

Troubleshooting del sistema de control de acceso seguro (ACS 5.x y posterior)

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Problema: "Error: Guardó la configuración corriente del archivo de manifiesto del lanzamiento con éxito a % no encontrado en el conjunto" en el dispositivo ACS durante la actualización del dispositivo](#)

[Solución](#)

[Problema: Incapaz de recomenzar al servidor ACS 5.x del GUI](#)

[Solución](#)

[Problema: Problema que configura la autenticación del Active Directory con ACS 5.2](#)

[Solución](#)

[Problema: No puede ver más de 100 páginas en el informe de las estadísticas](#)

[Solución](#)

[Problema: Incapaz de generar el informe de la autenticación del paso/del fall para un grupo de dispositivos](#)

[Solución](#)

[Problema: La supervisión y la base de datos de los informes es actualmente inasequibles. El intentar volver a conectar en 5 segundos.](#)

[Solución](#)

[Problema: Tema 22056 no encontrado en los almacenes aplicables de la identidad](#)

[Solución](#)

[Problema: Incapaz de integrar el ACS con el Active Directory](#)

[Solución](#)

[Problema: Incapaz de integrar el ACS con el LDAP](#)

[Solución](#)

[Problema: "error del acs internal operations diagnostics del cisco: no podía escribir mensaje de error al archivo del almacenamiento local el"](#)

[Solución](#)

[Problema: Incapaz de integrar el ACS 5.1 con el Active Directory](#)

[Solución](#)

[Problema: Incapaz de configurar ACS 5.x para reconocer las expresiones normales en las reglas de selección del servicio](#)

[Solución](#)

[Problema: El respaldo SFTP no está funcionando al usar Cisco trabaja como el servidor SFTP](#)

[Solución](#)

Problema: "Payload inválido EAP caído"

Solución

Problema: "El proceso del tiempo de ejecución ACS no se está ejecutando en este caso ahora."

Solución

Problema: Incapaz de exportar a los usuarios con la contraseña

Solución

Problema: Inhabilitan a los usuarios internos ACS intermitentemente

Solución

Problema: "Autenticación de TACACS+ petición terminada con el error"

Solución

Problema: "Rechazada petición de la autenticación de RADIUS debido al error de registro crítico"

Solución

Problema: Demostraciones "actualización de la interfaz de la opinión ACS de los datos fallada" en la cima de la página cuando el ACS se actualiza a partir el 5.2 a 5.3

Solución

Problema: Problema con la "contraseña del cambio en los acs siguientes del login" en Cisco ACS 5.0

Solución

Problema: "% de la actualización de aplicación fallada, error - -999. Marque por favor ADE los registros para los detalles, o el reestreno con - la aplicación del debug instala - habilitado" en el dispositivo ACS durante la actualización

Solución

Problema: Autenticación del error "fallada: Resultado enviado 12308 clientes TLV que indica el error"

Solución

Problema: Los servidores Active Directory del error "24495 no están disponibles"

Solución

Problema: Sesión del error "5411 EAP medida el tiempo hacia fuera"

Solución

Problema: la autenticación del 802.1x no trabaja si las restricciones del inicio se configuran en el Active Directory

Solución

Problema: Error: "Le no autorizan a ver la página pedida" cuando el ACS 5.x admin con el papel de ChangeUserPassword cambia la contraseña

Solución

Problema: Consiguiendo el error en ACS 5.x para los servidores Active Directory de la autenticación fallida "24495 no esté disponible."

Solución

Problema: Incapaz de conectar con el dispositivo ACS usando el BMC

Solución

Problema: Una alarma amonestadora "cancelación 20000 sesiones" con la causa "sesiones activas está sobre el límite", aparezca en el monitor y señale el panel general.

Solución

Problema: Paquete RADIUS del error "11013 ACS 5.x ya en el de proceso"

Solución

Problema: La autenticación de RADIUS fallada con el paquete RADIUS del error "11012 contiene la encabezado inválida"

Solución

Problema: La autenticación RADIUS/TACACS+ fallada con el error "11007 no podía localizar el dispositivo de red o al cliente AAA"

Solución

Problema: La autenticación de RADIUS falló con caída pedido de RADIUS del error "11050 debido a la sobrecarga del sistema".

Solución

Problema: La autenticación de RADIUS falló con el atributo incorrecto del v2 del error "11309 RADIUS MS-CHAP."

Solución

Problema: El ACS señala el uso de la memoria sobre el 90%. Alarma

Solución

Problema: error: com.cisco.nm.ac s.mgmt.msgbus.FatalBusException: No podido conectar los Nodos

Solución

Problema: error: com.cisco.nm.ac s.mgmt.msgbus.FatalBusException: No podido conectar los Nodos

Solución

Problema: el error 11026 el dACL pedido no se encuentra

Solución

Problema: el error 11025 el pedido el dACL pedido está faltando un atributo del Cisco-av-pair con el valor aaa: event=acl-download. Se rechaza la petición

Solución

Problema: el error 11023 el dACL pedido no se encuentra. Esto es un nombre desconocido del dACL

Solución

Problema: Autenticación de administrador fallada con el error interno del error 10001. Versión de la configuración incorrecta

Solución

Problema: Autenticación de administrador fallada con el error interno del error 10002: Error cargar el servicio apropiado

Solución

Problema: Autenticación de administrador fallada con el error interno del error 10003: La autenticación de administrador recibió el nombre en blanco del administrador

Solución

Problema: Razón del error: El error relacionado de 24428 conexiones ha ocurrido en LRPC, el LDAP o el KERBEROS

Solución

Problema: La autenticación auth-proxy TACACS+ no está trabajando en un router que ejecuta IOS 15.x del servidor ACS 5.x

Solución

Problema: Conseguir el error del almacén de mensaje de error (acs-xxx, TacacsAccounting) de ACS 5.x

Solución

Problema: La autenticación de usuario fallada con el error "11036 el atributo de RADIUS del Mensaje-authenticator es inválida."

