Solución de problemas de terminal seguro bloqueado en aislamiento con métodos de recuperación

Contenido

Introducción

Este documento describe el proceso para recuperar un punto final con el conector de punto final seguro instalado desde el modo de aislamiento.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conector de terminal seguro
- Consola de terminal segura
- función de aislamiento de terminales

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Secure Endpoint console versión v5.4.2021092321

- Conector de Secure Endpoint para Windows versión v7.4.5.20701
- Versión v1.21.0 de conexión Mac de terminal seguro

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

El procedimiento descrito en este documento es útil en situaciones en las que el dispositivo de punto final está atascado en este estado y no es posible inhabilitar el modo de aislamiento.

El aislamiento de terminales es una función que permite bloquear la actividad de la red (entrada y salida) en un ordenador para evitar amenazas como la fuga de datos y la propagación de malware. Está disponible en:

- Versiones de 64 bits de Windows compatibles con la versión 7.0.5 y posteriores del conector de Windows
- Versiones para Mac compatibles con la versión 1.21.0 y posteriores del conector para Mac.

Las sesiones de aislamiento de terminales no afectan a la comunicación entre el conector y la nube de Cisco. Los terminales cuentan con el mismo nivel de protección y visibilidad que antes de la sesión. Puede configurar las Listas de direcciones de IP Isolation Allow para evitar que el conector bloquee las direcciones IP en cuestión mientras una sesión de aislamiento de terminal activa está activa. Puede revisar información más detallada sobre la función de aislamiento de terminales aquí.

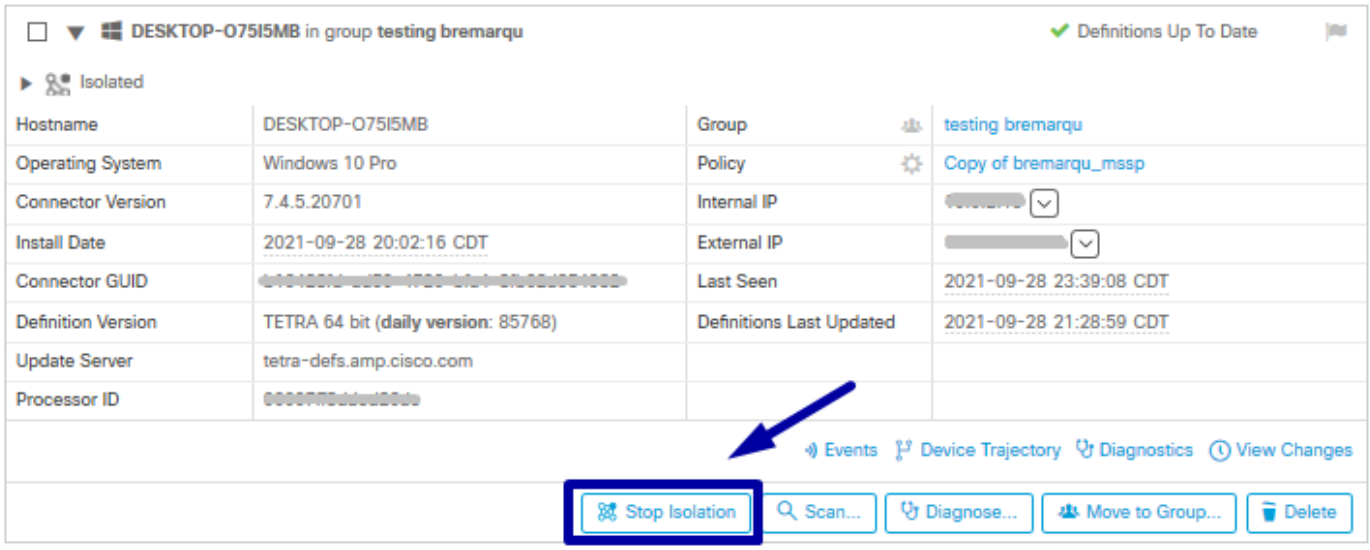
Detener el aislamiento

Una vez que desee detener el aislamiento de terminales en un equipo, siga estos pasos rápidos a través de la consola de Secure Endpoint o la línea de comandos.

