

Solucionar falhas de autenticação do ISE TACACS+ devido à sobrecarga do sistema

Contents

Problema

As autenticações do Cisco Identity Services Engine (ISE) Terminal Access Controller Access-Control System Plus (TACACS+) param de funcionar intermitentemente e fazem com que os logons do dispositivo de rede retornem aos usuários locais em vez da autenticação TACACS+. Durante as interrupções, os motivos de falha da solicitação "TACACS+ foi descartado devido à sobrecarga do sistema" são exibidos nos registros em tempo real. As falhas de autenticação ocorrem sem que nenhuma alteração de configuração seja feita no ISE para TACACS+ ou nos dispositivos de rede com relação à configuração TACACS+.

Ambiente

- Cisco Identity Services Engine (ISE) versão 3.3 patch 7
- Implantação distribuída do ISE com PSNs específicas para administração de dispositivos
- Serviço de autenticação TACACS+ para acesso administrativo
- Configuração de destino do Syslog do Transmission Control Protocol (TCP)

Resolução

A habilitação de depurações AAA em tempo de execução no Policy Service Node (PSN) durante o problema e a revisão de prrt-server.log revelam valores ContextN extremamente altos, indicando que foi feito o backup do processamento no PSN:

AcsLoggerReatorThread e TCPSyslogReatorThread são os pools de threads elevados que causam o backup:

```
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
```

As conexões TACACS+ são descartadas devido ao limite de espaço atingido:

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

Qualquer destino de Syslog TCP habilitado em Administration > System > Logging > Remote Logging Targets com a configuração "Buffer Messages When Server Down" habilitada na configuração não deve ficar inacessível por longos períodos de tempo devido ao [defeito Cisco CSCwt35414](#). Se a acessibilidade não puder ser garantida, uma versão fixa do ISE deve ser instalada ou o recurso "Buffer Messages When Server Down" deve ser desmarcado no destino de Syslog TCP para evitar esse comportamento.

Causa

A causa raiz foi identificada como [defeito Cisco CSCwt35414](#). Esse defeito faz com que o processamento de autenticação no PSN seja bloqueado sempre que o buffer configurado no destino TCP Syslog ficar cheio. Os logs são gravados no buffer quando o destino TCP Syslog está inacessível ou não responde para ser enviado quando estiver respondendo novamente, mas se o destino estiver inacessível por longos períodos de tempo com tráfego pesado na PSN, o buffer será preenchido e o processamento de autenticação será afetado.

Conteúdo relacionado

- [Cisco defeito CSCwt35414](#)
- [Configurações de Destinos de Log Remoto](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.