Solución

[Problema: Las estadísticas RADIUS fallaron con la petición caída "11037 de las estadísticas del error recibida vía el puerto sin apoyo."](#)

[Solución](#)

[Problema: Las estadísticas RADIUS falladas con la encabezado de la Estadística-petición del error "11038 RADIUS contienen el campo inválido del authenticator."](#)

[Error: "24493 ACS tiene problemas que comunican con el Active Directory usando sus credenciales de la máquina."](#)

[Solución](#)

[Problema: "Al crear los nombres del perfil del shell con los caracteres especiales tenga gusto "del ê", ACS puede causar un crash."](#)

[Solución](#)

[Problema: Conseguir el "error sintáctico en la línea 2: no bien formado \(token inválido\)" mientras que ejecuta "la demostración ejecútese" en el ACS 5.x CLI.](#)

[Solución](#)

[Problema: La división ACS 5.x /opt se llena muy rápidamente](#)

[Solución](#)

[Problema: Preguntar el dominio deseado](#)

[Solución](#)

[Problema: Padre y Dominios hijo al mismo tiempo](#)

[Solución](#)

[Problema: Registro a la base de datos remota](#)

[Solución](#)

[Problema: Soporte de VMware](#)

[Solución](#)

[Problema: Requisitos de espacio de disco](#)

[Solución](#)

[Problema: "24401 no podía establecer la conexión con el agente del Active Directory ACS."](#)

[Solución](#)

[Problema: El proceso del "Runtime" muestra el estado fallado "ejecución"](#)

[Solución](#)

[Problema: Autenticación ACS fallada cuando el UCS fuerza la reautenticación](#)

[Solución](#)

[Problema: La operación del Active Directory "24444 ha fallado debido a un error no especificado en el ACS"](#)

[Solución](#)

[Problema: Incapaz de autenticar a los usuarios ACS 5.1 con el servidor del r2 AD 2008](#)

[Solución](#)

[Error: Tema 22056 no encontrado en los almacenes aplicables de la identidad.](#)

[Solución](#)

[Problema: ipt_connlimit: Oops: ¿Estado inválido ct?](#)

[Solución](#)

[Problema: Los AC 5.x/ISE no ven el atributo llamar-estación-identificación del radio en un pedido de RADIUS del Cisco IOS Software Release 15.x NAS](#)

[Solución](#)

[Problema: Las cuentas de usuario consiguen bloqueadas en el primer caso de las credenciales incorrectas incluso si están configuradas para 3 tentativas](#)

[Solución](#)

[Problema: Unbale para salvar la salvaguardia del ACS](#)

[Solución](#)

[Información Relacionada](#)

[Introducción](#)

Este documento proporciona la información sobre cómo resolver problemas el Cisco Secure Access Control System (ACS) y cómo resolver los mensajes de error.

Para la información sobre cómo resolver problemas el Cisco Secure ACS 3.x y 4.x, refiera al [troubleshooting del servidor del control de acceso seguro \(ACS 3.x y 4.x\)](#).

[prerrequisitos](#)

[Requisitos](#)

No hay requisitos específicos para este documento.

[Componentes Utilizados](#)

La información en este documento se basa en la versión 5.x y posterior del Cisco Secure Access Control System.

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.

[Problema: "Error: Guardó la configuración corriente del archivo de manifiesto del lanzamiento con éxito a % no encontrado en el conjunto" en el dispositivo ACS durante la actualización del dispositivo](#)

El error: Guardó la configuración corriente del archivo de manifiesto del lanzamiento con éxito a % no encontrado en el conjunto que aparece el error cuando una tentativa se hace para actualizar el ACS expreso a partir del 5.0 a 5.0.1.

[Solución](#)

Complete estos pasos para actualizar el dispositivo ACS sin ningún problema:

1. Descargue la corrección 9 ([5-0-0-21-9.tar.gpg](#)) y ADE-OS (ACS_5.0.0.21_ADE_OS_1.2_upgrade.tar.gpg) de: **Cisco.com > > Security (Seguridad) del software del soporte > de la descarga > Cisco Secure Access Control System 5.0 > software del sistema > 5.0.0.21 de control de acceso seguro**
2. Después de que usted instale los dos archivos, instale la actualización [ACS 5.1.0.44.tar.gz](#) ACS 5.1. Ésta es disponible desde la misma trayectoria del paso anterior.
3. Utilice este comando para instalar la actualización:
[application upgrade <application-bundle> remote-repository-name](#)

Esto completa el procedimiento de actualización.

Refiera a [actualizar a un servidor ACS a partir del 5.0 a 5.1](#) para más información sobre cómo actualizar el dispositivo ACS.

[Problema: Incapaz de recomenzar al servidor ACS 5.x del GUI](#)

Esta sección explica porqué usted no puede recomenzar la versión 5.x del servidor ACS del GUI.

[Solución](#)

No hay opción disponible recomenzar el servidor ACS 5.x del GUI. El ACS se puede recomenzar solamente del CLI.

[Problema: Problema que configura la autenticación del Active Directory con ACS 5.2](#)

Al configurar la autenticación del Active Directory (AD) para un nuevo servicio de 5.2 ACS, se recibe este mensaje de error:

```
Error inesperado RPC: Negada acceso debido a la configuración o al Error de red inesperada.  
Intente por favor --adinfo de la opción detallada o del funcionamiento " --diag".
```

[Solución](#)

El ACS necesita los permisos de escritura para autenticar con el AD. Para resolver este problema, proporcione los permisos de escritura temporales a la Cuenta de servicio.

[Problema: No puede ver más de 100 páginas en el informe de las estadísticas](#)

Al intentar generar un informe de las estadísticas de la aduana AAA con el ACS versión 5.1, usted no puede ver más de 100 páginas. Esto no cubre varios más viejos informes. ¿Cómo usted cambia esta configuración para ver todas las páginas?

[Solución](#)

Usted no puede cambiar el número de páginas en el ACS porque el número máximo de páginas visualizadas es solamente 100 por abandono. Para superar esta limitación y ver más viejas

estadísticas, usted necesita cambiar las opciones de filtro para poder hacer coincidencias más específicas. Por ejemplo, si usted intenta generar el informe para los treinta días más pasados, contiene un de gran capacidad y las 100 páginas más recientes pudieron mostrar la actividad para solamente la hora más pasada. Aquí, usando las opciones de filtro se aconseja. Tomar la opción de filtro como identificación del usuario y especificar el tiempo-rango rendirán mucho más viejos informes.

Problema: Incapaz de generar el informe de la autenticación del paso/del fall para un grupo de dispositivos

Este problema ocurre al intentar generar el informe de la autenticación solamente para un grupo de seis Routers/Switches, no para todos los dispositivos. Se utiliza el ACS versión 4.x.

Solución

Esto no es posible con ACS 4.x. Usted necesita emigrar a ACS 5.x porque esta característica está disponible con esa versión. Usted puede extraer los informes para el grupo específico de dispositivos generando los [informes del catálogo](#).

Refiera a esta imagen para una mejor comprensión:

Problema: La supervisión y la base de datos de los informes es actualmente inasequibles. El intentar volver a conectar en 5 segundos.

Cuando usted hace clic la supervisión del lanzamiento y señala el Visualizador de ACS 5.x, se recibe este mensaje de error: La supervisión y la base de datos de los informes es actualmente inasequibles. El intentar volver a conectar en 5 segundos. Si persiste el problema, satisfaga entran en contacto a su administrador ACS.

Solución

Realice una de estas soluciones alternativas para resolver este problema:

- Recomience los servicios ACS del CLI publicando estos comandos:
`application stop acs`
`application start acs`
- Actualización a la última corrección disponible. Refiera a [aplicar las correcciones de la actualización](#) para más información sobre esto.

