Dispositivo NAC (CCA): Configure y resuelva problemas muestra de Windows del Active Directory la sola en (el SSO)

Contenido

Introducción

Este documento describe cómo utilizar muestra del Active Directory de Microsoft Windows la sola (AD) encendido (SSO) para configurar y resolver problemas el dispositivo del Cisco Network Admission Control (NAC), conocido antes como acceso limpio de Cisco (CCA).

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Aseegurese el Windows 2000 SP4 o Windows 2003 (estándar o empresa) SP1 de los funcionamientos de DC o r2 de Windows 2003. Windows 2003 sin el SP1 no se soporta.
- Aseegurese Windows SSO se soporta en un entorno AD solamente. El entorno del Windows NT no se soporta. Se requiere el agente limpio del acceso.
- Configure la cuenta limpia del servidor de acceso (CAS) según lo descrito en el dispositivo NAC de Cisco - guía de instalación y configuración limpia del servidor de acceso, la versión 4.1(2).

Componentes Utilizados

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

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 TécnicosCisco para obtener más información sobre las convenciones del documento.

Configure Windows SSO

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

Configure el proveedor AD SSO

- Usted no puede realizar una prueba de la autenticación a un proveedor o a un VPN SSO AD SSO.
- Se necesita el servidor de las operaciones de búsqueda LDAP solamente si los usuarios quieren hacer las reglas de la asignación para el AD SSO, de modo que después de AD SSO, coloquen a los usuarios en los papeles basados en los atributos AD. Esto no es necesario conseguir el funcionamiento básico SSO (sin la asignación del papel).

Ejecute KTPass en DC

KTPass es una herramienta disponible como parte de Windows 2000/2003 instrumento de apoyo. Refiera al dispositivo NAC de Cisco - Limpie la guía de instalación y configuración del servidor de acceso, libere 4.1(2) para más información.

Cuando usted ejecuta KTPass, es importante observar que el nombre de computadora que baja siempre entre “/” y “@” hace juego el nombre de DC pues aparecería bajo el panel de control > el sistema > nombre de computadora > por completo nombre de computadora en DC.

