Javas 7 problemas con AnyConnect, CSD/Hostscan, y el WebVPN - guía de Troubleshooting

Contenido

Introducción

Este documento describe cómo resolver problemas los problemas con las Javas 7 en el (CSD) /Cisco Hostscan del Cliente de movilidad Cisco AnyConnect Secure, del Cisco Secure Desktop, y el clientless SSL VPN (WebVPN).

> Nota: El bug Cisco ID marcado como investigador no se restringe a los síntomas descritos. Si usted hace frente a los problemas con las Javas 7, asegúrese de que usted actualice la versión de cliente de AnyConnect a la última versión de cliente o por lo menos 3.1 a la versión de la versión de mantenimiento 3 disponible en el Cisco Connection Online (CCO).

Resolución general de problemas

Funcione con el verificador de las Javas para marcar si la Java se soporta en los navegadores funcionando. Si la Java se habilita correctamente, revise la consola Java abre una sesión la orden para analizar el problema.

Windows:

Este procedimiento describe cómo habilitar la consola abre una sesión Windows:

1. Abra el panel de control de Windows, y la búsqueda para las Javas.

2. Haga doble clic las **Javas** (el icono de la taza de café). El panel de control Java aparece.
3. Haga clic en la ficha Advanced (Opciones avanzadas).

   Amplíe el **debugging**, y seleccione el **seguimiento del permiso** y **habilite el registro**.Amplíe la **consola Java**, y haga clic la **consola de la demostración**.

Mac

Este procedimiento describe cómo habilitar la consola abre una sesión un mac:

1. Las preferencias del sistema operativo, y hacen doble clic el icono de las Javas (taza de café). El panel de control Java aparece.

2. Haga clic en la ficha Advanced (Opciones avanzadas).

   Bajo la consola Java, haga clic la **consola de la demostración**.Bajo debugging, haga clic el **seguimiento del permiso** y **habilite el registro**.

Troubleshooting específico

AnyConnect

Para los problemas AnyConnect-relacionados, recoja los registros de diagnóstico de la información de AnyConnect (DARDO) así como los registros de la consola Java.

Windows:

El Id. de bug Cisco CSCuc55720, “IE causa un crash con las Javas 7 cuando el paquete 3.1.1 se habilita en el ASA,” era un problema conocido, donde el Internet Explorer causó un crash cuando un WebLaunch fue realizado y AnyConnect 3.1 fue habilitado en el headend. Se ha reparado este bug.

Usted puede ser que encuentre los problemas cuando usted utiliza algunas versiones de AnyConnect y de las Javas 7 con los subprogramas Java. Para más información, vea el Id. de bug Cisco CSCue48916, “rotura del subprograma Java al usar AnyConnect 3.1.00495 o 3.1.02026 y Java el v7."

Problemas con las Javas 7 y las llamadas del socket del IPv6

Si AnyConnect no conecta incluso después usted actualiza el Entorno de tiempo de ejecución Java (JRE) a las Javas 7, o si una aplicación Java no puede conectar sobre el túnel VPN, revise los registros de la consola Java y busque estos mensajes:

```
java.net.SocketException: Permission denied: connect
at java.net.DualStackPlainSocketImpl.waitForConnect(Native Method)
at java.net.DualStackPlainSocketImpl.socketConnect(Unknown Source)
```

Estas entradas de registro indican que el cliente/la aplicación hace las llamadas del IPv6.

Una solución para este problema es inhabilitar el IPv6 (si es parada) en el adaptador Ethernet y el adaptador virtual de AnyConnect (VA):

Una segunda solución es configurar las Javas para preferir el IPv4 sobre el IPv6. Fije la propiedad Propiedad del sistema 'java.net.preferIPv4Stack “verdad” tal y como se muestra en de estos ejemplos:

- Agregue el código para la propiedad Propiedad del sistema al código de las Javas (para las aplicaciones Java escritas por el cliente):

  ```
  System.setProperty("java.net.preferIPv4Stack" , "true");
  ```
- Agregue el código para la propiedad Propiedad del sistema de la línea de comando:

  ```
  -Djava.net.preferIPv4Stack=true
  ```
- Fije las variables de entorno _JPI_VM_OPTIONS y _JAVA_OPTIONS para incluir la propiedad Propiedad del sistema:

  ```
  -Djava.net.preferIPv4Stack=true
  ```

Para la información adicional, refiérase:

- ¿Cómo fijar java.net.preferIPv4Stack=true en el código de las Javas?
- ¿Cómo forzar las Javas para utilizar en lugar de otro el IPv6 ipv4?

