Preguntas frecuentes sobre Secure Access Control System 5.x y posteriores

Contenido

[Introducción](#)
[Problemas relacionados con la autenticación](#)
[Información Relacionada](#)

Introducción

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

Problemas relacionados con la autenticación

P. ¿Pueden excluirse algunos usuarios/grupos de la base de datos interna ACS 5.x de la política de contraseñas de usuario (Administración del sistema > Usuarios > Configuración de autenticación)?

A. De forma predeterminada, cada usuario de la base de datos interna debe cumplir con la política de contraseñas de usuario. Actualmente, no se puede excluir a ningún usuario/grupo de la base de datos interna ACS 5.x.

P. ¿Pueden excluirse algunos administradores de GUI de ACS 5.x de la política administrativa de contraseñas de usuario (Administración del sistema > Administradores > Configuración > Autenticación)?

A. De forma predeterminada, cada usuario administrativo de GUI debe cumplir con la política de contraseña administrativa de usuario. Actualmente, no se puede excluir ningún usuario administrativo de ACS 5.x.

P. ¿ACS 5.x proporciona soporte para las herramientas VMWare?

A. No. Actualmente, las herramientas VMWare no son compatibles con ACS versión 5.x. Consulte Cisco bug ID CSCtg50048 (sólo clientes registrados) para obtener más información.

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

A. Cuando LDAP se utiliza como almacén de identidad, ACS 5.2 soporta solamente los protocolos PEAP-GTC, EAP-FAST-GTC y EAP-TLS. No admite EAP-FAST MSCHAPv2, PEAP EAP-

MSCHAPv2 y EAP-MD5. Para obtener más información, refiérase a Authentication Protocol y User Database Compatibility.

P. ¿Por qué falló la autenticación para el WLC con el radio de uso en el ACS, y por qué ACS no mostró ningún intento fallido?

A. Existe un problema con la **interoperabilidad ACS 5.0 y WLC** antes del parche 4. Descargue el parche 8 y aplique el parche en la CLI. No use TFTP para solucionar este problema.

P. ¿Por qué no puedo restaurar los archivos tar.gz a los que se hizo una copia de seguridad con el comando backup-log en ACS 5.2?

A. No puede restaurar los archivos de registro a los que se hace una copia de seguridad con el comando **backup-log**. Sólo puede restaurar los archivos de los que se ha realizado una copia de seguridad para la configuración ACS y ADE-OS. Refiérase a los comandos **backup** y **backup-logs en la** Guía de Referencia de CLI para Cisco Secure Access Control System 5.1 para obtener más información.

P. ¿Puedo limitar el número de intentos fallidos de contraseña en ACS 5.2?

A. No. Esta función no está disponible en ACS 5.2, pero se espera que esté integrada en ACS 5.3. Consulte la sección Características no Soportadas de Release Notes para Cisco Secure Access Control System 5.2 para obtener más información.

P. No puedo utilizar la opción para cambiar la contraseña en el siguiente inicio de sesión para los usuarios internos en ACS 5.0. ¿Cómo resuelvo este problema?

A. La opción para cambiar la contraseña en el siguiente inicio de sesión no se soporta en ACS 5.0. El soporte para esta función está disponible en ACS 5.1 y versiones posteriores.

P. ¿Qué significa esta alarma en ACS?

```
Cisco Secure ACS - Alarm Notification
Severity: Warning
Alarm Name delete 20000 sessions
Cause/Trigger active sessions are over limit
Alarm Details session is over 250000
```

A. Este error significa que cuando la Vista ACS alcanza un límite de 250.000 sesiones, produce una alarma para eliminar 20.000 sesiones. La base de datos de vista ACS almacena todas las sesiones de autenticación anteriores y cuando alcanza 250,000, da una alarma para borrar la memoria caché y eliminar 20,000 sesiones.

P. Cómo resuelvo este mensaje de error: `Error de autenticación: 24407 Error de autenticación de usuario en Active Directory porque se requiere que el usuario cambie su contraseña`?

