# Fout bij validatie van beveiligd toegangscertificaat met Splunk-clientlogbestanden uploaden

## Inhoud

## uitgeven

Windows-clients met de Splunk-client konden geen logboeken uploaden naar Splunk-cloud vanwege fouten in de certificaatvalidatie toen het verkeer werd gedecodeerd door Cisco Secure Access. Meer dan 5000 Windows-logboekbronnen konden geen gegevens naar de Splunk-cloud verzenden, wat gevolgen had voor de logboekopname. De specifieke fout die werd waargenomen in Splunk-clientlogboeken was:

```
02-27-2026 16:51:54.830 +0530 ERROR X509Verify [15668 TcpOutEloop] - Server X509 certificate failed val
```

Het verkeer naar de bestemming *.splunkcloud.com liep via de firewall, maar de certificaatvalidatie op toepassingsniveau mislukte. Webbrowsen naar sites waar SSL-decodering was ingeschakeld, bleef normaal werken.

## milieu

- Cisco Secure Access met SSL/TLS-decodering ingeschakeld
- Windows-clients waarop Splunk Universal Forwarder is geïnstalleerd
- Splunk cloud-bestemming: *.splunkcloud.com
- Meer dan 5000 Windows-logboekbronnen getroffen
- Splunk-client gebruikt zijn eigen certificaatarchief, niet het Microsoft-systeemcertificaatarchief

# resolutie

Het probleem werd opgelost door het implementeren van een decodering bypass beleid voor Splunk cloud verkeer in Cisco Secure Access.

Er werden verschillende stappen gezet.

## Stap 1: Identificeer het probleem

Tijdens een WebEx-sessie werd het gedrag bevestigd en gereproduceerd. Testen toonden aan dat wanneer Secure Access-decodering was uitgeschakeld voor een client of wanneer de SWG-service was uitgeschakeld op de client, Splunk-logboekuploads zijn gelukt. Dit bevestigde dat het SSL/TLS-decoderingsproces de oorzaak was van de fout in de certificaatvalidatie.

## Stap 2: Bestemmingslijst maken

Er is een bestemmingslijst gemaakt met de Splunk cloud FQDN's en IP-adressen om specifiek verkeer te targeten dat bestemd is voor Splunk cloud-diensten.

## Stap 3: Implementeer het beleid voor het omzeilen van decodering

Er is een Cisco Secure Access-beleid geïmplementeerd om SSL/TLS-decodering uit te schakelen voor verkeer dat overeenkomt met de Splunk-lijst met cloudbestemmingen. Dit bypass-beleid stelde Splunk-klanten in staat om directe gecodeerde verbindingen met Splunk cloud tot stand te brengen zonder certificaatonderschepping door Secure Access.

## Stap 4: Validatie

Na het implementeren van het beleid voor decodering en bypass, bevestigde validatie dat:

- Splunk-clients konden logboeken met succes uploaden
- Het totale aantal klanten dat rapporteert in Splunk cloud is aanzienlijk toegenomen
- Er werden geen verdere fouten in de certificaatvalidatie waargenomen

De ernst van het geval werd teruggebracht van 1 tot 3 en in de monitoringstatus geplaatst om aanhoudende succesvolle log-inname te observeren.

## Oorzaak

De hoofdoorzaak was dat de Splunk-client zijn eigen certificaatopslag gebruikt en het Cisco Secure Access Primary SubCA-certificaat niet vertrouwt dat werd gepresenteerd tijdens SSL / TLS-decodering. Toen Cisco Secure Access het SSL-verkeer naar Splunk cloud onderschepte en decodeerde, hercodeerde het het verkeer met behulp van zijn eigen certificaatautoriteit. Het Splunk-proces voor de validatie van clientcertificaten heeft dit certificaat afgewezen omdat het de certificaatketen niet kon terugsturen naar een vertrouwde rootcertificeringsinstantie in het eigen certificaatarchief.

De specifieke X.509-validatiefout "Kan geen certificaat van lokale uitgever ophalen" (foutcode 20) geeft aan dat het certificaatvalidatieproces de instantie van afgifte van het certificaat niet kon vinden in het vertrouwde certificaatarchief van de client, waardoor de verbinding mislukt.

## Verwante inhoud

- Cisco Technical Support en downloads

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.