Contenido

Introducción

Este documento proporciona respuestas a las preguntas más frecuentes (FAQ) relacionadas con Cisco Secure Access Control System (ACS) 5.x y posteriores.

Asuntos relacionados de la autenticación

Q. ¿Pueden algunos usuarios/grupos de la base de datos interna ACS 5.x ser excluidos de la directiva de la contraseña del usuario (administración del sistema > Users > las configuraciones de la autenticación)?

A. Por abandono, cada usuario de la base de datos interna debe cumplir con la directiva de la contraseña del usuario. Actualmente, ningunos usuarios/grupos de la base de datos interna ACS 5.x pueden ser excluidos.

Q. ¿Pueden algunos administradores GUI de ACS 5.x ser excluidos de la política de contraseña del usuario administrador (administración del sistema > administradores > configuraciones > autenticación)?

A. Por abandono, cada usuario administrador GUI debe cumplir con la política de contraseña del usuario administrador. Actualmente, ningún usuario administrador de ACS 5.x puede ser excluido.

Q. ¿El ACS 5.x proporciona el soporte para las herramientas de VMware?

A. No. Actualmente, las herramientas de VMware no se soportan con el ACS versión 5.x. Refiera al Id. de bug Cisco CSCtg50048 (clientes registrados solamente) para más información.

Q. ¿Cuáles son los protocolos de autenticación EAP soportados para ACS 5.x cuando el LDAP se configura como el almacén de la identidad?

A. Cuando el LDAP se utiliza como el almacén de la identidad, el ACS 5.2 soporta los protocolos PEAP-GTC, EAP-FAST-GTC, y del EAP-TLS solamente. No soporta el MSCHAPv2 del EAP-FAST, el EAP MSCHAPv2 PEAP, y el EAP-MD5. Para más información, refiera a la compatibilidad del protocolo de autenticación y de la base de datos de usuarios.

Q. ¿Por qué la autenticación para el WLC con el radio del uso en el ACS falló, y por qué el ACS no mostró ninguna intentos fallidos?

A. Un problema existe con la **Interoperabilidad ACS 5.0 y del WLC** antes de que la corrección 8 de la descarga de la corrección 4., y aplica la corrección en el CLI. No utilice el TFTP para reparar este problema.

Q. ¿Por qué yo son incapaz de restablecer tar.gz los archivos que fueron sostenidos con el comando del respaldo- en ACS 5.2?

A. Usted no puede restablecer los archivos del registro que se sostienen con el comando del respaldo-**registro**. Usted puede restablecer solamente esos archivos sostenidos para la configuración de ACS y el ADE-OS. Refiera al **respaldo** y a los comandos de los respaldo-**registros** en el guía de referencia CLI para el Cisco Secure Access Control System 5.1 para más información.

Q. ¿Puedo limitar el número de tentativas fracasadas de la contraseña en ACS 5.2?

A. No. Esta característica no está disponible en ACS 5.2, sino que se espera que sea integrado en ACS 5.3. Refiera a la sección no soportada de las características de los Release Note para el Cisco Secure Access Control System 5.2 para más información.

Q. No puedo utilizar la opción para cambiar la contraseña en el login siguiente para los usuarios internos en ACS 5.0. ¿Cómo resuelvo este problema?

A. La opción para cambiar la contraseña en el login siguiente no se soporta en ACS 5.0. El soporte para esta característica está disponible en las versiones ACS 5.1 y posterior.

Q. ¿Qué esta alarma en el ACS significa?

A. Este error significa que cuando la opinión ACS alcanza un límite de 250,000 sesiones, lanza una alarma para borrar 20,000 sesiones. La base de datos de la opinión ACS salva todas las sesiones anteriores de la autenticación y cuando alcanza 250,000, da una alarma para borrar el caché y para borrar 20,000 sesiones.

Q. Cómo lo hago resuelva este mensaje de error: `Autenticación fallada: ¿La autenticación de usuario 24407 contra el Active Directory falló puesto que requieren al usuario cambiar su contraseña`?

A. Este mensaje de error aparece cuando hay un problema con la administración de contraseñas durante Autenticación SDI. Se utiliza el ACS 5.x mientras que una representación de RADIUS y los usuarios se deben autenticar por un servidor RSA. La representación de RADIUS al RSA trabajará solamente sin la administración de contraseñas. La razón es que el valor OTP debe ser recuperable por el proxy del servidor de RADIUS para el valor de contraseña al servidor RSA. Cuando habilitan a la administración de contraseñas en el grupo de túnel, el pedido de RADIUS se envía con los atributos MS-CHAPv2. El RSA no soporta el MS-0CHAPv2; soporta solamente el PAP.

