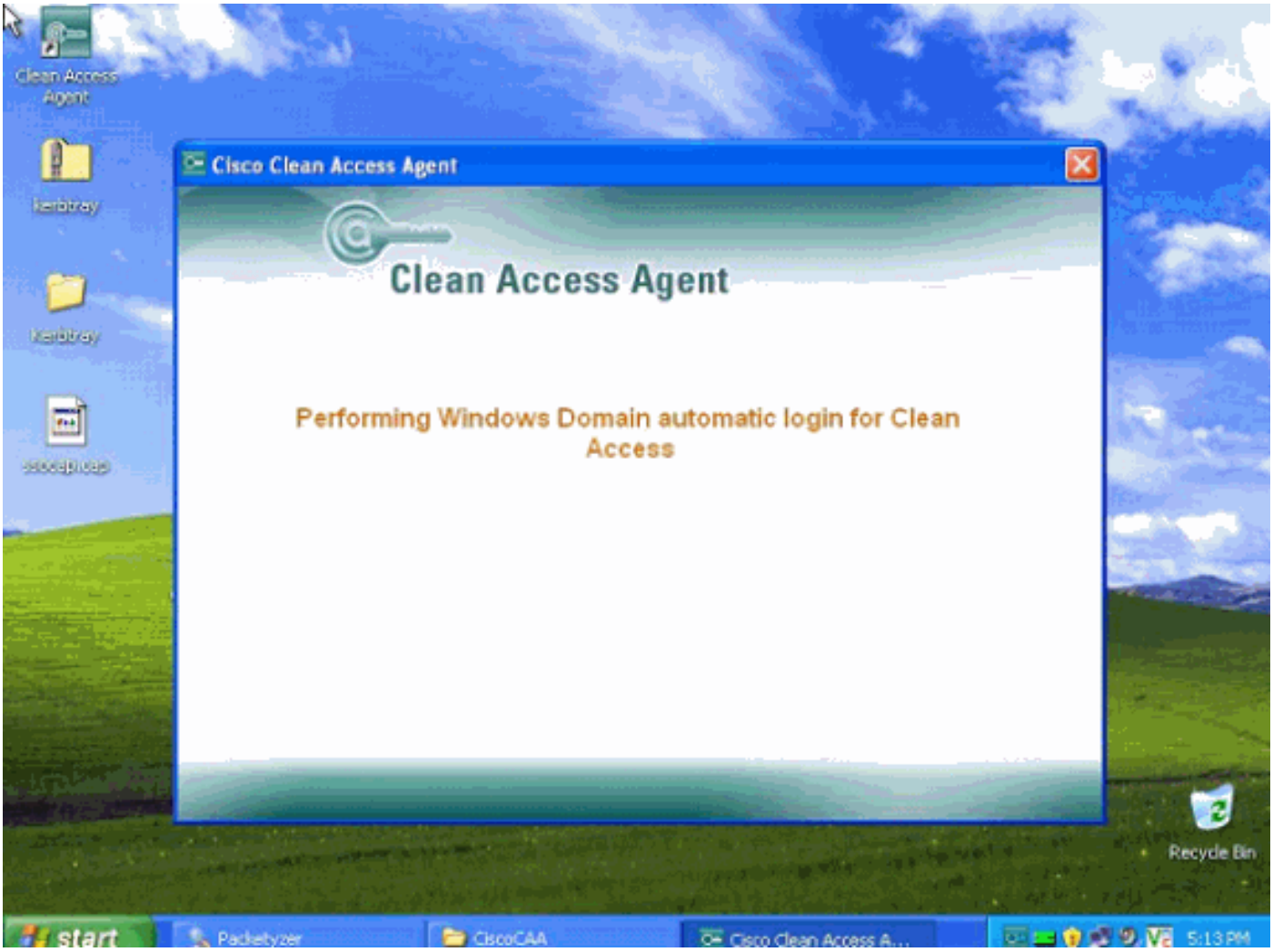
Nota: Para las pruebas, siempre abra el acceso completo al DC. Luego, una vez que el SSO funciona, puede atarlo a puertos específicos.

