

Problemen met ISE TACACS+-verificatie oplossen als gevolg van systeemoverbelasting

Inhoud

uitgeven

Cisco Identity Services Engine (ISE) Terminal Access Controller Access-Control System Plus (TACACS+)-verificaties werken niet meer met tussenpozen en zorgen ervoor dat aanmeldingen van netwerkapparaten terugvallen op lokale gebruikers in plaats van TACACS+-verificatie. Tijdens de uitval, mislukking redenen van "TACACS+ verzoek werd geschrapt als gevolg van het systeem overbelasting" weergegeven in de Live Logs. De verificatiefouten treden op zonder dat er configuratiewijzigingen worden aangebracht in ISE voor TACACS+ of op de netwerkapparaten met betrekking tot de TACACS+-configuratie.

milieu

- Patch 7 voor Cisco Identity Services Engine (ISE) versie 3.3
- Gedistribueerde ISE-implementatie met specifieke PSN's voor apparaatbeheer
- TACACS+-verificatieservice voor administratieve toegang
- Transmissiecontroleprotocol (TCP) Syslog-doelconfiguratie

resolutie

Het inschakelen van runtime-AAA-debug's op de Policy Service Node (PSN) tijdens het probleem en het bekijken van prrt-server.log onthult extreem hoge ContextN-waarden die aangeven dat er een back-up wordt gemaakt van de verwerking op de PSN:

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

De AcsLoggerReactorThread en TCPSyslogReactorThread zijn de threadpools die zijn verhoogd en de back-up veroorzaken:

```
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
```

De TACACS+-verbindingen zijn verbroken omdat de ruimtebeperking is bereikt:

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

Alle TCP Syslog-doelen die zijn ingeschakeld onder Beheer > Systeem > Logboekregistratie > Doelstellingen voor externe logboekregistratie met de instelling "Buffer Berichten wanneer server down" ingeschakeld in de configuratie, mogen gedurende langere perioden niet onbereikbaar zijn vanwege het [Cisco-defect CSCwt35414](#). Als bereikbaarheid niet kan worden gegarandeerd, moet een vaste versie van ISE worden geïnstalleerd of moet de functie "Buffer Berichten wanneer server down" worden uitgeschakeld op het TCP Syslog-doel om dit gedrag te voorkomen.

Oorzaak

De oorzaak werd geïdentificeerd als [Cisco defect CSCwt35414](#). Dit defect zorgt ervoor dat de verificatieverwerking op de PSN wordt geblokkeerd wanneer de geconfigureerde buffer op het TCP Syslog-doel vol raakt. Logs worden naar de buffer geschreven wanneer het TCP Syslog-doel onbereikbaar of niet-reagerend is om te worden verzonden zodra het opnieuw reageert, maar als het doel lange tijd onbereikbaar is met zwaar verkeer op de PSN, zal de buffer zich vullen en wordt de authenticatieverwerking beïnvloed.

Verwante inhoud

- [Cisco defect CSCwt35414](#)
- [Instellingen voor doelen voor extern vastleggen](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.