Problema: Tema 22056 no encontrado en los almacenes aplicables de la identidad

Los usuarios AD no consiguen autenticados con el ACS versión 5.x y reciben este mensaje de error: Tema 22056 no encontrado en los almacenes aplicables de la identidad.

Solución

Este mensaje de error ocurre cuando el ACS no pudo encontrar al usuario en la primera base de datos enumerada que se configura en la secuencia del almacén de la identidad. Esto es un mensaje de información y no afecta al funcionamiento del ACS. La manera que el ACS 5.x realiza la autenticación para interno o los usuarios externos es diferentes que la versión anterior 4.x. Con la versión 5.x, hay una opción llamada secuencia de Identity Store para definir la secuencia de bases de datos de usuarios que se autenticarán. Para más información, refiera a [configurar las secuencias del almacén de la identidad](#).

Si usted recibe este error cuando usted está utilizando el ACS para autenticar las peticiones contra un Dominio hijo, después usted tiene que agregar un sufijo del UPN o el prefijo NETBIOS al nombre de usuario. Para más información, refiera a las notas en la sección de [Microsoft AD](#).

Problema: Incapaz de integrar el ACS con el Active Directory

Los usuarios no pueden integrar el ACS con el Active Directory, y se recibe el mensaje de error del error del estado del puerto de la samba.

Solución

Para resolver este problema, asegúrese estos puertos están abierto soportar las funciones del Active Directory:

- Puerto de la samba - TCP 445
- LDAP - TCP 389
- LDAP - UDP 389
- KDC - TCP 88
- kpasswd - TCP 464
- NTP UDP 123
- Catálogo global - TCP - 3268
- DNS - UDP 53

El ACS necesita alcanzar todo el DCS en el dominio para que la integración ACS-AD sea completo. Incluso si uno de DCS no es accesible del ACS, la integración no sucede. Refiera al Id. de bug Cisco [CSCte92062](#) ([clientes registrados solamente](#)) para más información.

Problema: Incapaz de integrar el ACS con el LDAP

En este documento, el ACS 5.2 se utiliza como RADIUS AAA servidor para la implementación del 802.1x. el 802.1x se puede utilizar con éxito con el ACS usando el almacén del usuario interno, pero hay problemas que integran el ACS y el LDAP. Se visualiza este mensaje de error:

```
Radius authentication failed for USER: example MAC:  
UU-VV-WW-XX-YY-ZZ AUTHTYPE: PEAP(EAP-MSCHAPv2)  
EAP session timed out : 5411 EAP session timed out
```

Solución

El en este caso, LDAP se está utilizando con el PEAP y el método de autenticación interna usado es el v2 EAP-MSCHAP. Esto fallará porque el LDAP no se soporta para PEAP (v2 EAP-MSCHAP). Se recomienda para utilizar EAP-TLS o el AD.

Problema: “error del acs internal operations diagnostics del cisco: no podía escribir mensaje de error al archivo del almacenamiento local el”

Durante la replicación del ACS, el ACS primario no replica correctamente y visualiza este mensaje de error:

```
cisco acs_internal_operations_diagnostics error: could
not write to local storage file
```

Solución

Recomience los servicios ACS y asegúrese el registro crítico se inhabilita. Para más información, refiera al Id. de bug Cisco [CSCth66302](#) ([clientes registrados solamente](#)). Si esto no ayuda, entrar en contacto el [TAC de Cisco](#) para conseguir la última corrección ACS conveniente resolver este problema.

Problema: Incapaz de integrar el ACS 5.1 con el Active Directory

Al intentar implementar la integración AD, se recibe este mensaje de error:

```
Error while configuring Active Directory:Using writable
domain controller:test1.test.pvt Authentication error due unexpect
configuration or network error. Please try the --verbose option or run 'adinfo
-dia' to diagnose the problem. Join to domain 'test.pvt', zone 'null'
failed.
```

Solución

Complete esta solución alternativa para reparar este problema:

1. Borre la cuenta de equipo existente en el AD.
2. Cree un nuevo OU.
3. Vaya a las propiedades del OU y desmarque **heredan los permisos**.
4. Cree una nueva máquina explican el ACS en el nuevo OU.
5. Permita que el AD replique.
6. Intente unirse al AD del ACS GUI.

En algunos casos, es también útil si usted entra en contacto Microsoft y aplica el [arreglo caliente](#) .

Problema: Incapaz de configurar ACS 5.x para reconocer las expresiones normales en las reglas de selección del servicio

Solución

Esto no es posible porque todavía no se soporta en ACS 5.x.

Problema: El respaldo SFTP no está funcionando al usar Cisco trabaja como el servidor SFTP

Cuando el recurso de red está en Servidor CiscoWorks, el planificador de trabajos de reserva trabaja muy bien con otros clientes SFTP, pero no ACS 5.2. Específicamente, al intentar conectar con el servidor SFTP del ACS, se recibe el `incapaz de negociar un mensaje de error del método del intercambio de claves`.

Solución

En este caso, el servidor SFTP no es un dispositivo obediente FIP usando el DH 14 grupos. Servidores de los soportes ACS solamente con el soporte DH 14 pues es FIP obedientes. Para más información sobre este problema, refiera a las [limitaciones conocidas en ACS 5.2](#).

Problema: "Payload inválido EAP caído"

El error: Se recibe el mensaje de error `caído payload inválido EAP` mientras que autentica a los usuarios de red inalámbrica a la corrección 7. ACS 5.0.

Solución

Esto es una conducta observada y dirigido en el bug Cisco ID [CSCsz54975](#) ([clientes registrados solamente](#)) y [CSCsy46036](#) ([clientes registrados solamente](#)).

Para resolver este problema, actualización a la corrección 9 ACS 5.0, que se requiere como parte de la actualización a 5.1 o a 5.2. Refiera a [actualizar la base de datos](#) para los detalles completos. Esto también incluye la información sobre cómo actualizar para parchear 9.

Problema: "El proceso del tiempo de ejecución ACS no se está ejecutando en este caso ahora."

Los usuarios no pueden iniciar sesión al ACS GUI y se recibe este mensaje de error:

"El proceso del tiempo de ejecución ACS no se está ejecutando en este caso ahora. Los cambios se pueden realizar a la configuración de ACS (éstos serán guardados en la base de datos), pero los cambios no tomarán el efecto hasta que se recomience el proceso del tiempo de ejecución."

Solución

Manualmente el recomienzo del proceso del tiempo de ejecución del CLI y reiniciar el dispositivo resuelve este problema. Esto es un problema de menor importancia y no crea ningún problema de rendimiento para el ACS. Hay dos bug de menor importancia clasificados para observar este comportamiento. Para más información, refiera al bug Cisco ID [CSCtb99448](#) ([clientes registrados solamente](#)) y [CSCtc75323](#) ([clientes registrados solamente](#)).