1. Asegúrese de que los siguientes puertos estén permitidos en la función no confiable a Active

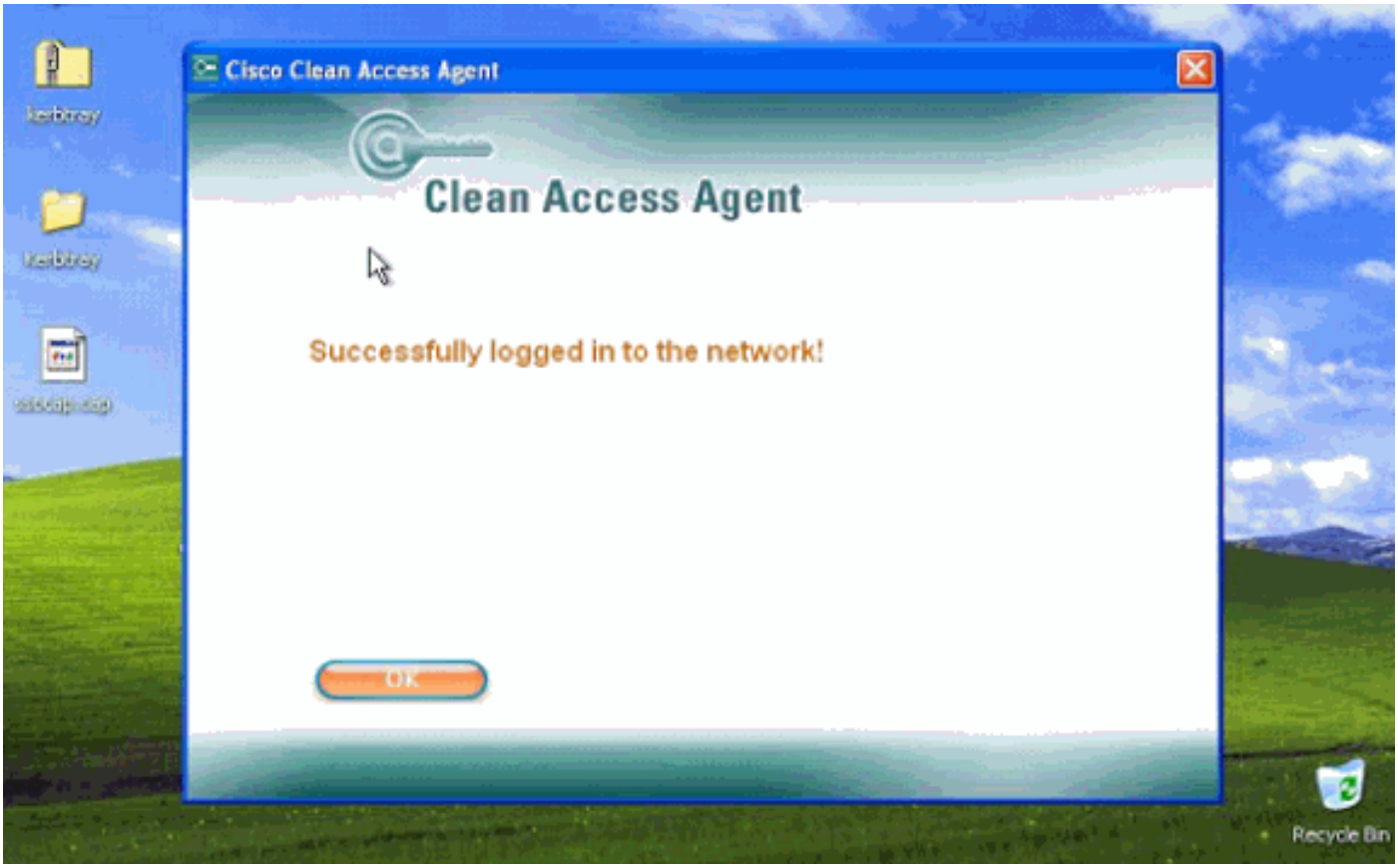
Directory:TCP: 88, 135, 445, 389/636, 1025, 1026UDP: 88, 389**Nota:** *El PUERTO TCP 445* debe estar abierto para que el restablecimiento de contraseña de Windows funcione correctamente.

2. Asegúrese de que el cliente ejecute CCA Agent 4.0.0.1 o posterior.
3. Inicie sesión en el equipo con las credenciales de Windows Domain.**Nota:** Asegúrese de que está iniciando sesión en el dominio y no en la cuenta local.

