Syslog in der ACI konfigurieren und Fehlerbehebung dafür durchführen

Einleitung

In diesem Dokument wird beschrieben, wie die Systemprotokollierung (Syslog) in der Cisco Application Centric Infrastructure (ACI) konfiguriert, überprüft und Fehler behoben werden. Es umfasst den kompletten Konfigurations-Workflow, die programmatische Verifizierung mithilfe des MO-Modells (Managed Object) des Application Policy Infrastructure Controllers (APIC) und einen strukturierten Workflow zur Fehlerbehebung für die APIC-Controller sowie die Leaf- und Spine-Switches.

Überblick

Das ACI-Syslog ist vollständig richtlinienbasiert. Im Gegensatz zur Standalone Cisco NX-OS® Software gibt es auf ACI-Leaf- oder Spine-Switches keine **logging server** CLI-Befehle. Die gesamte Syslog-Konfiguration erfolgt über APIC-Richtlinien, die der APIC automatisch an alle Fabric-Knoten weiterleitet.

Wichtige Komponenten

Das Syslog-Subsystem der ACI basiert auf den folgenden verwalteten Objekten:

- Syslog-Zielgruppe (syslogGroup) - Der Container der obersten Ebene für alle Syslog-Ziele. Sie steuert das Nachrichtenformat (im ACI- oder NX-OS-Stil) und die Zeitstempeloptionen. Er kann ein oder mehrere Remote-Ziele, ein lokales Dateiziel und ein Konsolenziel enthalten.
- Syslog-Profil (syslogProf) - Ein untergeordnetes Element der Zielgruppe, das den Verwaltungsstatus auf Gruppenebene und das Transportprotokoll (UDP, TCP oder SSL) steuert.
- Syslog-Remote-Ziel (syslogRemoteDest) - Ein untergeordnetes Element der Zielgruppe, das einen Remote-Syslog-Server darstellt. Steuert die Server-IP oder den Hostnamen, den Port, den Schweregradfilter, die Syslog-Funktion und die Management-Endpunktgruppe (EPG), die zum Erreichen des Servers verwendet wird.
- Syslog Local File (syslogFile) - Ein untergeordnetes Element der Zielgruppe, das das Schreiben von Syslog-Meldungen in die lokale Datei /var/log/external/messages auf jedem Fabric-Knoten steuert.
- Syslog-Quelle (syslogSrc) - Wird an eine Überwachungsrichtlinie angehängt. Steuert, welche Meldungsarten (Audit, Ereignisse, Fehler, Sitzung) und welcher Mindestschweregrad

gesendet werden, und stellt über eine syslogRsDestGroup Beziehung Links zur Zielgruppe bereit.

Syslog-Quellangriffspunkte

Die ACI verwendet vier Überwachungsrichtlinienbereiche, die steuern, welche Knoten und Objekte Syslog-Meldungen generieren:

- Gemeinsame Überwachungsrichtlinie (monCommonPol, uni/fabric/moncommon) - Fabric-weiter Geltungsbereich. Eine grundlegende Überwachungsrichtlinie, die für alle Fehler und Ereignisse gilt und automatisch für alle Knoten (Leaf- und Spine-Switches) und alle Controller (APICs) in der Fabric bereitgestellt wird. Umfasst alle Fabric-, Zugriffs- und Tenant-Hierarchien. Gefunden bei Fabric > Fabric-Richtlinien > Richtlinien > Überwachung > Gemeinsame Richtlinie.
- Fabric-Überwachungsrichtlinie (monInfraPol, uni/infra/moninfra-default) - Fabric-Umfang. Generiert Syslog für Fabric-Objekte: Fabric-Ports, Karten, Chassis-Komponenten und Lüftereinschübe. Gefunden bei Fabric > Fabric-Richtlinien > Richtlinien > Überwachung > Standard.
- Zugriffsüberwachungsrichtlinie (monFabricPol, uni/fabric/monfab-default) - Zugriffsbereich (Infrastruktur). Generiert Syslog für zugriffsgerichtete Komponenten: Access-Ports, Fabric Extender (FEX)-Geräte und VM-Controller-Ereignisse. Gefunden in Fabric > Zugriffsrichtlinien > Richtlinien > Überwachungsrichtlinien > Standard.
- Tenant-Überwachungsrichtlinie (monEPGPol, uni/tn-common/monepg-default) - Tenant-Bereich. Generiert Syslog für Objekte mit Tenant-Bereich: Endpunktgruppen (EPGs), Anwendungsprofile und Services. Gefunden unter jedem Tenant unter [Tenant] > Überwachungsrichtlinien > Standard.