Para recomenzar los procesos del tiempo de ejecución manualmente, publique estos comandos del ACS CLI:

- tiempo de ejecución de la parada de los acs
- tiempo de ejecución del comienzo de los acs

Problema: Incapaz de exportar a los usuarios con la contraseña

Usted puede exportar e importar la base de datos de usuarios a otro ACS 5.x con archivo CSV, pero no incluye el campo de contraseña del usuario (aparece en blanco). ¿Cómo usted mueve el almacén de la identidad de un usuario local a partir de un ACS a otro que incluya la información de contraseña?

Solución

Esto no es tan posible que esto llegará a ser una violación de la seguridad. En este caso, una solución alternativa es realizar un procedimiento de backup y restauración. Sin embargo, la limitación a esta solución alternativa es que el de reserva y el restore trabaja solamente para otro ACS con una configuración similar.

Problema: Inhabilitan a los usuarios internos ACS intermitentemente

Inhabilitan a los usuarios de ACS intermitentemente con una `contraseña expiraron` mensaje. La directiva del vencimiento de contraseña se fija por 60 días, pero estos usuarios deben ser habilitados manualmente para que consigan el acceso.

Solución

Este comportamiento se observa y se clasifica en el Id. de bug Cisco [CSCtf06311](#) ([clientes registrados solamente](#)). Este problema puede ser resuelto aplicando la corrección 3 a ACS 5.1. Para ver todos los Problemas resueltos bajo la corrección 3, refiera a los [Problemas resueltos en la corrección acumulativa ACS 5.1.0.44.3](#). Para la información relacionada en cómo actualizar la corrección, refiera a [aplicar las correcciones de la actualización](#).

Problema: “Autenticación de TACACS+ petición terminada con el error”

El informe de la autenticación ACS muestra `autenticación de TACACS+ la petición terminada con el mensaje de error del error`.

Solución

Esto ocurre cuando la autenticación de TACACS tiene el tipo de servicio fijado al PPP. Refiera al Id. de bug Cisco [CSCte16911](#) ([clientes registrados solamente](#)) para más información.

Problema: La “petición de la autenticación de RADIUS rechazó debido al error de registro crítico”

La autenticación de RADIUS se rechaza con el `rechazada petición de la autenticación de RADIUS debido al mensaje de error crítico del error de registro`.

Solución

Este error se detalla en el Id. de bug Cisco [CSCth66302](#) ([clientes registrados solamente](#)).

Problema: Las demostraciones “actualización de la interfaz de la opinión ACS de los datos fallaron” en la cima de la página cuando el ACS se actualiza a partir el 5.2 a 5.3

La actualización de los datos de las demostraciones de la interfaz de la opinión ACS falló en la cima de la página cuando el ACS se actualiza a partir el 5.2 a 5.3.

Solución

Este error se detalla en el Id. de bug Cisco [CSCtu15651](#) ([clientes registrados solamente](#)).

Problema: Problema con la “contraseña del cambio en los acs siguientes del login” en Cisco ACS 5.0

Solución

En ACS 5.0, la función del vencimiento de contraseña (el usuario debe cambiar la contraseña en el inicio siguiente) en el almacén local de la identificación del usuario es a elección, pero no trabaja. El pedido de mejora [CSCtc31598](#) repara el problema en el ACS versión 5.1.

Problema: “% de la actualización de aplicación fallaron, error - - 999. Marque por favor ADE los registros para los detalles, o el reestreno con - la aplicación del debug instala - habilitado” en el dispositivo ACS durante la actualización

Los % de la actualización de aplicación fallaron, error - -999. Marque por favor ADE los registros para los detalles, o el reestreno con - la aplicación del debug instala - el error habilitado aparece cuando una tentativa se hace para actualizar un ACS expreso a partir del 5.0 a 5.0.1.

Solución

Este error ocurre cuando el repositorio usado es TFTP y el tamaño del archivo es mayor que 32MB. El ACS expreso no puede manejar los archivos mayores que 32MB. Utilice el FTP como repositorio para resolver este problema incluso si el tamaño del archivo es más que 32MB.

Problema: Autenticación del error “fallada: Resultado enviado 12308 clientes TLV que indica el error”

La autenticación fallada: El resultado enviado 12308 clientes TLV que indica el error del error ocurre en el ACS cuando usted intenta autenticar por primera vez. La autenticación trabaja muy bien la segunda vez.

Solución

Este error puede ser resuelto cuando usted inhabilita **rápidamente vuelve a conectar**. Una actualización **para parchear 2 del ACS versión 5.2** ayuda a resolver el problema sin el rápido vuelve a conectar ser inhabilitado.

Este error puede también ser resuelto cuando usted inhabilita **cryptobinding forzado** en el supplicant. Refiera al Id. de bug Cisco [CSCtj31281 \(clientes registrados solamente\)](#) para más información.

Problema: Los servidores Active Directory del error "24495 no están disponibles"

La autenticación comienza a fallar con este error: 24495 servidores Active Directory no están disponibles. en los registros ACS 5.3.

Solución

Marque el archivo de ACSADAgent.log con el CLI del ACS 5.x para los mensajes por ejemplo: 11 de marzo 00:06:06 xlpacs01 adclient[30401]: <bg de la INFORMACIÓN: conexión perdida del bindingRefresh> base.bind.healing al xxxxxxxx. El ejecutarse en el modo disconnected: abra. Si usted ve el funcionamiento en el disconnectedmode: abra el mensaje de error, esto significa que el ACS 5.3 no puede mantener una conexión estable con el Active Directory. La solución alternativa está al Switch al LDAP o retrocede el ACS a la versión 5.2. Refiera al Id. de bug Cisco CSCtx71254 ([registeredcustomersonly](#)) para más información.

Problema: Sesión del error "5411 EAP medida el tiempo hacia fuera"

5411 mensajes de error hacia fuera medidos el tiempo sesión EAP se reciben en ACS 5.x.

Solución

Los tiempos de espera de la sesión EAP son muy comunes con el PEAP donde el supplicant recomienza la autenticación después de que el paquete inicial salga al servidor de RADIUS y, la mayor parte del tiempo, no es indicativo de un problema.

El flujo que está comúnmente - considerado es:

```
Supplicant ----- Authenticator ----- ACS
Connect
<-----Request for Identity
-----> Response Identity ----->
<----- EAP Challenge <-----
EAPOL-Start ----->
normal flow ending in successful authentication.....
```

En el extremo la autenticación es acertada. Sin embargo, hay un hilo dejado abierto en el ACS debido al reinicio precipitado de la sesión EAP del supplicant que causa una autenticación satisfactoria seguida por el mensaje del tiempo de espera de la sesión EAP. Muchas veces esto

es debido al driver llano de la máquina. Asegúrese que los drivers NIC/Wireless son actualizados en la máquina del cliente. Usted puede capturar en el cliente y el filtro en el EAP || EAPOL para ver lo que recibe o envía el cliente al conectar.