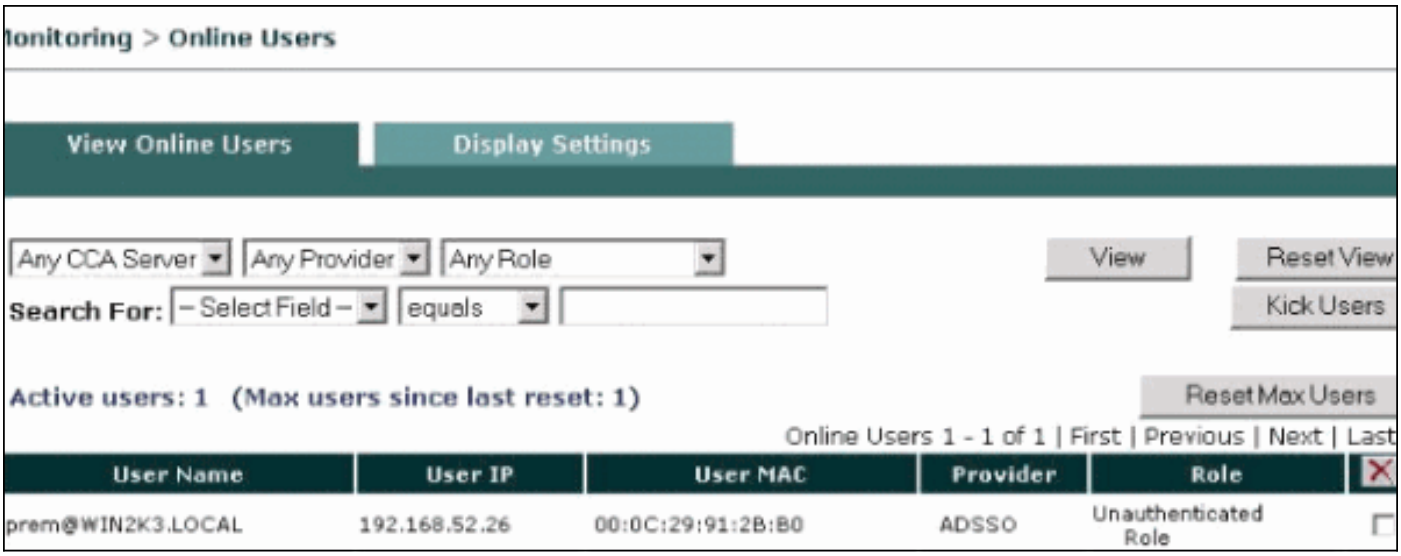
El cliente ve al agente realizando SSO



SSO completado



Usuario SSO visto en la lista de usuarios online

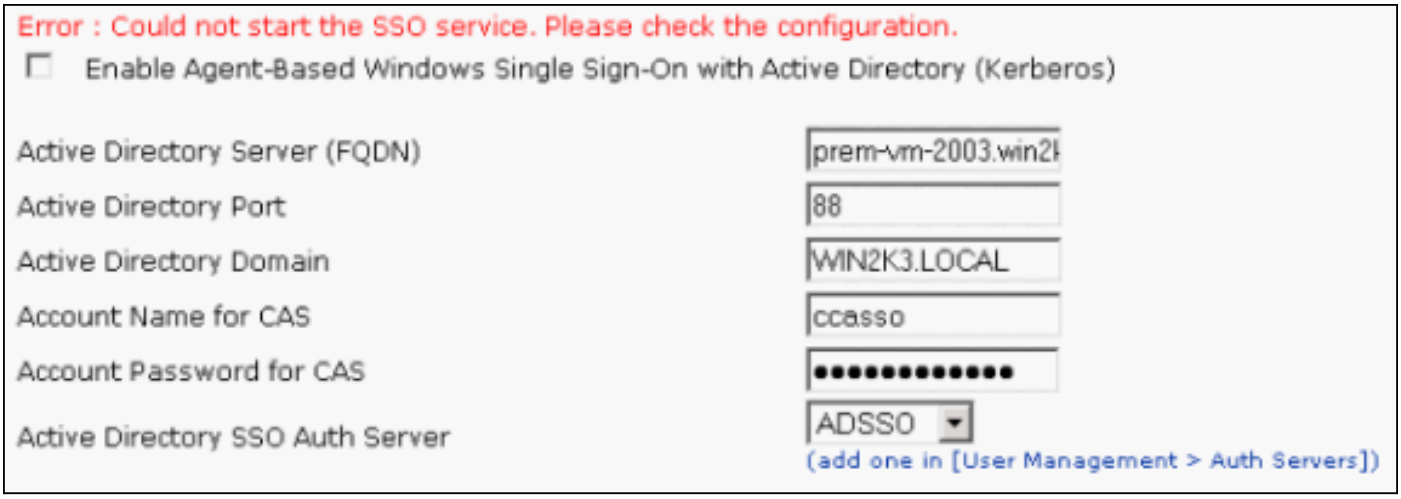


Solución de problemas de Windows SSO

Error: No se pudo iniciar el servicio SSO. Compruebe la configuración.

Problema

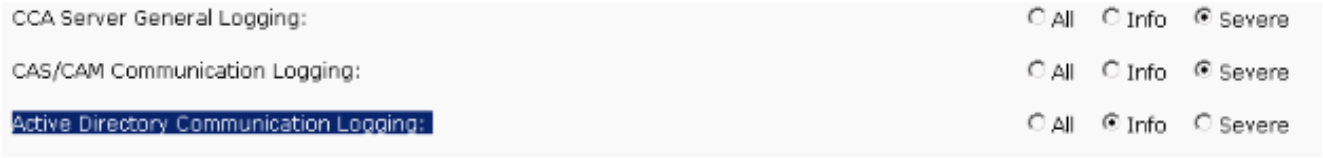
Recibe este error:



Solución

Complete estos pasos para resolver el problema:

1. Verifique para asegurarse de que KTPass se ejecute correctamente. Es importante verificar los campos como se menciona en la diapositiva X. Si KTPass se ejecutó incorrectamente, elimine la cuenta y cree una nueva cuenta en AD y ejecute KTPass de nuevo.
2. Asegúrese de que el tiempo en el CAS esté sincronizado con el DC.Este paso se puede realizar apuntando ambos al mismo servidor de hora. En las configuraciones de laboratorio, señale el CAS al propio DC por tiempo (el DC ejecuta el tiempo de Windows). Kerberos es sensible al reloj y el sesgo no puede ser mayor de 5 minutos (300 segundos).**Nota:** Cuando intenta iniciar el servicio AD SSO del CAS, puede producirse un problema con la sincronización horaria, NTP. Si se configura NTP y no se sincronizan los relojes, los servicios no funcionarán. Una vez reparados, los servicios deben funcionar.
3. Asegúrese de que el dominio de Active Directory esté en mayúsculas (rango) y que el CAS pueda resolver FQDN en DNS. Para configuraciones de laboratorio, puede señalar un DC que ejecute DNS (AD requiere al menos un servidor DNS).