Anmerkung: Die gemeinsame Überwachungsrichtlinie ist der empfohlene Ausgangspunkt für die Syslog-Konfiguration, da sie eine Fabric-weite Abdeckung über alle Hierarchien hinweg bietet und automatisch auf allen Knoten bereitgestellt wird. Die Fabric- und Zugriffsüberwachungsrichtlinien können zusätzlich zur Common Policy konfiguriert werden, um eine detailliertere Kontrolle über bestimmte Objekthierarchien zu erhalten, oder anstelle der Common Policy, um Syslog auf einen engeren Bereich zu beschränken.

Syslog-Nachrichtenformat

ACI-Syslog-Meldungen folgen dem RFC 3164-Format, wenn das Gruppenformat auf aci (der Standard) festgelegt ist:

```
TIMESTAMP SOURCE %FACILITY-SEVERITY-MNEMONIC: Message-text
```

Beispiele:

```
Apr 10 08:25:33 apic1 %LOG_LOCAL0-3-SYSTEM_MSG [F0022][soaking][inoperable][major][topology/pod-1/node-1/.../fault-F0022] LDAP Provider unreachable
```

Der Nachrichtentext enthält den ACI-Fehlercode, den Lebenszyklusstatus (z. B. soaking, retaining, cleared), den Schweregrad und den Distinguished Name (DN) des betroffenen Objekts, sodass die Meldungen automatisch beschrieben werden.

Es stehen drei Optionen für das Nachrichtenformat zur Verfügung:

- aci (Standard) - RFC 3164-konformes Format. Empfohlen für die meisten Bereitstellungen.
- nxos - NX-OS-Format. Verwenden Sie diese Option, wenn die Syslog-Plattform Meldungen im NX-OS-Format erwartet.
- Enhanced Log (APIC 5.2(8) und höher) - RFC 5424-konformes Format mit erweiterten Zeitstempeln, die das Jahr enthalten.

Schweregradzuordnung

Das Syslog-Schweregrad-Feld ist eine einzelne Ziffer zwischen 0 (höchste Priorität) und 7 (niedrigste Priorität). Die folgende Tabelle zeigt die Zuordnung zwischen den Syslog-Schweregraden und der Schweregrad-Terminologie für die ACI/ITU:

Syslog-Schweregrad	ACI-/ITU-Ebene	Beschreibung
0 — Notfall	—	System kann nicht verwendet werden
1 — Alarm	Critical (Kritisch)	Sofortige Maßnahme erforderlich
2 — kritisch	Major (Schwerwiegend)	Kritischer Zustand
3 — Fehler	Geringfügig	Fehlerbedingung
4 — Warnung	Warnung	Warnzustand
5 — Anmeldung	Unbestimmt/Gelöscht	Normaler, aber bedeutsamer Zustand
6 — informativ	—	Nur informative Nachricht
7 — Debugging	—	Nur Debug-Ausgabe

Transportoptionen

Die ACI unterstützt drei Transportprotokolle für Remote-Syslog:

- UDP (Standard) - In allen APIC-Versionen verfügbar. Standardmäßige Lieferung ohne große Probleme.

