Secure Access Certificate Validation Error with Splunk Client Log Uploads

Contents

Issue

Windows clients running the Splunk client were unable to upload logs to Splunk cloud due to certificate validation errors when traffic was decrypted by Cisco Secure Access. More than 5000 Windows log sources failed to send data to Splunk cloud, impacting log ingestion. The specific error observed in Splunk client logs was:

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

Traffic to the destination *.splunkcloud.com was flowing via the firewall, but the application-level certificate validation was failing. Web browsing to sites where SSL decryption was enabled continued to work normally.

Environment

- Cisco Secure Access with SSL/TLS decryption enabled
- Windows clients with Splunk Universal Forwarder installed
- Splunk cloud destination: *.splunkcloud.com
- More than 5000 Windows log sources affected
- Splunk client uses its own certificate store, not the Microsoft system certificate store

Resolution

The issue was resolved by implementing a decryption bypass policy for Splunk cloud traffic in Cisco Secure Access.

Several steps were taken.

Step 1: Identify the Problem

During a WebEx session, the behavior was confirmed and reproduced. Testing showed that when Secure Access decryption was disabled for a client or when the SWG service was disabled on the client, Splunk log uploads succeeded. This confirmed that the SSL/TLS decryption process was causing the certificate validation failure.

Step 2: Create Destination List

A destination list was created containing the Splunk cloud FQDNs and IP addresses to specifically target traffic destined for Splunk cloud services.

Step 3: Implement Decryption Bypass Policy

A Cisco Secure Access policy was implemented to disable SSL/TLS decryption for traffic matching the Splunk cloud destination list. This bypass policy allowed Splunk clients to establish direct encrypted connections to Splunk cloud without certificate interception by Secure Access.

Step 4: Validation

After implementing the decryption bypass policy, validation confirmed that:

- Splunk clients were able to upload logs successfully
- The overall number of reporting clients in Splunk cloud increased substantially
- No further certificate validation errors were observed

The case severity was reduced from 1 to 3 and placed into monitoring status to observe continued successful log ingestion.

Cause

The root cause was that the Splunk client uses its own certificate store and does not trust the Cisco Secure Access Primary SubCA certificate that was being presented during SSL/TLS decryption. When Cisco Secure Access intercepted and decrypted the SSL traffic to Splunk cloud, it re-encrypted the traffic using its own certificate authority. The Splunk client certificate validation process rejected this certificate because it could not verify the certificate chain back to a trusted root certificate authority in its own certificate store.

The specific X.509 validation error "unable to get local issuer certificate" (error code 20) indicates that the certificate validation process could not locate the issuing certificate authority in the client trusted certificate store, causing the connection to fail.

Related Content

- Cisco Technical Support & Downloads