4. Inicie sesión en CAS directamente como https://<*CAS-IP-address*>/admin. A continuación, haga clic en **Registros de soporte** y cambie el nivel de registro para el Registro de comunicación de Active Directory a **Información**.



5. Vuelva a crear el problema y descargue los registros de soporte.

La autenticación de cliente no funciona

Problema

El servicio AD SSO se inicia, pero la autenticación del cliente no funciona.

Solución

Los puertos UDP no estaban abiertos en el rol no autenticado. Después de agregar estos puertos a las políticas de tráfico, la autenticación debe funcionar.

No se puede ejecutar SSO en el PC de Windows 7

Problema

SSO no funciona para equipos que ejecutan el sistema operativo Windows 7.

Solución 1

Para resolver este problema, habilite el cifrado DES en el equipo que ejecuta el sistema operativo Windows 7 y, a continuación, vuelva a ejecutar el KTPass. Complete estos pasos para habilitar DES en un PC con Windows 7:

1. Inicie sesión en el equipo cliente de Windows 7 como administrador.
2. Vaya a **Inicio > Panel de control > Sistema y seguridad > Herramientas administrativas > Política de seguridad local > Políticas/Seguridad local > Opciones**.
3. Elija **Network security > Configure encryption types allowed** .
4. En la ficha Configuración de seguridad local, active las casillas de verificación para activar todas las opciones, excepto la opción Tipos de cifrado futuros.