Detención de la sesión de aislamiento de la consola

Para detener una sesión de aislamiento y restaurar todo el tráfico de red a un terminal.

Paso 1. En la consola, navegue hasta **Administración > Equipos**.
Paso 2. Busque el equipo en el que desea detener el aislamiento y haga clic para mostrar los detalles.
Paso 3. Haga clic en el botón **Stop Isolation**, como se muestra en la imagen.



Paso 4. Introduzca cualquier comentario sobre por qué ha detenido la función de aislamiento en el terminal.

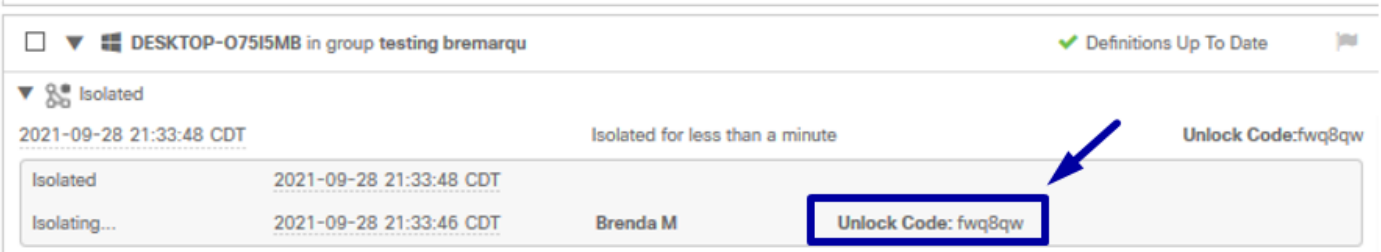
Detener la sesión de aislamiento desde la línea de comandos

Si un terminal aislado pierde su conexión con la nube de Cisco y no puede detener la sesión de aislamiento desde la consola. En estas situaciones, puede detener la sesión localmente desde la línea de comandos con el código de desbloqueo.

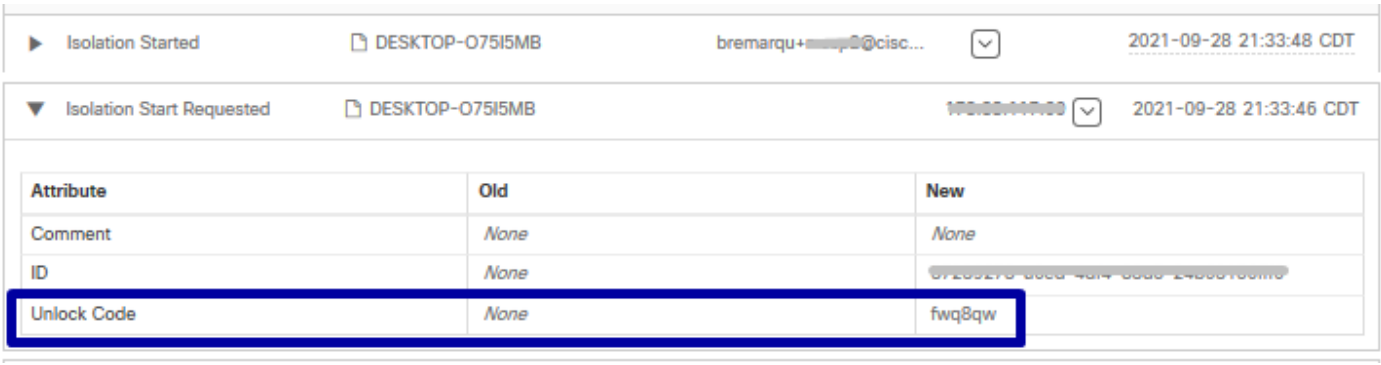
Paso 1. En la consola, navegue hasta **Administración > Equipos**.