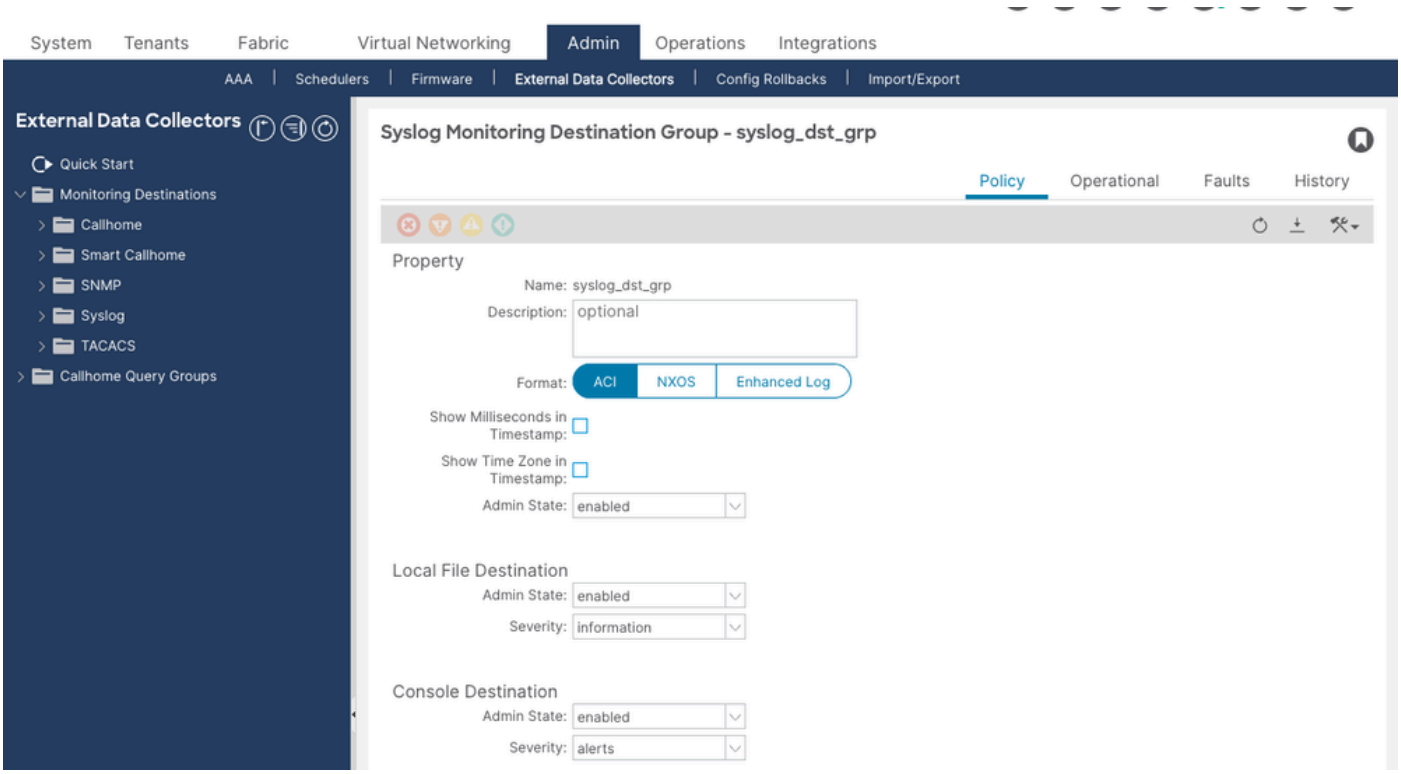
- TCP - Verfügbar ab APIC-Version 5.2(3). Zuverlässige Lieferung durch verbindungsorientierten Transport.
- SSL - verfügbar ab APIC-Version 5.2(4). Stellt verschlüsselten Transport mithilfe von TLS bereit. Jeder ACI-Knoten (APIC oder Switch) agiert als TLS-Client und initiiert eine ausgehende Verbindung zum Syslog-Server. Das Serverzertifikat muss in den APIC hochgeladen werden: Admin > AAA > Security > Public Key Management > Certificate Authorities.

Anmerkung: Wenn ein Remote-Ziel mit SSL-Transport konfiguriert und der APIC auf eine Version herabgestuft wird, die SSL nicht unterstützt, wird das Transportprotokoll automatisch auf UDP zurückgesetzt. Stellen Sie sicher, dass der Syslog-Server auch UDP-Verbindungen als Fallback akzeptieren kann.

Konfiguration

Mit den folgenden Schritten wird das ACI-Syslog vollständig konfiguriert. Führen Sie alle Schritte aus, um die Syslog-Weiterleitung von den APIC-Controllern sowie von den Leaf- und Spine-Switches zu aktivieren.

Schritt 1: Erstellen der Syslog-Zielgruppe



Die Zielgruppe definiert, wohin Syslog-Meldungen gesendet werden und in welchem Format.