Solución 2

Para resolver este problema, ejecute este comando en Windows 2003 Server (si también necesita soporte para 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
```

Para obtener más información, consulte Configuración de AD SSO en un Entorno de Windows 7.

No se puede configurar el soporte de cliente linux para un usuario en el entorno NAC

Problema

No se puede configurar el soporte del cliente Linux para un usuario en el entorno NAC.

Solución

Web Agent o Agent no son compatibles con Linux. NAC soporta Linux con inicio de sesión web solamente sin ninguna evaluación de estado. Una vez que la máquina se autentica a través del Login Web, el usuario debe ser asignado a una función de usuario final que configure. El usuario tendrá acceso de acuerdo con la política de tráfico de la función de usuario. Refiérase al bug Cisco CSCti54517 (sólo clientes registrados) para obtener más información.

El servicio SSO se inicia, pero el cliente no realiza SSO

Esto suele deberse a algún problema de comunicación entre el PC cliente/DC o entre el PC cliente y el CAS.

A continuación se indican algunas cosas que se deben verificar:

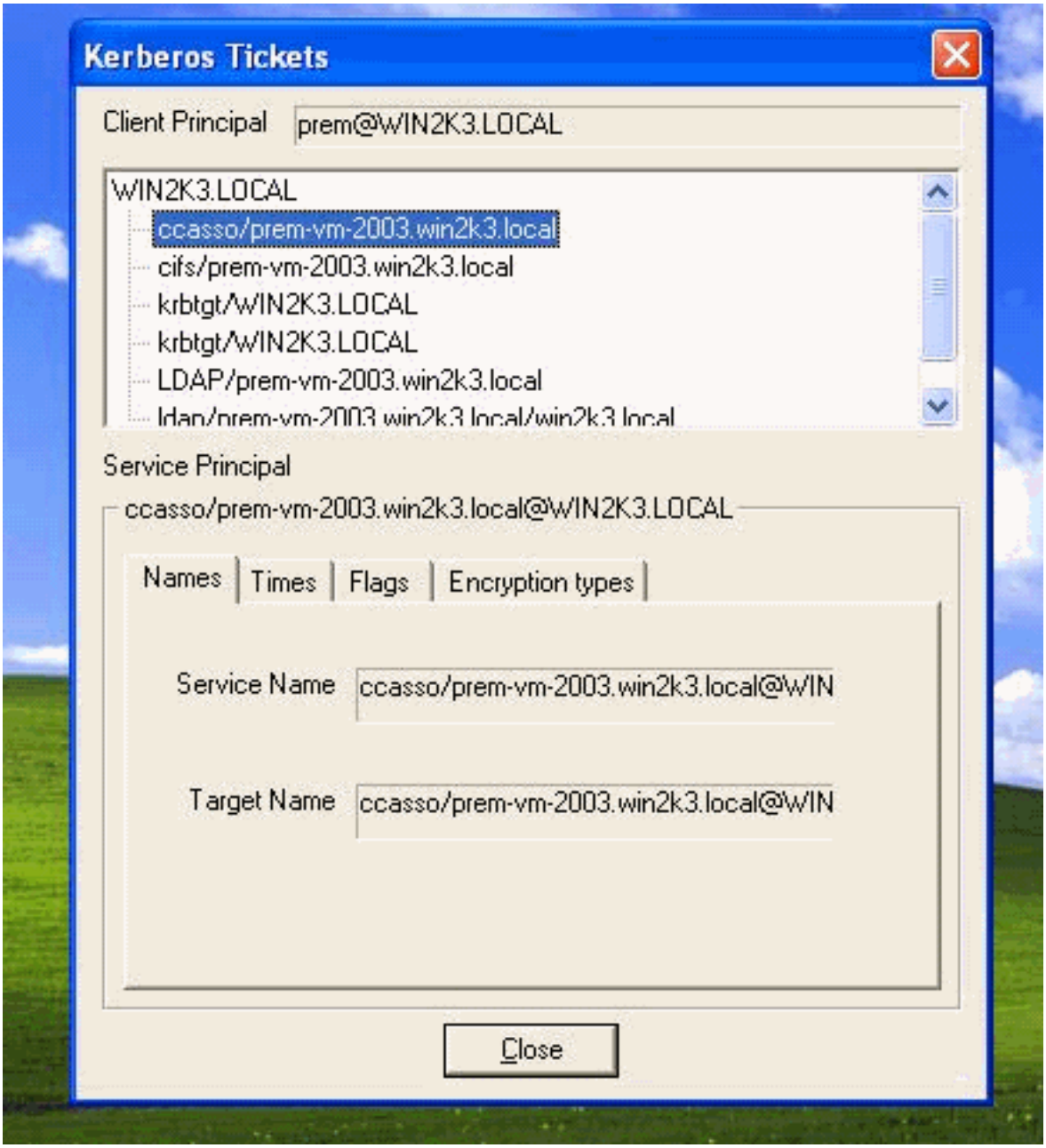
- El cliente tiene claves Kerberos.
- Los puertos están abiertos al DC para que el cliente pueda conectarse, recibir registros de agente y recibir registros en el CAS.
- La hora o el reloj del PC cliente se sincronizan con el DC.
- Confirme que CAS esté escuchando en el puerto 8910. Un rastro del sabueso en el equipo cliente también ayudará.
- CCA Agent es 4.0.0.1 o posterior.
- El usuario ha iniciado sesión utilizando la cuenta de dominio y no utilizando la cuenta local.

Kerbbandeja

Kerbbandeja se puede utilizar para confirmar que el cliente ha obtenido los tickets Kerberos (TGT y ST). La preocupación es por el ticket de servicio (ST), que es para la cuenta CAS que creó en el DC.

Kerbbandeja es una herramienta gratuita disponible en las herramientas de soporte de Microsoft. También se puede utilizar para purgar las notificaciones Kerberos en un equipo cliente.

Un icono verde de la bandeja del sistema indica que el cliente tiene entradas Kerberos activas. Sin embargo, debe verificar que el ticket sea correcto (válido) para la cuenta CAS.



Registros CAS - No se puede iniciar el servicio SSO

El archivo de registro de interés en el CAS es /perfigo/logs/perfigo-redirect-log0.log.0.

El servicio AD SSO no se inicia en CAS es un problema de comunicación CAS-DC:

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
   ```