Paso 2. Busque el equipo en el que desea detener el aislamiento y haga clic para mostrar los detalles.

Paso 3. Observe el **Código de desbloqueo**, como se muestra en la imagen.



Paso 4. También puede encontrar el **Código de desbloqueo** si navega hasta **Cuenta > Registro de auditoría**, como se muestra en la imagen.



Paso 5. En el equipo aislado, abra un símbolo del sistema con privilegios de administrador.

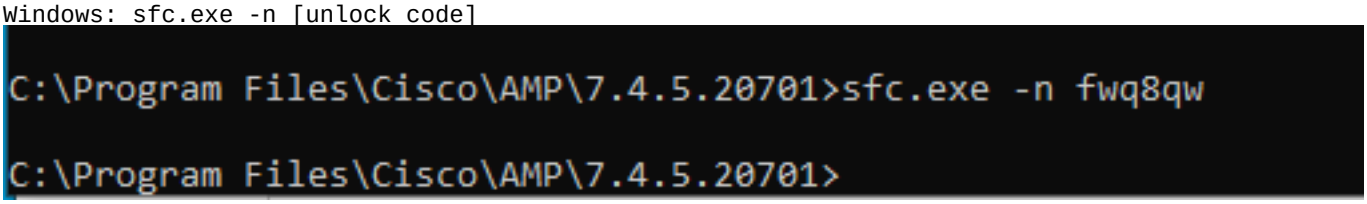
Paso 6. Desplácese hasta el directorio donde está instalado el conector

Windows: C:\Program Files\Cisco\AMP\[número de versión]

Mac: /opt/cisco/amp

Paso 7. Ejecute el comando stop

```
Windows: sfc.exe -n [unlock code]
```




```
Mac: ampcli isolate stop [unlock code]
```

> **Precaución**: Si el código de desbloqueo se ingresa incorrectamente 5 veces, es necesario esperar 30 minutos antes de realizar otro intento de desbloqueo.

Solución de problemas de recuperación

En caso de que haya agotado todas las vías y aún no pueda recuperar un terminal aislado de la consola de Secure Endpoint o localmente con el código de desbloqueo, puede recuperar el terminal aislado con los métodos de recuperación de emergencia.

Recuperación de Mac:

Quite la configuración de aislamiento y reinicie Secure Endpoint Service

```
sudo rm /Library/Application\ Support/Cisco/Secure\ Endpoint/endpoint_isolation.xml
sudo launchctl unload /Library/LaunchDaemons/com.cisco.amp.daemon.plist
sudo launchctl load /Library/LaunchDaemons/com.cisco.amp.daemon.plist
```

Recuperación de Windows:

Método de aislamiento de recuperación desde la línea de comandos

En situaciones en las que el dispositivo de terminal esté atascado de forma aislada y no sea posible desactivar el aislamiento a través de la consola de terminal seguro o con el código de desbloqueo, siga estos pasos.

Paso 1. Detenga el servicio de conector a través de la interfaz de usuario del conector o los **servicios de Windows**.

Paso 2. Localice el servicio de conector de terminal seguro y detenga el servicio.

Paso 3. En el equipo aislado, abra un símbolo del sistema con privilegios de administrador.

Paso 4. Ejecute el comando **reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\Immunet Protect" /v "unlock_code" /f** como se muestra en la imagen.

```
reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\Immunet Protect" /v "unlock_code" /f
```

