Solucionar problemas de errores de autenticación de ISE TACACS+ debido a sobrecarga del sistema

Contenido

Problema

Las autenticaciones de Cisco Identity Services Engine (ISE) Terminal Access Controller Access-Control System Plus (TACACS+) dejan de funcionar de forma intermitente y provocan que los inicios de sesión de los dispositivos de red vuelvan a depender de los usuarios locales en lugar de la autenticación TACACS+. Durante las interrupciones, los motivos de error de "solicitud TACACS+ se descartó debido a la sobrecarga del sistema" se muestran en los registros en directo. Los fallos de autenticación se producen sin que se realice ningún cambio de configuración en ISE para TACACS+ o en los dispositivos de red con respecto a la configuración de TACACS+.

Entorno

- parche 7 de Cisco Identity Services Engine (ISE) versión 3.3
- Implementación de ISE distribuido con PSN específicos para la administración de dispositivos
- Servicio de autenticación TACACS+ para acceso administrativo
- Configuración de destino de Syslog del protocolo de control de transmisión (TCP)

Resolución

La habilitación de los debugs de tiempo de ejecución AAA en el Policy Service Node (PSN) durante el problema y la revisión de port-server.log revela valores de ContextN extremadamente

altos que indican que se realiza una copia de seguridad del procesamiento en PSN:

```
ContextCounter,2026-05-05 12:17:08,442,DEBUG,0x7f42bead0700,ContextN incremented, number=113687,Context
```

AcsLoggerReactorThread y TCPSyslogReactorThread son los grupos de subprocesos que están elevados y que provocan la copia de seguridad:

```
EventHandler,2026-05-05 12:17:10,461,DEBUG,0x7f42bead0700,Passed event to the next thread pool name=Acs
EventHandler,2026-05-05 12:17:12,859,DEBUG,0x7f429b6d0700,Passed event to the next thread pool name=TCP
```

Las conexiones TACACS+ se descartan debido al límite de espacio alcanzado:

```
TCPListener,2026-05-05 12:17:08,804,DEBUG,0x7f429b4cf700,NIL-CONTEXT,Hit space limit. Dropping request!
```

Cualquier destino de Syslog TCP habilitado en Administration > System > Logging > Remote Logging Targets con la configuración "Buffer Messages When Server Down" habilitada en la configuración no debe ser inalcanzable durante períodos de tiempo extendidos debido al defecto de Cisco CSCwt35414. Si no se puede garantizar la disponibilidad, se debe instalar una versión fija de ISE o se debe anular la selección de la función "Buffer Messages When Server Down" en el destino de Syslog TCP para evitar este comportamiento.

Causa

La causa raíz se identificó como defecto de Cisco CSCwt35414. Este defecto hace que el procesamiento de autenticación en PSN se bloquee cada vez que el búfer configurado en el destino de Syslog TCP se llene. Los registros se escriben en el búfer cuando el destino de Syslog TCP no se puede alcanzar o no responde para enviarse una vez que responde de nuevo, pero si el destino no se puede alcanzar durante largos períodos de tiempo con mucho tráfico en el PSN, el búfer se llenará y el procesamiento de autenticación se verá afectado.

Contenido relacionado

- defecto de Cisco CSCwt35414
- Configuración de destinos de registro remoto

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).