Erstellen Sie diese zuerst, da die in späteren Schritten konfigurierten Syslog-Quellen auf diese Gruppe anhand ihres Namens verweisen.

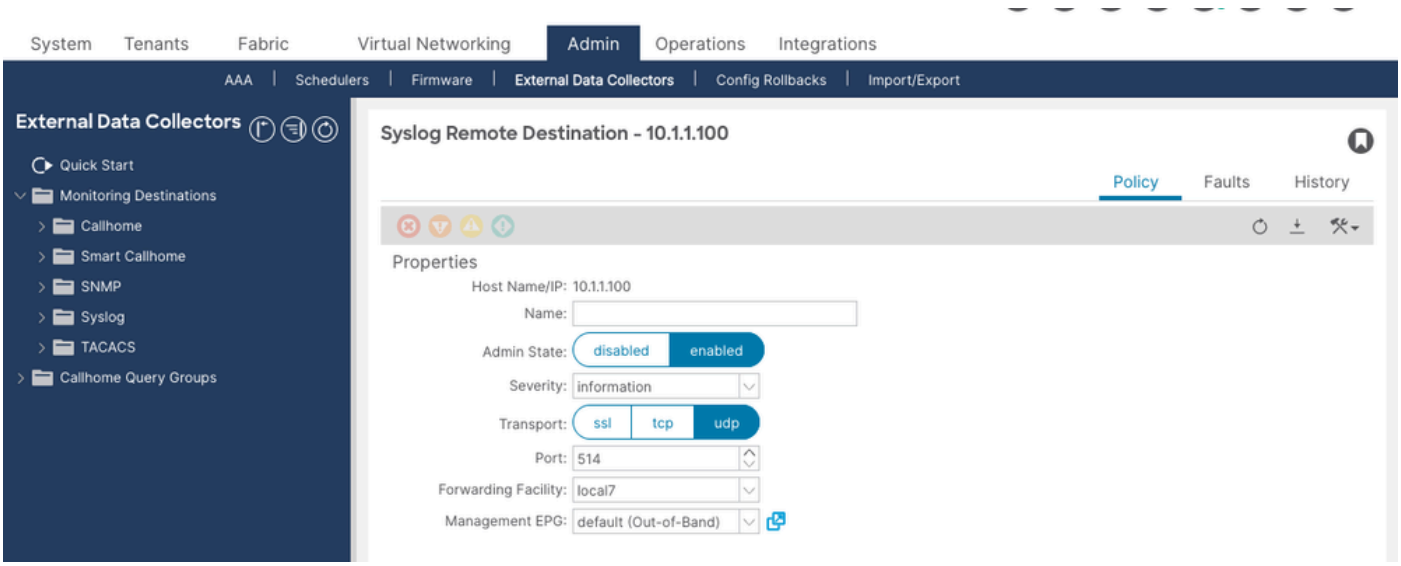
Navigieren Sie zu Admin > External Data Collectors > Monitoring Destinations > Syslog. Klicken Sie mit der rechten Maustaste auf Syslog, und wählen Sie Zielgruppe für Syslog-Überwachung erstellen aus.

Konfigurieren Sie im Assistenten auf der ersten Seite (Gruppenprofil) Folgendes:

- Name - Ein beschreibender Name wie Syslog-Dest-Group.
- Format - aci (Standard, RFC 3164-kompatibel) oder nxos.
- Admin-Status — enabled.
- Admin-Status des lokalen Dateiziels — enabled (empfohlen). Dadurch werden Nachrichten auf /var/log/external/messages jedem Fabric-Knoten geschrieben, was auch dann für die lokale Fehlerbehebung wichtig ist, wenn ein Remote-Server nicht erreichbar ist.
- Schweregrad des lokalen Dateiziels — information.
- Konsolenziel-Admin-Status disabled (empfohlen für Produktionsumgebungen).

Klicken Sie auf Next (Weiter). Klicken Sie auf der zweiten Seite im Bereich Remote-Ziele erstellen auf +, um einen Remote-Syslog-Server hinzuzufügen.