Para resolver este problema, administración de contraseñas de la neutralización. Para más información, refiera al Id. de bug Cisco CSCsx47423 (clientes registrados solamente).

Q. ¿Es posible restringir ACS admin para manejar solamente ciertos dispositivos dentro de ACS 5.1?

A. No, no es posible restringir ACS admin para manejar solamente ciertos dispositivos dentro de

ACS 5.1.

Q. ¿El ACS soporta QoS en la autenticación para poder dar prioridad el RADIUS sobre el TACACS?

A. No, ACS no soporta QoS en la autenticación. El ACS no dará prioridad a las peticiones de la autenticación de RADIUS sobre las peticiones TACACS o TACACS sobre el RADIUS.

Q. ¿Pueden el proxy TACACS ACS 5.x y las autenticaciones de RADIUS a otro TACACS o servidores de RADIUS?

A. Sí, todas las versiones ACS 5.x pueden el proxy las autenticaciones de RADIUS a otros servidores de RADIUS. El ACS 5.3 y posterior puede proxy las autenticaciones de TACACS a otros servidores TACACS.

Q. ¿Puede el ACS 5.x marcar los atributos del dial-in de un usuario de Active Directory para conceder el acceso?

A. Sí, en ACS 5.3 y posterior usted puede permitir, negar, y controlar el acceso de los permisos de dial in de un usuario. Los permisos se marcan durante las autenticaciones o las interrogaciones del Active Directory. Se fija en el diccionario dedicado Active Directory.

Q. ¿El ACS 5.x soporta la GRIETA o la autenticación de MSCHAP teclea para el TACACS+?

A. Sí, soportan la GRIETA TACACS+ y a los tipos de la autenticación de MSCHAP en los ACS versión 5.3 y posterior.

Q. ¿Puedo fijar el tipo de contraseña de un usuario interno ACS a base de datos externa?

A. Sí, en ACS 5.3 y posterior usted puede fijar el tipo de contraseña de un usuario interno ACS. Esta característica estaba disponible en ACS 4.x.

Q. ¿Puede yo pasó/fall una autenticación basada en el tiempo en el cual crearon al usuario en el almacén interno de la identidad ACS?

A. Sí, en ACS 5.3 y posterior usted puede utilizar el **número de horas puesto que** atributo de la **creación del usuario** para crear sus directivas. Este atributo contiene el número de horas puesto que crearon al usuario en el almacén interno de la identidad a la época del pedido de autenticación actual.

Q. ¿Puedo utilizar a los comodines para agregar una nueva entrada de host en la base de datos interna ACS?

A. Sí, el ACS 5.3 y posterior permite que usted utilice a los comodines cuando usted agrega los nuevos host en el almacén interno de la identidad. También permite que usted ingrese a los comodines (después de que usted ingresa a los primeros tres octetos) para especificar todos los

dispositivos del fabricante identificado.

Q. ¿Puedo configurar a los pools de la dirección IP en el ACS 5.x y asignarlos del ACS?

A. No, no es actualmente posible crear a los pools de la dirección IP en el ACS 5.x.

Q. ¿Puedo ver la dirección IP del cliente AAA adonde la petición vino en el informe de la AUTENTICACIÓN FALLIDA?

A. No, no es posible ver la dirección IP del cliente AAA de donde vino la petición adentro.

Q. ¿Cuál es recuperación del mensaje del View log en ACS 5.3?

A. El ACS 5.3 proporciona una nueva función para recuperar cualquier registro se falte que cuando la visión está abajo. El ACS recoge estos registros faltados y los salva en su base de datos. Usando esta característica, usted puede extraer los registros faltados de la base de datos ACS a la base de datos de la visión después de que la visión sea salvaguardia. Para utilizar esta característica, usted debe fijar la configuración de la recuperación del mensaje del registro a **encendido**. Para más detalles en configurar la recuperación del mensaje del View log, refiera a la supervisión y señale las operaciones del sistema del Visualizador.

Q. ¿Puedo comprimir la base de datos ACS 5.x publicando el comando de la base de datos- motor de solución CLI? Esta característica estaba disponible en ACS 4.x.