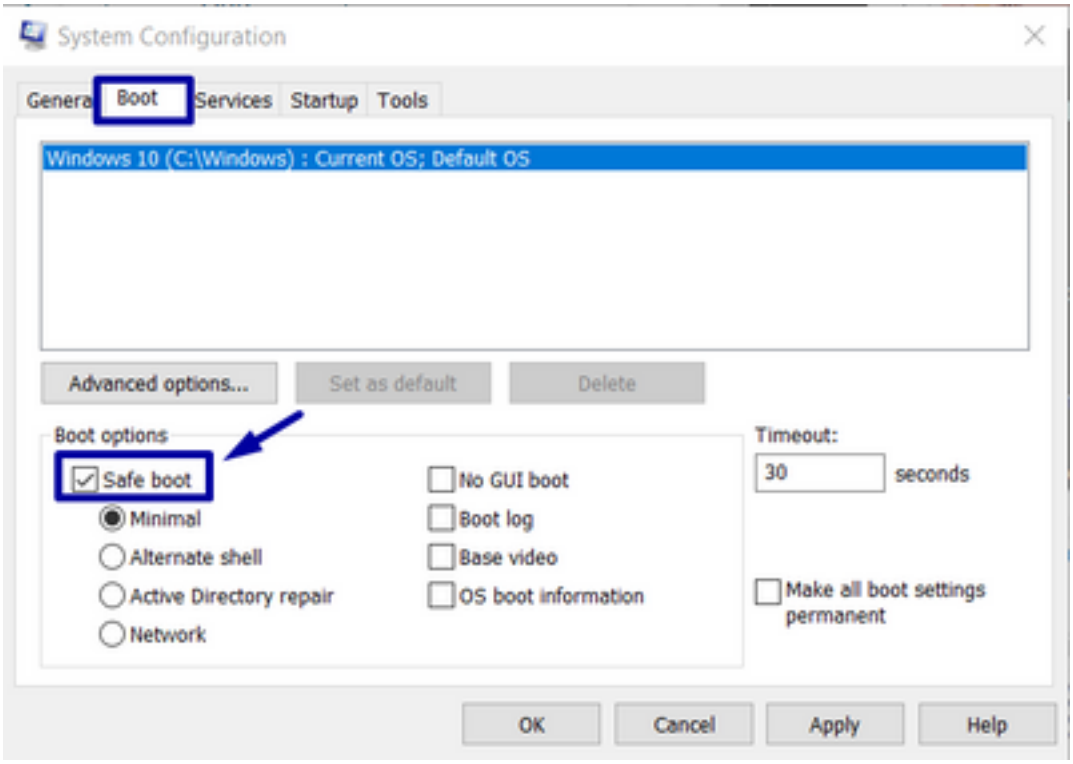
```
C:\Windows\system32>reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\Immunet Protect" /v "unlock_code" /f
The operation completed successfully.

C:\Windows\system32>
```

Paso 5. El mensaje **La operación se completó correctamente** indica que la operación se completó. (Si se muestra otro mensaje, como "Error: Access is denied" (Error: Acceso denegado), debe detener el servicio de conector de Secure Endpoint antes de ejecutar el comando).

Paso 6. Inicie el servicio de conector de terminal seguro.

> **Sugerencia**: si no puede detener el servicio conector de Secure Endpoint desde la interfaz de usuario del conector o los servicios de Windows, puede realizar un arranque seguro.

En el terminal aislado, navegue hasta **System Configuration > Boot > Boot options** y seleccione **Safe boot**, como se muestra en la imagen.