Problema: la autenticación del 802.1x no trabaja si las restricciones del inicio se configuran en el Active Directory

la autenticación del 802.1x no trabaja si los usuarios tienen restricciones del inicio configuradas en el Active Directory.

Solución

Si usted tiene Active Directory fijado las restricciones del inicio para una sola máquina e intenta una autenticación del 802.1x. La autenticación falla porque en la perspectiva del Active Directory que la autenticación está viniendo del ACS, no la máquina que la restricción del inicio está fijada a. Para que la autenticación sea acertada, las restricciones del inicio se pueden fijar para incluir las cuentas de equipo ACS.

Problema: Error: “Le no autorizan a ver la página pedida” cuando el ACS 5.x admin con el papel de ChangeUserPassword cambia la contraseña

El Usuario administrador ACS 5.x GUI con el papel de **ChangeUserPassword** no puede cambiar la contraseña del usuario AAA salvado en la base de datos interna. Después de cambiar la contraseña, el usuario recibe este mensaje de error móvil: Le no autorizan a ver la página pedida.

Solución

Esto puede ocurrir cuando la base de datos ACS 5.x se emigra de ACS 4.x. Utilice el privilegio de **SuperAdmin** para cambiar la contraseña del usuario. Refiera al Id. de bug Cisco [CSCty91045](#) ([clientes registrados solamente](#)) para más información.

Problema: Consiguiendo el error en ACS 5.x para los servidores Active Directory de la autenticación fallida "24495 no esté disponible.”

Solución

Usted necesita verificar la integración de Active Directory con ACS 5.x. Si es una configuración distribuida, asegúrese que el ACS primario y secundario 5.x en la configuración esté integrado correctamente con el Active Directory.

Problema: Incapaz de conectar con el dispositivo ACS usando el BMC

Cuando utilizan al cliente BMC (una herramienta del nivel del hardware) para conseguir en los servidores de IBM ACS 1121, se observa que el cliente BMC tiene dos IP Addresses.

Solución

Este comportamiento se ha identificado y abrió una sesión el Id. de bug Cisco [CSCtj81255](#) ([clientes registrados solamente](#)). Para resolver esto, usted necesita inhabilitar al Cliente de DHCP BMC en el ACS 1121.

Problema: Una alarma amonestadora “cancelación 20000 sesiones” con la causa “sesiones activas está sobre el límite”, aparezca en el monitor y señale el panel general.

Hay un límite a la cantidad de registros que un directorio de la sesión puede sostener. Porque las peticiones que sondan son pesadas en la configuración de cliente, el límite se alcanza rápidamente. Después de alcanzar el límite, por el diseño, la ACS-vista borra algunos expedientes (por ejemplo, 20k) del directorio de la sesión y envía una alerta. Usted puede aumentar este límite, pero no ayuda a mucho excepto para prolongar la alerta.

Solución

Para resolver esto, realice el siguiente:

- Se sugiere para inhabilitar la orden de apertura de sesión para ver la base de datos. Van al **Cisco Secure ACS > a la administración del sistema > a la configuración > las categorías a la configuración > al registro del registro > global > las “autenticaciones pasajeras” > blanco del syslog remoto** y quitan **LogCollector** de las blancos seleccionadas. Van al **Cisco Secure ACS > a la administración del sistema > a la configuración > las categorías a la configuración > al registro del registro > global > los “intentos fallidos” > blanco del syslog remoto** y quitan **LogCollector** de las blancos seleccionadas. Van al **Cisco Secure ACS > a la administración del sistema > a la configuración > las categorías a la configuración > al registro del registro > global > editan: Las “estadísticas RADIUS” > blanco del syslog remoto** y quitan **LogCollector** de las blancos seleccionadas.
- Usted puede ignorar los pedidos de autenticación que sondan porque éstos no son pedidos de autenticación reales. Siga los pasos descritos a continuación: Vaya al **Cisco Secure ACS > monitoreando Configuration > System el filtro de la configuración > Add** y cree el filtro. Crear el filtro basado en el *Nombre de usuario* es más apropiado porque se entienden las peticiones que sondan de ser enviado con un nombre de usuario falso. Si usted crea una política de acceso separada en el ACS para procesar estas peticiones que sondan, después los filtros se pueden crear sobre la base del *servicio del acceso* también.

Problema: Paquete RADIUS del error "11013 ACS 5.x ya en el de proceso"

En un despliegue ACS 5.3, autenticación del dot1x del fall de los usuarios. La base de datos usada es un Active Directory. El código de falla RADIUS se muestra aquí:

Solución

El ACS ha ignorado esta petición porque es un duplicado de otro paquete que se esté procesando actualmente. Esto puede ocurrir debido a ninguno de estos:

- La estadística media del tiempo de espera del pedido de RADIUS está cercana a o excede el descanso del pedido de RADIUS del cliente del cliente.
- El almacén externo de la identidad puede ser muy lento.
- Se ha sobrecargado El ACS.

Realice estos pasos para resolver:

1. Aumente el descanso del pedido de RADIUS del cliente del cliente.
2. Utilice un almacén externo más rápido o adicional de la identidad.
3. Siga las maneras de reducir la sobrecarga en el ACS.

Problema: La autenticación de RADIUS fallada con el paquete RADIUS del error "11012 contiene la encabezado inválida"

Solución

La encabezado del paquete RADIUS entrante no analizó correctamente. Para resolver esto, verifique el siguiente:

- Marque el dispositivo de red o al cliente AAA por problemas de hardware.
- Marque la red que conecta el dispositivo con el ACS por problemas de hardware.
- Marque si el dispositivo de red o el cliente AAA tiene cualesquiera problemas de compatibilidad sabidos RADIUS.

Problema: La autenticación RADIUS/TACACS+ fallada con el error "11007 no podía localizar el dispositivo de red o al cliente AAA"

Este mensaje de error se recibe en el ACS cuando un ASA envía un mensaje del pedido de acceso del radio:

11007 no podía localizar el dispositivo de red o al cliente AAA

Solución

Esto ocurre porque hay una discordancia entre el IP del cliente ACS y el IP de la interfaz que envía realmente la petición. El Firewall realiza a veces una traducción de la dirección a este cliente AAA. Verifique si configuran al cliente AAA correctamente con la dirección IP traducida correcta en esta trayectoria:

Recursos de red > dispositivos de red y clientes AAA

Problema: Autenticación de RADIUS fallada con caída pedido de RADIUS del error "11050 debido a la sobrecarga del sistema".