A. Este mensaje de error aparece cuando hay un problema con la administración de contraseñas durante la autenticación SDI. ACS 5.x se utiliza como proxy Radius y los usuarios deben ser autenticados por un servidor RSA. El proxy Radius a RSA funcionará solamente sin administración de contraseñas. La razón es que el valor OTP debe ser recuperable por el servidor

Radius para proxy el valor de la contraseña al servidor RSA. Cuando se habilita la administración de contraseñas en el grupo de túnel, la solicitud Radius se envía con atributos MS-CHAPv2. RSA no admite MS-0CHAPv2; solo admite PAP.

Para resolver este problema, inhabilite la administración de contraseñas. Para obtener más información, consulte el Id. de bug Cisco CSCsx47423 (sólo clientes registrados) .

P. ¿Es posible restringir el administrador ACS para administrar solamente ciertos dispositivos dentro de ACS 5.1?

A. No, no es posible restringir el administrador ACS para administrar solamente ciertos dispositivos dentro de ACS 5.1.

P. ¿ACS soporta QoS en la autenticación para que RADIUS pueda ser priorizado sobre TACACS?

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

P. ¿Pueden las autenticaciones RADIUS y TACACS del proxy ACS 5.x a otros servidores TACACS o RADIUS?

A. Sí, todas las versiones ACS 5.x pueden proxy las autenticaciones RADIUS a otros servidores RADIUS. ACS 5.3 y posteriores pueden proxy las autenticaciones TACACS a otros servidores TACACS.

P. ¿Puede ACS 5.x verificar los atributos de marcado de un usuario de Active Directory para conceder acceso?

A. Sí, en ACS 5.3 y posteriores puede permitir, denegar y controlar el acceso de los permisos de marcado de un usuario. Los permisos se comprueban durante las autenticaciones o consultas de Active Directory. Se establece en el diccionario dedicado de Active Directory.

P. ¿ACS 5.x soporta tipos de autenticación CHAP o MSCHAP para TACACS+?

A. Sí, los tipos de autenticación TACACS+ CHAP y MSCHAP se soportan en las versiones ACS 5.3 y posteriores.

P. ¿Puedo establecer el tipo de contraseña de un usuario interno ACS en cualquier base de datos externa?

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

P. ¿Puedo aprobar/fallar una autenticación basada en la hora en que el usuario fue creado en el almacén de identidad interno de ACS?

A. Sí, en ACS 5.3 y posterior puede utilizar el atributo **Número de horas desde la creación del**

usuario para crear sus políticas. Este atributo contiene el número de horas transcurridas desde que se creó el usuario en el almacén de identidades interno hasta la hora de la solicitud de autenticación actual.

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

A. Sí, ACS 5.3 y posteriores le permite utilizar comodines cuando agrega nuevos hosts a Internal Identity Store. También le permite introducir comodines (después de ingresar los primeros tres octetos) para especificar todos los dispositivos del fabricante identificado.

P. ¿Puedo configurar grupos de direcciones IP en ACS 5.x y asignarlos desde ACS?

A. No, actualmente no es posible crear conjuntos de direcciones IP en el ACS 5.x.

P. ¿Puedo ver la dirección IP del cliente AAA donde se produjo la solicitud en el informe de AUTENTICACIÓN FALLIDA?

A. No, no es posible ver la dirección IP del cliente AAA desde donde entró la solicitud.

P. ¿Qué es View Log Message Recovery en ACS 5.3?

A. ACS 5.3 proporciona una nueva función para recuperar los registros que se pierden cuando la vista está inactiva. ACS recopila estos registros perdidos y los almacena en su base de datos. Con esta función, puede recuperar los registros perdidos de la base de datos ACS en la base de datos de vistas después de que la vista esté de respaldo. Para utilizar esta función, debe establecer la Configuración de Recuperación de Mensajes de Registro en **On**. Para obtener más detalles sobre la configuración de View Log Message Recovery, refiérase a Monitoring & Report Viewer System Operations.

P. ¿Puedo comprimir la base de datos ACS 5.x ejecutando el comando database-compress desde la CLI de Solution Engine? Esta función estaba disponible en ACS 4.x.