   Esto significa que el reloj no está sincronizado entre el CAS y el controlador de dominio.
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.
   ```

Esto significa que el nombre de usuario es incorrecto. Observe el nombre de usuario "ccass" incorrecto, el código de error 6 y la última advertencia.

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.
```

La contraseña es incorrecta o el rango no es válido (¿no en mayúsculas?). ¿FQDN erroneo? ¿KTPass se ejecuta incorrectamente? Observe el Error 24 y la última advertencia.**Nota:** Asegúrese de que la versión de KTPass sea 5.2.3790.0. A menos que haya una versión incorrecta de KTPass que, incluso si el script se ejecuta correctamente, el servicio SSO no se iniciará.

Cliente - Problema de comunicación CAS:

```
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))
```

Este error aparece cuando la hora del PC cliente no está sincronizada con el DC.

Nota: La diferencia entre este error y aquel en el que la hora CAS no está sincronizada con el DC.

Problemas conocidos

- Id. de error de Cisco CSCse64395 (sólo clientes registrados) —4.0 El agente no resuelve DNS para Windows SSO.Este problema se resuelve en CCA Agent 4.0.0.1.
- Id. de error de Cisco CSCse46141 (sólo clientes registrados): SSO falla en caso de que CAS no pueda alcanzar el servidor AD durante el inicio.La solución alternativa es ir a **CCA Servers > Manage [CAS_IP] Authentication > Windows Auth > Active Directory SSO**, y hacer clic en **Update** para reiniciar el servicio AD SSO.
- Realice un reinicio del perfigo de servicio en el CAS. Hay un problema de almacenamiento en caché cuando las credenciales antiguas se almacenan en la memoria caché en el CAS y no utiliza la nueva hasta que se reinicie Tomcat.
- No puede limitar el inicio de sesión de usuario único para SSO. Este es el comportamiento normal para SSO porque es un protocolo Kerberos, y no hay opción de limitar el registro de usuario único en un protocolo Kerberos.
- *Windows 7* y *Windows 2008* no admiten SSO ya que SSO utiliza el cifrado DES *que no es compatible con Windows 7 o Windows 2008.*

Información Relacionada

- Página de soporte de Cisco NAC Appliance (Clean Access)
- Soporte Técnico y Documentación - Cisco Systems