Una tercera solución es inhabilitar el IPv6 totalmente en las máquinas de Windows; edite esta entrada de registro:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\TCPIP6\Parameters
```

Para la información adicional, vea cómo inhabilitar el IP versión 6 o a sus componentes específicos en Windows.

Problemas con AnyConnect WebLaunch después de la actualización de las Javas 7

El código del Javascript de Cisco buscó previamente Sun como el valor para el vendedor de las Javas. Sin embargo, el Oracle cambió ese valor según lo descrito en JDK7: Cambios de la propiedad del vendedor de las Javas. Este problema fue reparado por el Id. de bug Cisco CSCub46241, “weblaunch de AnyConnect falla del Internet Explorer con las Javas el 7."

Mac

No se ha señalado ningunos problemas. Las pruebas con AnyConnect 3.1 (con la configuración de WebLaunch/del safari/del mac 10.7.4/Javas 7.10) no muestran ningún error.

Miscelánea

Problemas con el Apps de las Javas 7 en Cisco AnyConnect

Se ha clasifiado el Id. de bug Cisco CSCue48916, “rotura del subprograma Java al usar AnyConnect 3.1.00495 o 3.1.02026 y Java el v7,". La investigación inicial indica que los problemas no son un bug en el lado del cliente, pero se pudo relacionar con la configuración de la máquina virtual Java (VM) en lugar de otro.

Previamente, para utilizar las Javas 7 apps en el cliente de AnyConnect 3.1(2026), usted desmarcó las configuraciones del adaptador virtual del IPv6. Sin embargo, es necesario ahora completar todos los pasos en este procedimiento:

1. Instale la versión 3.1(2026) de AnyConnect.
2. Desinstale las Javas 7.
3. Reiniciar.
4. Instale las Javas SE 6, la actualización 38, disponible en el sitio web del Oracle.
5. Navegue a las Javas 6 configuraciones del panel de control, después haga clic la lengueta de la **actualización** para actualizar a la última versión de Java 7.
6. Abra un comando prompt y ingrese:

```
setx _JAVA_OPTIONS -Djava.net.preferIPv4Stack=true
```

7. Inicie sesión con AnyConnect, y los subprogramas Java deben trabajar.

Nota: Este procedimiento se ha probado con las Javas 7 actualizaciones 9, 10, y 11.

CSD/Hostscan

Para los problemas CSD/Hostscan-related, recoja los registros del DARDO así como los registros de la consola Java.

Para obtener los registros del DARDO, el nivel de registro CSD se debe dar vuelta a hacer el debug de en el ASA:

1. Navegue al **ASDM** > a la **configuración** > al **VPN de acceso remoto** > al **administrador** > a las **configuraciones globales del Secure Desktop**.
2. Dé vuelta encima del CSD que registra a hacer el debug de en el Cisco Adaptive Security Device Manager (ASDM).
3. Utilice el DARDO para recoger los registros CSD/Hostscan.

Windows:

Hostscan es susceptible a las caídas similares a ésas descritas previamente para AnyConnect en Windows (Id. de bug Cisco CSCuc55720). El problema hostscan ha sido resuelto por el Id. de bug Cisco CSCuc48299, “IE con las Javas 7 caídas en HostScan Weblaunch.”

Mac

Problemas con las versiones 3.5.x CSD y las Javas 7

En CSD 3.5.x, todo el fall de las conexiones WebVPN; esto incluye los lanzamientos de la red de AnyConnect. Los registros de la consola Java no revelan ninguna problemas:

```
Java Plug-in 10.10.2.12
Using JRE version 1.7.0_10-ea-b12 Java HotSpot(TM) 64-Bit Server VM
User home directory = /Users/rtpvpn
----------------------------------------------------
c: clear console window
f: finalize objects on finalization queue
g: garbage collect
h: display this help message
l: dump classloader list
m: print memory usage
o: trigger logging
q: hide console
r: reload policy configuration
s: dump system and deployment properties
t: dump thread list
v: dump thread stack
x: clear classloader cache
0-5: set trace level to <n>
----------------------------------------------------
```

Si usted retrocede a JRE 6 o actualiza el CSD a 3.6.6020 o más adelante, los registros de la consola Java revelan los problemas:

```
Java Plug-in 10.10.2.12
Using JRE version 1.7.0_10-ea-b12 Java HotSpot(TM) 64-Bit Server VM
User home directory = /Users/rtpvpn
----------------------------------------------------
c: clear console window
f: finalize objects on finalization queue
g: garbage collect
h: display this help message
l: dump classloader list
m: print memory usage
o: trigger logging
q: hide console
r: reload policy configuration
s: dump system and deployment properties
t: dump thread list
v: dump thread stack
x: clear classloader cache
0-5: set trace level to <n>
----------------------------------------------------
CacheEntry[ https://rtpvpnoutbound6.cisco.com/CACHE/sdesktop/install/binaries/
instjava.jar ]: updateAvailable=false,lastModified=Wed Dec 31 19:00:00 EST
1969,length=105313
Fri Oct 19 18:12:20 EDT 2012 Downloaded
https://rtpvpnoutbound6.cisco.com/CACHE/sdesktop/hostscan/darwin_i386/cstub
to /var/folders/zq/w7l9gxks7512fsl4vk07v9nc0000gn/T/848638312.tmp/cstub
```

```
Fri Oct 19 18:12:20 EDT 2012 file signature verification
PASS: /var/folders/zq/w7l9gxks7512fsl4vk07v9nc0000gn/T/848638312.tmp/cstub
Fri Oct 19 18:12:20 EDT 2012 Spawned CSD stub.
```

La resolución es actualizar el CSD o retroceder las Javas. Porque Cisco recomienda que usted funciona con la última versión del CSD, usted debe actualizar el CSD, bastante que las Javas del downgrade, especialmente puesto que un downgrade de las Javas puede ser difícil en un mac.

Problemas con Chrome y safari con WebLaunch en el mac 10.8

Los problemas con Chrome y el safari son conducta esperada:

- Chrome es navegador de 32 bits y no soporta las Javas 7.
- Chrome nunca ha sido oficialmente buscador admitido para WebLaunch.
- El mac 10.8 inhabilitó el uso de las Javas 7 en el safari, y las versiones anteriores de las Javas no se habilitan por abandono.

Si usted hace ya las Javas 7 instalar, las resoluciones son:

- Utilice Firefox.
- Habilite las Javas 7 en el safari:

  Verifique que la Java 7 esté instalada en el mac y que se ha recomenzado el mac. Abra Firefox, y vaya al verificador de las Javas.Abra el safari, y vaya el verificador de las Javas otra vez. Usted debe ahora ver esta pantalla:

- Inhabilite las Javas 7, y habilite las Javas SE 6 proporcionadas por Apple.

  Consejo: Si usted no hace las Javas instalar o usted tiene una versión anterior de las Javas, usted es probable ver el mensaje de error “Java bloqueada para este sitio web” en java.com. Vea las actualizaciones de las Javas disponibles para OS X en agosto 28, 2013 en el foro del soporte de Apple para la información sobre las actualizaciones de la instalación de java.

Problemas con el safari con WebLaunch en el mac 10.9

Si usted usted está en el mac 10.9 y tiene ya el habilitado del plug-in de Javas (según lo descrito en los problemas con Chrome y el safari con WebLaunch en la sección del mac 10.8), el WebLaunch pudo continuar fallando. Se inician todos los subprogramas java, pero el navegador continúa simplemente haciendo girar. Si los registros de las Javas se habilitan según lo descrito en la sección de Troubleshooting general, los registros se llenan rápidamente como se muestra aquí:

```
at java.lang.Thread.run(Thread.java:744)
Mon Dec 16 16:00:17 EST 2013 Failed to download cstub
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
```

```
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
network: Created version ID: 1.7.0.45
```

Busque este tipo de entrada anterior en el registro:

```
Mon Dec 16 16:00:17 EST 2013 Downloaded https://rave.na.sage.com/CACHE/
sdesktop/hostscan/darwin_i386/manifest java.io.FileNotFoundException:
/Users/user1/.cisco/hostscan/bin/cstub (Operation not permitted) at
java.io.FileInputStream.open(Native Method)
```

Esto indica que usted está encontrando el Id. de bug Cisco CSCuj02425, “WebLaunch en OSX 10.9 falla si se inhabilita el modo inseguro de las Javas.” Para la solución alternativa este problema, modifica las preferencias de las Javas así que las Javas pueden ejecutarse en el modo inseguro para el safari:

1. **Preferencias del** tecleo.
2. El tecleo **maneja las configuraciones del sitio web**.
3. En la **ficha de seguridad**, seleccione las **Javas**, y observe que **Allow** está seleccionada por abandono.
4. El cambio **permite ejecutarse en el modo inseguro**.

WebVPN

Para los problemas del WebVPN relacionados con las Javas, recoja estos datos para los propósitos de Troubleshooting:

- Salida del comando **showtech-support**.
- Registros de la consola Java con y sin el dispositivo de seguridad adaptante (ASA) como se explica en la sección de Troubleshooting general.
- Capturas del WebVPN.
- Capturas del reloj HTTP en la máquina local con y sin el ASA.

- Capturas estándar de los paquetes en el ASA y en la máquina local. En la máquina local, estas capturas se pueden hacer con Wireshark.Para la información sobre cómo capturar el tráfico en el ASA, vea configurar a las capturas de paquetes.
- Todos los archivos JAR descargados a las Javas ocultan al pasar con el ASA. Esto es un ejemplo de la consola Java:

  ```
  Reading Signers from 8412
  https://rtpvpnoutbound6.cisco.com/+CSCO+00756767633A2F2F7A2D73767972662E6
  E7067727A76687A2E6179++/mffta.jar
  C:\Users\wvoosteren\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\41\
  6a0665e9-1f510559.idx
  ```
  En este ejemplo, 6a0665e9-1f510559.idx es la versión ocultada de mffta.jar 7. Si usted no tiene acceso a estos archivos, usted puede recogerlos del caché de las Javas al usar la conexión directa.

Una Configuración de prueba puede apresurar la resolución.

Funciones de seguridad en las Javas 7 U51 y cómo ese afecta a los usuarios de WebVPN

Los cambios recientemente anunciados programaron para la actualización 51 (enero de 2014) de las Javas 7 han establecido que el resbalador predeterminado de la Seguridad requiere las firmas del código y los permisos manifiesten el atributo. En resumen, todos los subprogramas java requieren:

- para ser firmado (applet y aplicaciones de comienzo de la red).
- para fijar el atributo de los “permisos” dentro del evidente.

Las aplicaciones son afectadas si utiliza las Javas comenzadas a través de un buscador Web. Las aplicaciones se ejecutan de ningunos donde fuera de un buscador Web están muy bien. Cuál este los medios para WevVPN son todos los plug-in del cliente que son distribuidos por Cisco podrían ser afectados. Puesto que estos plug-in no son mantenidos ni son soportados por Cisco, Cisco no puede realizar los cambios al certificado de firma del código o al applet para asegurarlo cumple con estas restricciones. La solución apropiada para esto es utilizar el certificado de firma del código temporal en el ASA. Los ASA proporcionan un certificado temporal de la firma de código para firmar los subprogramas java (para el rewriter y los plug-in de las Javas). El certificado temporal deja los subprogramas java realizar sus funciones previstas sin un mensaje de advertencia. Los administradores ASA deben substituir el certificado temporal antes de que expire con su propio certificado de firma del código publicado por un Certificate Authority (CA) de confianza. Si esto no es una opción viable, la solución alternativa es completar estos pasos:

1. Usted puede utilizar la característica de la lista de sitios de la excepción en las configuraciones de las Javas de la máquina del cliente del extremo para ejecutar las aplicaciones bloqueadas por los ajustes de seguridad. Los pasos para hacer esto se describen en los problemas con el safari con WebLaunch en el mac 10.9.
2. Usted puede también bajar los ajustes de seguridad de las Javas. Esta configuración también se fija en las configuraciones de las Javas de la máquina del cliente como se muestra aquí:

   Advertencia: El uso de las estas soluciones alternativas todavía le da algunos errores, pero la Java no bloquea la aplicación pues habría hecho sin las soluciones alternativas en el lugar.

Windows:

Las aplicaciones que inician los subprogramas java han estado señaladas para fallar sobre el WebVPN después de una actualización a las Javas 7. Este problema es causado por la falta del algoritmo de troceo seguro (soporte SHA)-256 para el rewriter de las Javas. El Id. de bug Cisco CSCud54080, el soporte "SHA-256 para el rewriter de las Javas del webvpn," se ha clasifiado para este problema.

Las aplicaciones que comienzan los subprogramas java a través del portal con el túnel elegante pudieron fallar cuando se utiliza JRE7; esto es la más común con los sistemas 64-bit. En las capturas, observe que la Java VM envía los paquetes en el texto claro, no a través de la conexión del túnel elegante al ASA. Esto ha sido dirigida por el Id. de bug Cisco CSCue17876, "algunos subprogramas java no conectará vía el túnel elegante en las ventanas con el jre1.7."