A. Sí, en ACS 5.3 y posterior, el comando **database-compress** reduce el tamaño de la base de datos ACS con una opción para eliminar la tabla de transacciones ACS. Los administradores ACS pueden ejecutar este comando para reducir el tamaño de la base de datos. Esto ayuda a reducir el tamaño de la base de datos y el tiempo necesario para realizar copias de seguridad y realizar la sincronización completa necesaria para el mantenimiento.

P. ¿Puedo buscar una entrada de cliente AAA en función de su dirección IP?

A. Sí, ACS 5.3 y posteriores le permite buscar un dispositivo de red usando su dirección IP. También puede utilizar comodines y el rango para buscar un conjunto específico de dispositivos de red.

P. ¿Puedo crear una condición en función de la hora en la que se creó el usuario en ACS Internal Identity Store?

A. Sí, en ACS 5.3 y posterior puede utilizar el atributo **Número de Horas desde la Creación del Usuario** que permite configurar las condiciones de regla de política, en función de la hora en que el usuario fue creado en ACS Internal Identity Store. Por ejemplo: IF **group=HelpDesk&Number ofHoursSinceUserCreation>48**, rechace. Este atributo contiene el número de horas transcurridas desde que se creó el usuario en Internal Identity Store hasta la hora de la solicitud de autenticación actual.

P. ¿Puedo comprobar en qué almacén de identidad se autenticó el usuario en la sección Autorización de una política de servicio?

A. Sí, en ACS 5.3 y posterior puede utilizar el atributo **Authentication Identity Store**, que permite configurar las condiciones de regla de política basándose en el Almacén de Identidad de Autenticación. Por ejemplo: IF **AuthenticationIdentityStore=LDAP_NY** entonces rechaza. Este atributo contiene el nombre del almacén de identidades utilizado y se actualiza con el nombre del almacén de identidades correspondiente después de la autenticación correcta.

P. ¿Cuándo se dirige el ACS al siguiente almacén de identidad definido en la secuencia del almacén de identidad?

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

- No se ha encontrado ningún usuario en el primer almacén de identidades
- Un almacén de identidad no está disponible en la secuencia

P. ¿Cuál es la política de Discapacidad de Cuenta en ACS 5.3?

A. La Política de Inhabilitación de Cuenta le permite inhabilitar a los usuarios de Internal Identity Store cuando la fecha configurada supera la fecha permitida, el número configurado de días excede los días permitidos o el número de intentos consecutivos de inicio de sesión fallidos excede el umbral. El valor predeterminado para la fecha supera es de 30 días a partir de la fecha actual. El valor predeterminado para los días no debe ser superior a 60 días a partir del día actual. El valor predeterminado para los intentos fallidos es 5.

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

A. Sí, puede cambiar la contraseña de un usuario de base de datos interna mediante TACACS+ a través de telnet. Debe seleccionar **Enable TELNET Change Password** en **Password Change Control** en ACS 5.x.

P. ¿La instancia primaria ACS 5.x actualiza automáticamente las instancias de respaldo de forma periódica o sólo debería ocurrir cuando una configuración ha cambiado?

A. ACS 5.x se replicará inmediatamente en el ACS secundario cada vez que realice cambios en el ACS primario. Además, si no realiza ningún cambio en el ACS primario, entonces hará una replicación de fuerza cada 15 minutos. En este punto, no hay una opción para controlar el temporizador para que ACS pueda replicar la información después de un tiempo específico.

P. ¿Puedo ver/exportar un informe sobre ACS 5.x de todos los usuarios que actualmente están conectados y autenticados desde ACS en diferentes clientes NAS?

A. Sí, es posible. Hay dos informes independientes para RADIUS y TACACS+. Puede encontrarlos en Monitoring & Reports > Reports > Catalog > **Session Directory** > RADIUS Active Sessions y TACACS Active Sessions. Ambos informes se basan en la información de contabilidad de los clientes NAS, ya que le permite realizar un seguimiento cuando el usuario se conecta y cierra la sesión. El historial de sesiones incluso le permite obtener información desde el inicio y detener mensajes durante un día específico.

Información Relacionada

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