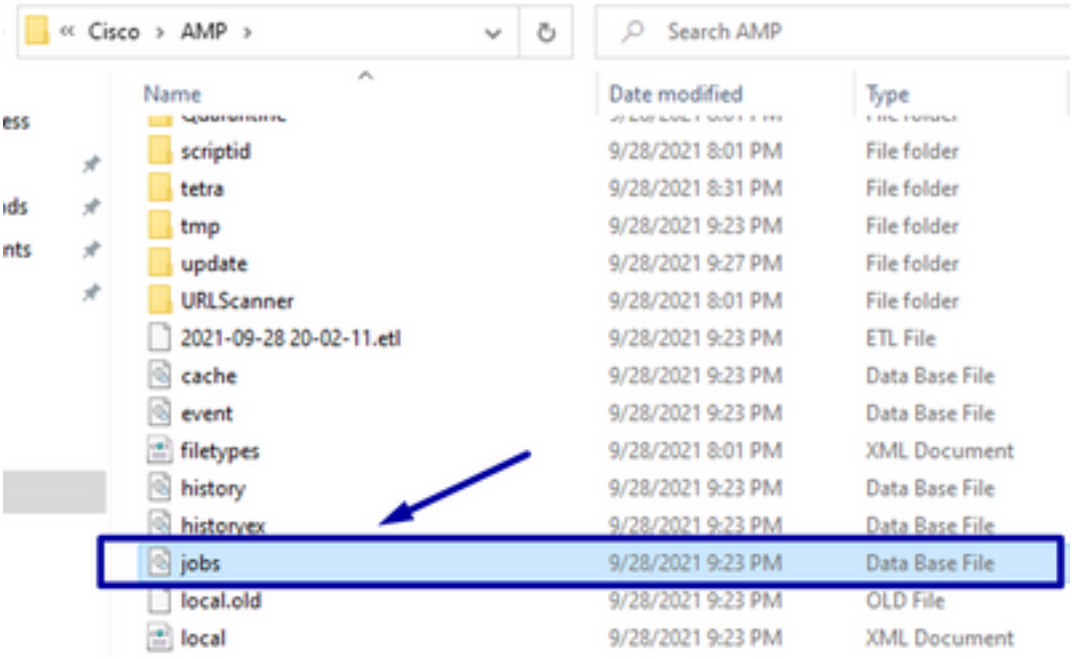
Método de aislamiento de recuperación sin la línea de comandos

En caso de que su dispositivo de terminal se quede atascado en aislamiento y no sea posible inhabilitar el aislamiento a través de la consola de Secure Endpoint o con el código de desbloqueo o incluso si no puede utilizar la línea de comandos, siga estos pasos:

Paso 1. Detenga el servicio de conector a través de la interfaz de usuario del conector o los **servicios de Windows**.

Paso 2. Navegue hasta el directorio donde está instalado el conector

(C:\Program Files\Cisco\AMP\) y elimine el archivo **jobs.db**, como se muestra en la imagen.



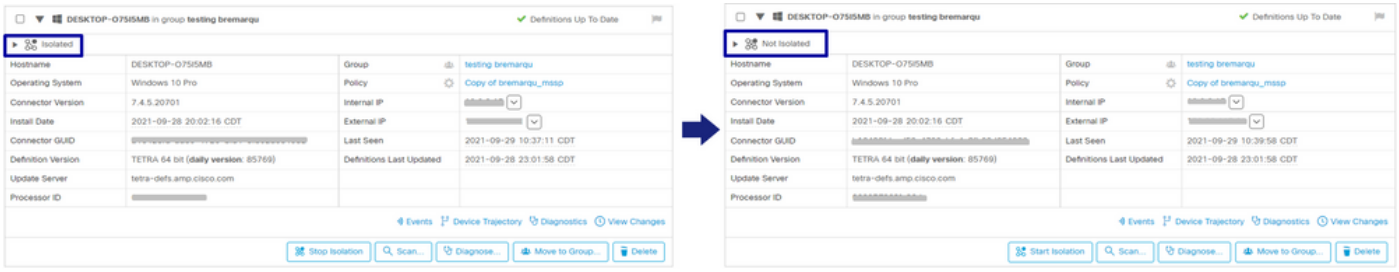
3. Reinicie el ordenador.

Además, si ve el evento Isolation en la consola, puede desplazarse hasta **Detalles del error** para revisar el código de error y su descripción, como se muestra en la imagen.

Verificación

Para verificar que el terminal ha vuelto del aislamiento o ya no está aislado, puede ver que la interfaz de usuario de Secure Endpoint Connector muestra el estado de aislamiento como **No aislado**, como se muestra en la imagen.

Desde la consola de Secure Endpoint, si navega por **Management > Computers** y localiza el equipo en cuestión, puede hacer clic para mostrar los detalles. El estado de aislamiento muestra **No aislado**, como se muestra en la imagen.



Información Relacionada

- [Guía del usuario de terminales seguros]
- [Soporte Técnico y Documentación - Cisco Systems]

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).