Los usuarios no pueden acceder la red debido a las fallas de autenticación. Este mensaje de error del ACS se recibe:

```
11050 caída pedido de RADIUS debido a la sobrecarga del sistema
```

Solución

Cisco ACS cae estos pedidos de autenticación debido a la sobrecarga. Esto se puede causar por la replicación de muchas peticiones paralelas del authentication. Para evitar esto, realice ninguno de estos:

- Modifique las configuraciones del **cliente de la red Device/AAA** de modo que utilice la opción del **soporte de la sola conexión de la herencia TACACS+**. Con esto, el cliente reutilizará la misma sesión para todas las peticiones en vez de crear muchas sesiones.
- Refrénese de los usuarios de invocar los nuevos pedidos de autenticación para una cierta punta del tiempo.
- Recomience al servidor ACS.

Problema: La autenticación de RADIUS falló con el atributo incorrecto del v2 del error "11309 RADIUS MS-CHAP."

Solución

Este error ocurre debido a la duración no válida o al valor incorrecto a partir del uno de los atributos del v2 MSCHAP (MS-GRIETA-desafío, MS-GRIETA-respuesta, MS-CHAP-CPW-2, o MS-GRIETA-NT-Enc-picovatio) en el paquete access-request recibido RADIUS.

Problema: El ACS señala el uso de la memoria sobre el 90%. Alarma

El ACS señala el uso de la memoria sobre 90%. Alarm tal como el siguiente: Cisco Secure ACS - Alarma NotificationSeverity: Nombre ACS de la Alarma crítica - El sistema HealthCause/la alarma del activador causada por el ACS - thresholdAlarm de los Estados generales del sistema detalla la utilización entrada-salida del disco de la utilización de la memoria de la utilización de la CPU del caso ACS (%) (%) (%) /opt usado espacio en disco (%) /localdisk usado espacio en disco: El espacio en disco (de %) utilizó/(%) KOM-AAA02 0.41 90.14 0.02 9.57 5.21 25.51

Solución

Este problema se considera generalmente en ACS 5.2. Para reparar este problema, recargue el ACS para liberar la memoria o la actualización la corrección a 7 ACS 5.2 o a más adelante. Refiera al Id. de bug Cisco [CSCtk52607](#) ([clientes registrados solamente](#)) para más información.

Problema: error: com.cisco.nm.ac

[s.mgmt.msgbus.FatalBusException: No podido conectar los Nodos](#)

En una configuración distribuida después de una tarea de mantenimiento (que se une a una replicación completa primaria, de la fuerza, parcheando), el caso A ACS señala el caso B ACS como off-liné adentro la pantalla distribuida del despliegue, mientras que B está realmente en línea y señala el caso A como en línea. En los registros de la Administración, usted ve el `error: com.cisco.nm.ac s.mgmt.msgbus.FatalBusException: No podido conectar los Nodos.`

[Solución](#)

Esto puede ocurrir si un caso anterior del servicio de administración de la replicación todavía está limitado al puerto 2030 cuando la nueva instancia sube e intenta atar a ese puerto. Del CLI del caso B ACS, ejecútese: `los acs-registros del sho clasifican ACSManagement. registro | i servicio de la replicación.` Usted verá los mensajes tales como `replicación mantener fallado.: Puerto ya funcionando: 2030.` Actualmente, la solución alternativa es recomenzar el caso B (el ACS que señala el otro como en línea). Refiera al Id. de bug Cisco [CSCtx56129](#) ([clientes registrados solamente](#)) para más información.

[Problema: error: com.cisco.nm.ac s.mgmt.msgbus.FatalBusException: No podido conectar los Nodos](#)

En una configuración distribuida después de una tarea de mantenimiento (que se une a una replicación completa primaria, de la fuerza, parcheando), el caso A ACS señala el caso B ACS como off-liné adentro la pantalla distribuida del despliegue, mientras que B está realmente en línea y señala el caso A como en línea. En los registros de la Administración, usted ve el `error: com.cisco.nm.ac s.mgmt.msgbus.FatalBusException: No podido conectar los Nodos.`

[Solución](#)

Actualice la corrección a 6 ACS 5.2 o a más adelante para reparar este problema. Refiera al Id. de bug Cisco [CSCto47203](#) ([clientes registrados solamente](#)) para más información.

Nota: El respaldo del viewDB fallará una vez que el uso del `""` del `"" /opt` excede del 30%. Se requiere configurar el estacionamiento NFS para realizar un respaldo cuando el `""` del `"" /opt` excede el uso del 30%.

[Problema: el error 11026 el dACL pedido no se encuentra](#)

La autenticación de RADIUS falla con este mensaje de error: `11026 el dACL pedido no se encuentra.`

[Solución](#)

Se rechaza la petición porque la versión del ACL descargable pedido en el pedido de acceso RADIUS no se encuentra. La petición para ACL descargable ocurrido de largo después del pedido de acceso original. Debido a esto, la versión del ACL descargable estaba no más disponible.

Encuentre la razón de este retardo en la petición para ACL descargable del cliente RADIUS.

Problema: el error 11025 el pedido el dACL pedido está faltando un atributo del Cisco-av-pair con el valor aaa: event=acl-download. Se rechaza la petición

La autenticación de RADIUS falla con este mensaje de error: 11025 el pedido el dACL pedido está faltando un atributo del Cisco-av-pair con el valor aaa: event=acl-download. Se rechaza la petición.

Solución

Cada pedido de acceso para ACL descargable debe tener un atributo del Cisco-av-pair con el valor aaa: event=acl-download. En este caso, ese atributo está faltando la petición y el ACS falló la petición. Marque si el dispositivo de red o el cliente AAA tiene cualesquiera problemas de compatibilidad sabidos RADIUS.

Problema: el error 11023 el dACL pedido no se encuentra. Esto es un nombre desconocido del dACL

La autenticación de RADIUS falla con este mensaje de error: 11023 el dACL pedido no se encuentra. Esto es un nombre desconocido del dACL.

Solución

Marque la configuración de ACS para verificar que ACL descargable especificado en el perfil de la autorización existe en la lista de ACL transferibles. Esto es un misconfiguration del lado ACS.

Problema: Autenticación de administrador fallada con el error interno del error 10001. Versión de la configuración incorrecta

La autenticación de administrador falla con este error: Error interno 10001. Versión de la configuración incorrecta.

Solución

Este error se puede causar por una base de datos ACS corrupta, o por un problema en los datos de configuración subyacentes. Entre en contacto el [TAC de Cisco](#) ([clientes registrados solamente](#)) para más información.

Problema: Autenticación de administrador fallada con el error interno del error 10002: Error cargar el servicio apropiado

La autenticación de administrador falla con este error: Error interno 10002: Error cargar el servicio apropiado.

Solución

El ACS 5.x no puede cargar el Servicio de configuración AAC. Esto se puede causar por una base de datos ACS corrupta, o por un problema en los datos de configuración subyacentes. Puede también ocurrir cuando agotan a los recursos del sistema. Entre en contacto el [TAC de Cisco \(clientes registrados solamente\)](#) para más información.