También, aseegurese que el Nombre de terreno que aparece después @ de resaltado está siempre en las cartas 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, usted debe ejecutar KTPASS tal y como se muestra en de 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
```

También, aseegurese que el Nombre de terreno que aparece después @ de resaltado está siempre en las cartas mayúsculas.

Configure el SSO en CAS

Elija **CCA los servidores > manejan > autenticación > auth de Windows > el Active Directory SSO** para abrir la ventana AD, y verifican estos elementos:

- Dominio de Active Directory: Necesidades del name= del terreno de Kerberos de ser mayúsculo.
- Servidor Active Directory (FQDN): Aseegurese que CAS puede resolver este nombre vía el DNS. Este campo no puede ser una dirección IP. Usando los valores en este ejemplo, usted puede abrir una sesión a CAS vía el Secure Shell (SSH), y realiza el “nslookup prem-vm-2003.win2k3.local”. Entonces, aseegurese lo resuelve con éxito.
- Aseegurese el FQDN hace juego el nombre del servidor AD (DC) exactamente como aparece bajo el panel de control > el sistema > nombre de computadora | Nombre de computadora completo en la máquina servidor AD (DC).

Verifique el servicio SSO se comienza

Complete estos pasos:

1. Va **CCA a los servidores > maneja > el estatus** para verificar que el servicio SSO está comenzado.
2. Funcione con este comando para verificar que CAS ahora escucha en TCP 8910 (usado para Windows SSO).`[root@cs-ccas02 ~]#netstat -a | grep 8910 tcp 0 0 *:8910 *:* LISTEN`

Puertos abiertos a DC

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

Nota: Para probar, abra siempre el acceso completo a DC. Entonces, una vez que el SSO trabaja, usted puede atarlo para tragar a los puertos específicos.

1. Aseegurese los puertos siguientes se permiten en el papel untrusted al Active

Directory:**TCP**: 88, 135, 445, 389/636, 1025, 1026**UDP**: 88, 389**Nota:** *El PUERTO TCP 445* debe estar abierto para la contraseña de Windows reajustada para trabajar correctamente.
2. Asegúrese de que el cliente funcione con CCA el agente 4.0.0.1 o más adelante.
3. Inicie sesión al PC con las credenciales del Dominio de Windows.**Nota:** Aseegurese le están registrando en el dominio y no la cuenta local.

El cliente ve el agente SSO de ejecución

El SSO completó

Usuario SSO visto en la lista de usuario en línea

Troubleshooting Windows SSO

Error: No podía comenzar el servicio SSO. Marque por favor la configuración.

Problema

Usted recibe este error:

Solución

Complete estos pasos para resolver el problema:

1. Marque para aseegurarse los funcionamientos de KTPass correctamente. Es importante marcar los campos como se menciona en la diapositiva X. Si KTPass fue ejecutado incorrectamente, borre la cuenta y cree una nueva cuenta en el AD y ejecute KTPass otra vez.
2. Aseegurese el tiempo en CAS se sincroniza con DC.Este paso puede ser realizado señalándolos ambos al mismo Servidor de tiempo. En configuraciones de laboratorio, señale CAS a DC sí mismo por el tiempo (DC funciona con el tiempo de Windows). El Kerberos es sensible cronometrar y la posición oblicua no puede ser mayor de 5 minutos (300 secs).**Nota:** Cuando usted intenta comenzar el servicio AD SSO de CAS, un problema pudo ocurrir con el syncronization del tiempo, NTP. Si se configura el NTP, y los relojes no syncronized, los servicios no trabajarán. Una vez que están reparados los servicios deben trabajar.
3. Aseegurese el dominio de Active Directory está en el mayúscula (reino) y CAS puede resolver el FQDN en el DNS. Para las configuraciones de laboratorio, usted puede señalar a DC que ejecuta el DNS (el AD requiere en el servidor DNS del arriendo uno).
4. Registro en CAS directamente como <CAS-IP-direccionamiento >/admin de https://. Entonces, los **registros del soporte del** tecleo y cambian el nivel de registro para la comunicación del Active Directory que registra a la **información**.
5. Reconstruya el problema y descargue los registros del soporte.

La autenticación de cliente no trabaja

Problema

Se comienza el servicio AD SSO, pero la autenticación de cliente no trabaja.

Solución

Los puertos UDP no estaban abiertos en el papel del unauthenticated. Después de que usted agregue estos puertos a las políticas de tráfico, la autenticación debe trabajar.

Incapaz de ejecutar el SSO en las ventanas 7 PC

Problema

El SSO no está trabajando para las máquinas que funcionan con el sistema operativo de Windows 7.

Solución 1

Para resolver este problema, la encripción de DES del permiso en la máquina que funciona con el sistema operativo de Windows 7, y entonces vuelve a efectuar el KTPass. Complete estos pasos para habilitar el DES en Windows 7 PC:

1. Inicie sesión a la máquina del cliente de Windows 7 como administrador.
2. Van al **comienzo > al panel de control > al sistema y a la Seguridad > Administrative Tools > Local Security (Seguridad local) la directiva > las políticas locales/Seguridad > opciones**.
3. Elija los **tipos de encripción de la seguridad de la red > de la configuración permitidos**.
4. En Local Security (Seguridad local) las configuraciones tabule, marque las casillas de verificación para habilitar todas las opciones, excepto la opción futura de los tipos de encripción.

Solución 2

Para resolver este problema, funcione con este comando en el servidor de Windows 2003 (si necesita soportar Windows 7 también):

```
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 más información, refiera a la configuración AD SSO en un entorno de Windows 7.

Incapaz de configurar el soporte del cliente de Linux para un usuario en el entorno del NAC

Problema

Incapaz de configurar el soporte del cliente de Linux para un usuario en el entorno del NAC.