A. Sí, en ACS 5.3 y posterior, el comando de la base de datos-**compresa** reduce el tamaño de la base de datos ACS con una opción para borrar a los administradores de la transacción table.ACS ACS puede publicar este comando para reducir el tamaño de la base de datos. Esto ayuda a reducir el tamaño de la base de datos y la época llevados para los respaldos y la sincronización completa que es necesaria para el mantenimiento.

Q. ¿Puedo buscar una entrada del cliente AAA basada en su dirección IP?

A. Sí, el ACS 5.3 y posterior permite que usted busque un dispositivo de red usando su dirección IP. Usted puede también utilizar los comodines y el rango para buscar un conjunto específico de los dispositivos de red.

Q. ¿Puedo crear una condición basada en el tiempo en el cual crearon al usuario en el almacén interno de la identidad ACS?

A. Sí, en ACS 5.3 y posterior usted puede utilizar el **número de horas puesto que el** atributo de la **creación del usuario** que le permite para configurar las condiciones de la regla de la directiva, sobre la base del tiempo en el cual crearon al usuario en el almacén interno de la identidad ACS. Por ejemplo: SI **group=HelpDesk&NumberofHoursSinceUserCreation>48** entonces rechazan. Este atributo contiene el número de horas puesto que crearon al usuario en el almacén interno de la identidad a la época del pedido de autenticación actual.

Q. ¿Puede el incorporar I que el almacén de la identidad el usuario fue autenticado en la autorización seccionar de una política de servicio?

A. Sí, en ACS 5.3 y posterior usted puede utilizar el atributo del **almacén de la identidad de la autenticación**, que le permite para configurar las condiciones de la regla de la directiva basadas en el almacén de la identidad de la autenticación. Por ejemplo: SI **AuthenticationIdentityStore=LDAP_NY** entonces rechaza. Este atributo contiene el nombre del almacén de la identidad usado y se pone al día con el nombre relevante del almacén de la identidad después de la autenticación satisfactoria.

Q. ¿Cuándo el ACS va al almacén siguiente de la identidad definido en la secuencia del almacén de la identidad?

A. El ACS va al almacén siguiente de la identidad definido en la secuencia del almacén de la identidad en estos escenarios:

- No encuentran a un usuario en el primer almacén de la identidad
- Un almacén de la identidad no está disponible en la secuencia

Q. ¿Cuál es la directiva de la incapacidad de la cuenta en ACS 5.3?

A. La directiva de la incapacidad de la cuenta permite que usted inhabilite a los usuarios del almacén interno de la identidad cuando la fecha configurada es más allá de la fecha permitida, el número configurado de días es más allá de los días permitidos, o el número de intentos de inicio de sesión fracasados consecutivos excede el umbral. El valor predeterminado para la fecha se excede está a 30 días a partir de la Fecha actual. El valor predeterminado por los días no debe estar a más de 60 días a partir del día actual. El valor predeterminado para los intentos fallidos es 5.

Q. ¿Puedo cambiar la contraseña de un usuario de la base de datos interna del ACS sobre el telnet?

A. Sí, a le se permite cambiar la contraseña de un usuario de la base de datos interna que usa el TACACS+ sobre el telnet. Usted necesita seleccionar los **cambios de contraseña de TELNET del permiso** bajo **control de cambios de la contraseña** en ACS 5.x.

Q. ¿El caso primario ACS 5.x pone al día automáticamente los casos de reserva periódicamente, o debe él suceder solamente cuando una configuración ha cambiado?

A. El ACS 5.x replicará inmediatamente al ACS secundario siempre que usted realice los cambios en el ACS primario. Además, si usted entonces no realiza ninguna cambios al ACS primario, hará una replicación de la fuerza cada 15 minutos. En este momento, no hay una opción para controlar el temporizador de modo que el ACS pueda replicar la información después de un tiempo específico.

Q. ¿Puede yo vio/exportación un informe sobre ACS 5.x de todos los usuarios que se abren una sesión y se autentican actualmente del ACS en diversos clientes NAS?

A. Sí, es posible. Hay dos informes separados para el RADIUS y el TACACS+. Usted puede encontrarlos bajo la **supervisión y los informes** > los **informes** > el **catálogo** > el **directorio de la**

sesión > las **sesiones activas RADIUS** y **sesiones activas TACACS**. Ambos informes se basan en la información de la cuenta de los clientes NAS puesto que permite que usted siga cuando el usuario conecta y termina la sesión. El historial de la sesión incluso permite que usted consiga la información desde el principio y que pare los mensajes durante un día específico.

Información Relacionada

- Página de soporte del Cisco Secure Access Control System
- Soporte Técnico y Documentación - Cisco Systems