Problema: Autenticación de administrador fallada con el error interno del error 10003: La autenticación de administrador recibió el nombre en blanco del administrador

La autenticación de administrador falla con este error: Error interno 10003: La autenticación de administrador recibió el nombre en blanco del administrador.

Solución

Al acceder el GUI del ACS 5.x, el ACS recibe un Nombre de usuario en blanco. Marque la validez del Nombre de usuario transmitido al ACS. Si es válido, entre en contacto el [TAC de Cisco \(clientes registrados solamente\)](#) para más información.

Problema: Razón del error: El error relacionado de 24428 conexiones ha ocurrido en LRPC, el LDAP o el KERBEROS

Este mensaje de error se recibe en el ACS:

Razón del error: El error relacionado de 24428 conexiones ha ocurrido en LRPC, el LDAP o el KERBEROS que este problema de conexión RPC puede ser porque el stub recibió los datos incorrectos

Solución

Para resolver este problema, actualice el ACS a la versión 5.2.

Problema: La autenticación auth-proxy TACACS+ no está trabajando en un router que ejecuta IOS 15.x del servidor ACS 5.x

La autenticación auth-proxy TACACS+ no está trabajando en un router que funcione con el Cisco IOS Software Release 15.x de un servidor ACS 5.x.

Solución

El Auténtico-proxy TACACS+ se soporta solamente después de que actualización de la corrección 5. ACS 5.3 su ACS 5.x, o el uso RADIUS para el Auténtico-proxy.

Problema: Conseguir el error del almacén de mensaje de error (acs-xxx, TacacsAccounting) de ACS 5.x

Solución

El informe de las estadísticas ACS 5.1 TACACS falta algunos atributos tales como nombre de usuario, nivel de privilegio, y Petición-tipo cuando recibe un paquete malformado de las estadísticas del cliente. En algunos casos, esto lleva a la generación "de alarma del error del almacén (acs-xxx, TacacsAccounting)" en la visión. Para resolver esto, verifique el siguiente:

- El paquete que considera enviado por el cliente tiene un argumento malformado TACACS (por ejemplo, una mal de largo y valor del argumento un de los enviado por el cliente AAA).
- Asegúrese de que el cliente envíe un paquete válido de las estadísticas con la longitud adecuada y el valor para los argumentos.

Refiera al Id. de bug Cisco [CSCte88357](#) ([clientes registrados solamente](#)) para más información.

Problema: La autenticación de usuario fallada con el error "11036 el atributo de RADIUS del Mensaje-authenticator es inválida."

Solución

Verifique lo siguiente:

- Marque si los secretos compartidos en el cliente AAA y el servidor ACS hacen juego.
- Asegúrese de que el cliente AAA y el dispositivo de red no tengan ningunos problemas de hardware o problema con la compatibilidad RADIUS.
- Asegúrese de que la red que conecta el dispositivo con el ACS no tenga ningún problema de hardware.

Problema: Las estadísticas RADIUS fallaron con la petición caída "11037 de las estadísticas del error recibida vía el puerto sin apoyo."

Solución

La petición que consideraba fue caída porque fue recibida vía un número del puerto sin apoyo UDP. Verifique lo siguiente:

- Asegúrese de que la configuración de número del puerto de contabilidad en el cliente AAA y en la coincidencia del servidor ACS.
- Asegúrese de que el cliente AAA no tenga ningunos problemas de hardware o problema con la compatibilidad RADIUS.

Problema: Las estadísticas RADIUS falladas con la encabezado

de la Estadística-petición del error "11038 RADIUS contienen el campo inválido del authenticator."

El ACS no puede validar el campo del authenticator en la encabezado del paquete de la Estadística-petición RADIUS. El campo del authenticator no se debe confundir con el atributo de RADIUS del Mensaje-authenticator. Asegúrese de que el secreto compartido RADIUS configurado en las coincidencias del cliente AAA que configuraron para el dispositivo de red seleccionado en el servidor ACS. También, asegúrese de que el cliente AAA no tenga ningunos problemas de hardware o problema con la compatibilidad RADIUS.

Error: "24493 ACS tiene problemas que comunican con el Active Directory usando sus credenciales de la máquina."

Solución

Marque el ACS para la Conectividad AD, y asegúrese de que la cuenta de equipo ACS está todavía presente en el AD.

Problema: "Al crear los nombres del perfil del shell con los caracteres especiales tenga gusto "del ê", ACS puede causar un crash."

Solución

Este comportamiento se ha identificado y abrió una sesión el Id. de bug Cisco [CSCts17763](#) ([clientes registrados solamente](#)). Usted necesita actualizar 5.3.40 a la corrección 1 o 5.2.26 la corrección 7.

Problema: Conseguir el "error sintáctico en la línea 2: no bien formado (token inválido)" mientras que ejecuta "la demostración ejecútese" en el ACS 5.x CLI.

Solución

Asegúrese que la comunidad SNMP configurada en el ACS tiene caracteres válidos. Solamente los caracteres alfanuméricos (las cartas y los números solamente) se permiten ser utilizados en el nombre de la comunidad.

Problema: La división ACS 5.x /opt se llena muy rápidamente

Solución

El ACS 5.x se ejecuta fuera del espacio en disco debido al espacio insuficiente en la división de /opt. Esto ocurre debido al número alto de datos de registro que inundan la opinión ACS. Como

solución alternativa, usted necesita substituir la base de datos de la visión a menudo. Porque la opinión ACS no puede hacer frente a los gigabytes de datos cada día, usted necesita ordenar los datos de registro. Cuando usted necesita todos los registros, utilice a un servidor Syslog externo en vez de la opinión ACS. Cuando usted necesita utilizar solamente a una parte de los datos de registro, utilice la *administración del sistema > la configuración > las categorías de la configuración > del registro del registro > global* para enviar solamente los registros requeridos al registro-colector de la opinión ACS.

[Problema: Preguntar el dominio deseado](#)

¿Puede el ACS 5.x preguntar los controladores de dominio deseados (DCS) al unirse a un dominio de Active Directory?

[Solución](#)

No. Actualmente, el ACS pregunta el DNS con el dominio para conseguir una lista de todo el DCS en el dominio. Entonces, intenta comunicar con todos. Si la conexión incluso a un DC falla, después la conexión ACS al dominio se declara según lo fallado.

[Problema: Padre y Dominios hijo al mismo tiempo](#)

¿Hay una manera de configurar ACS 5.x en el padre y los Dominios hijo al mismo tiempo?

[Solución](#)

No. Actualmente, el ACS 5.x puede solamente ser un dominio de parte de una. Sin embargo, el ACS 5.x puede autenticar los usuarios/las máquinas de los dominios confiables múltiples.