Solución

El agente de la red o el agente no se soporta en Linux. Soportes Linux del NAC con el login de la red solamente sin cualquier evaluación de la postura. Una vez que la máquina se autentica con el login de la red, el usuario debe ser asignado a un rol del usuario final que usted configure. El usuario entonces tendrá acceso según la política de tráfico del rol del usuario. Refiera al bug Cisco CSCti54517 (clientes registrados solamente) para más información.

Se comienza el servicio SSO, pero el cliente no realiza el SSO

Esto es generalmente debido a un cierto problema de comunicación entre el DC/client PC o entre PC del cliente y CAS.

Aquí están algunas cosas a verificar:

- El cliente tiene claves del Kerberos.
- Los puertos están abiertos a DC así que el cliente puede conectar, recibir los registros del agente, y recibir abre una sesión CAS.
- El tiempo o el reloj en PC del cliente se sincroniza con DC.
- Confirme CAS está escuchando en el puerto 8910. Una traza de sniffer en PC del cliente también ayudará.
- CCA el agente es 4.0.0.1 o más adelante.
- Abren una sesión al usuario realmente usando la cuenta de dominio y no usando la cuenta local.

Kerbtray

Kerbtray se puede utilizar para confirmar que el cliente ha obtenido los boletos del Kerberos (TGT y ST). La preocupación está para la vigencia máxima de vale de servicio (ST), que está para la cuenta de CAS que usted creó en DC.

Kerbtray es instrumentos de apoyo de la herramienta disponible desde libres de Microsoft. Puede también ser utilizado para purgar los boletos del Kerberos en una máquina del cliente.

Un icono verde de Kerbtray en la bandeja del sistema indica que el cliente tiene boletos activos del Kerberos. Sin embargo, usted necesita verificar que el boleto esté correcto (válido) para la cuenta de CAS.

Registros de CAS – No puede comenzar el servicio SSO

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

El servicio AD SSO no comienza 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 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 incorrecto “ccass”, el código de error 6 y la advertencia más reciente.
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 reino es inválido (no en el mayúscula?). ¿Mún FQDN? ¿KTPass se ejecuta incorrectamente? Observe el error 24 y la advertencia más reciente.**Nota:** Aseegurese que la versión de KTPass es 5.2.3790.0. A menos que haya una mala versión de KTPass que incluso si el script se ejecuta correctamente, el servicio SSO no comenzará.

Cliente – Problema de comunicación de 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))
```

Se considera este error cuando PC del cliente el tiempo no se sincroniza con DC.

Nota: La diferencia entre este error y el donde el tiempo de CAS no se sincroniza con DC.

Problemas conocidos

- El Id. de bug Cisco CSCse64395 (clientes registrados solamente) — el agente 4.0 no resuelve el DNS para Windows SSO.Este problema se resuelve en CCA el agente 4.0.0.1.
- Id. de bug Cisco CSCse46141 (clientes registrados solamente) — El SSO falla en caso de que CAS no pueda alcanzar el servidor AD durante el lanzamiento.La solución alternativa es ir **CCA a los servidores > maneja la autenticación del [CAS_IP] > el auth de Windows > el Active Directory SSO**, y hace clic la **actualización** para recomenzar el servicio AD SSO.
- Realice un reinicio del perfigo del servicio en CAS. Hay un problema de almacenamiento en memoria inmediata cuando las credenciales viejas se ocultan en CAS y no utiliza el nuevo hasta que se recomience Tomcat.
- Usted no puede limitar el login del único usuario para el SSO. Éste es el comportamiento normal para el SSO porque es un protocolo del Kerberos, y no hay opción para limitar el login del único usuario un protocolo del Kerberos.
- *Windows 7* y *Windows 2008* no soportan el SSO mientras que el SSO utiliza la **encripción de DES** que no es soportada por Windows 7 o Windows 2008.

Información Relacionada

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