[Problema: Registro a la base de datos remota](#)

¿Puedo registrar los datos de la opinión ACS 5.x a una base de datos remota?

[Solución](#)

Sí, el ACS 5.x permite que usted registre los datos de la opinión ACS al Microsoft SQL servers y a los servidores SQL del Oracle.

[Problema: Soporte de VMware](#)

[Solución](#)

El ACS 5.x se puede instalar en una máquina virtual. La última versión, ACS 5.3, se puede instalar en estas versiones de VMware:

- VMware ESX 3.5
- VMware ESX 4.0
- VMware ESX i4.1

- VMware ESX 5.0

Problema: Requisitos de espacio de disco

¿Cuáles son los requisitos de espacio de disco para la Versión de evaluación ACS 5.x?

Solución

Un mínimo de 60 GB de espacio en disco se requiere para la Versión de evaluación. 500 GB se requieren para la instalación de la producción.

Problema: "24401 no podía establecer la conexión con el agente del Active Directory ACS."

Solución

Para resolver este error, verifique el siguiente:

- Marque si la máquina ACS se une a al dominio del Active Directory.
- Marque el estatus de la Conectividad entre la máquina ACS y el servidor Active Directory.
- Marque si el agente del Active Directory ACS se está ejecutando.

Refiera al Id. de bug Cisco [CSCtx71254](#) ([clientes registrados solamente](#)) para más información.

Problema: El proceso del "Runtime" muestra el estado fallado "ejecución"

Al poner al día Cisco ACS con una corrección, el proceso del Runtime consigue pegado en la "ejecución fallada" se registra el estado y este mensaje:

```
"local0 yerran yerran ERROR del logforward 83 2012-06-12T12:11:08+0200 192.168.150.74 ACS ACS: /opt/CSCOacs/runtime/bin/run-logforward.sh: línea 18: Incidente de la segmentación 7097 (base vaciada). /$daemon - b - f $logfile"
```

Solución

Esto puede ser un problema con la corrección MD5 de la corrección más reciente. Verifique la suma de comprobación MD5 de la corrección más reciente aplicada a Cisco ACS. Descargue eso otra vez, después aplíquelo correctamente.

Problema: Autenticación ACS fallada cuando el UCS fuerza la reautenticación

El servidor UCS se configura para autenticar a un cliente de las Javas de Cisco ACS. El proceso de autenticación implica el uso del servidor Token RSA. Los primeros pasos de la autenticación. Sin embargo, cuando el UCS restaura y fuerza al cliente de las Javas a reautenticar, falla porque el RSA no permite reutilizar ningún token. Por lo tanto, la autenticación falla.

Solución

Esto es una limitación del perspective del servidor UCS, pero no de Cisco ACS. El servidor UCS sigue una autenticación bifactorial que sea una característica no admitida para Cisco ACS cuando está utilizada con los tokens RSA. Actualmente, no se soporta. Como solución alternativa, le aconsejan utilizar a cualquier servidor de bases de datos, tal como AD o LDAP, con excepción del servidor Token RSA.

Problema: La operación del Active Directory "24444 ha fallado debido a un error no especificado en el ACS"

Solución

Un error unmapped ha ocurrido en una operación relacionada AD. Refiera a la [integración ACS 5.x con el ejemplo de configuración de Microsoft AD](#) y configure la integración AD con el ACS correctamente. Si todo se configura correctamente según el documento, después TAC de Cisco del contacto para el troubleshooting adicional.

Problema: Incapaz de autenticar a los usuarios ACS 5.1 con el servidor del r2 AD 2008

Solución

Esto ocurre debido a los problemas de incompatibilidad. La integración del r2 AD 2008 se soporta de la versión ACS 5.2 solamente. Actualice su ACS a 5.2 o más adelante. Refiera al Id. de bug Cisco [CSCtg12399](#) ([clientes registrados solamente](#)) para más información.

Error: Tema 22056 no encontrado en los almacenes aplicables de la identidad.

Cuando los usuarios de VPN SSL están intentando conseguir autenticados de un dispositivo RSA, este mensaje de error se recibe del servidor ACS de Cisco:

Razón del error: Tema 22056 no encontrado en los almacenes aplicables de la identidad.

Solución

Marque si el usuario está presente en la base de datos donde el ACS se señala para buscar. En caso el almacén de la identidad RSA y RADIUS, se asegura de que la opción del **rechazo de la invitación** esté seleccionada como la **autenticación falló**. Esto está bajo ficha Avanzadas de la configuración del almacén de la identidad.

Problema: ipt_connlimit: Oops: ¿Estado inválido ct?

El `ipt_connlimit: Oops: ¿Estado inválido ct?` el mensaje de error aparece en la consola cuando el ACS 5.x se ejecuta en VMware.

Solución

Esto es un mensaje superfluo. Refiera al Id. de bug Cisco [CSCth25712](#) ([clientes registrados solamente](#)) para más información.

Problema: Los AC 5.x/ISE no ven el atributo llamar-estación-identificación del radio en un pedido de RADIUS del Cisco IOS Software Release 15.x NAS

Los AC 5.x/ISE no ven el atributo llamar-estación-identificación del radio en un pedido de RADIUS del Cisco IOS Software Release 15.x NAS.

Solución

Utilice el [atributo 31 del radio-servidor envían el](#) comando del NAS-puerto-[detalle](#) en el Cisco IOS Software Release 15.x para habilitar el envío del atributo.

Problema: Las cuentas de usuario consiguen bloqueadas en el primer caso de las credenciales incorrectas incluso si están configuradas para 3 tentativas

Cuando el ACS 5.3 se integra con el Active Directory en un nivel funcional del r2 de Windows 2008, las cuentas de usuario que se fijan con los parámetros del cierre (3 tentativas incorrectas) lockouted prematuramente después de que el usuario ingrese las credenciales incorrectas apenas una vez.

Solución

Refiera al Id. de bug Cisco [CSCtz03211](#) ([clientes registrados solamente](#)) para más información.

Problema: Unbale para salvar la salvaguardia del ACS

Durante una tentativa de salvar un respaldo del ACS, la causa: Detalles no configurados del backup de incremento: El backup de incremento no se configura. Configurar el backup de incremento es necesario hacer la purgación de la base de datos acertada. Esto ayudará a evitar los problemas del espacio en disco. El tamaño de la base de datos de la visión es 0.08GB y lo clasifica ocupa en el disco duro es la advertencia 0.08GB aparece.

Solución

Usted no puede ejecutar en paralelo un backup de incremento, salvaguardia completa, y los datos purgan. Si ninguno de estos trabajos se están ejecutando, usted debe esperar un período de 90 minutos antes de que usted puede comenzar el trabajo siguiente.

Información Relacionada

- [Página de soporte del Cisco Secure Access Control System](#)
- [Guías del usuario final del Cisco Secure Access Control System](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)