Phase 2: Remote-Ziel hinzufügen



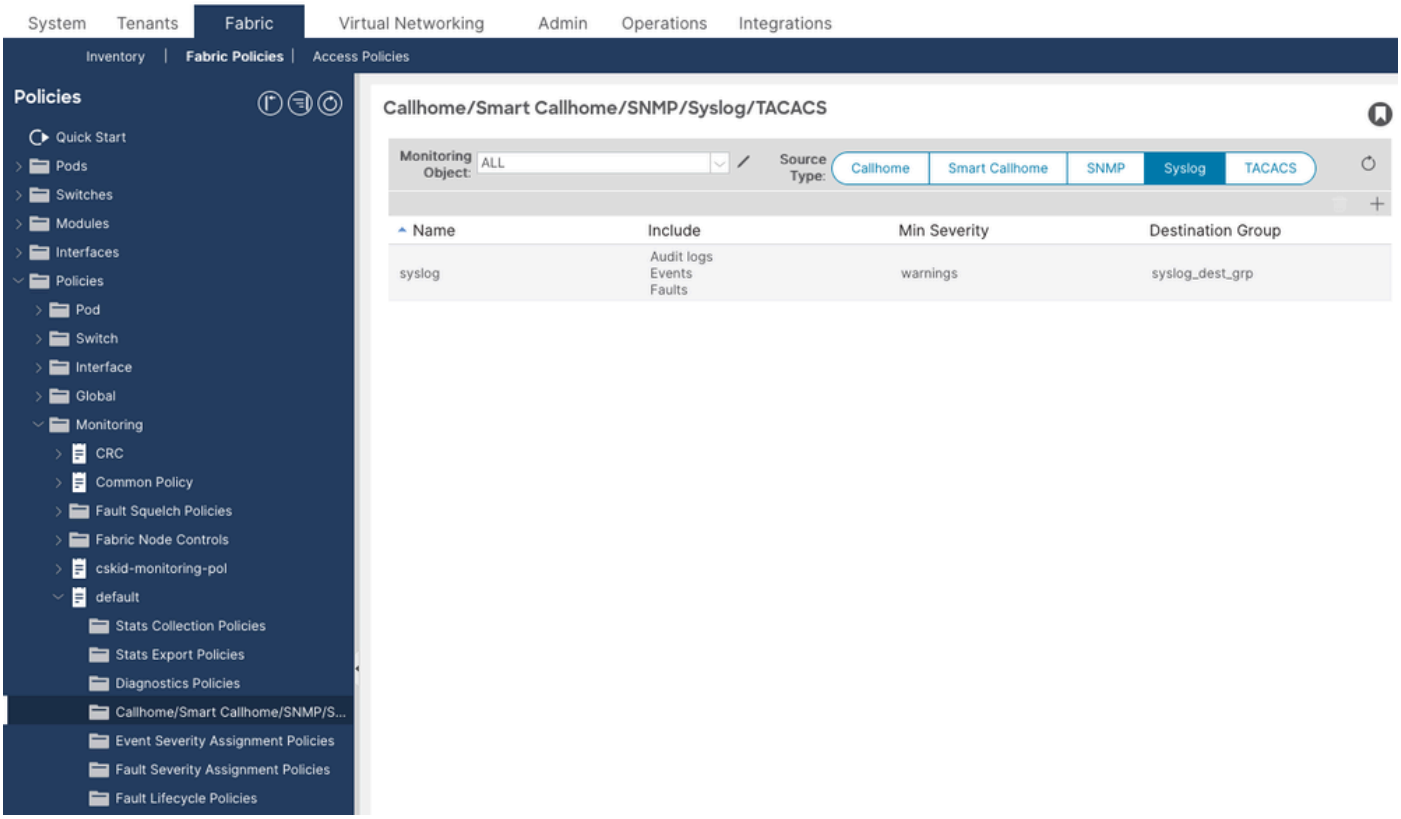
Konfigurieren Sie den Remote-Syslog-Server im Dialogfeld Create Syslog Remote Destination (Syslog Remote-Ziel erstellen):

- Host - IP-Adresse des Syslog-Servers Verwenden Sie eine IP-Adresse anstelle eines Hostnamens. Wenn Sie einen Hostnamen verwenden, müssen Sie sicherstellen, dass der DNS-Server (Domain Name System) über die OOB-Verwaltungsschnittstelle erreichbar ist. DNS-Server, die nur über In-Band-Verbindungen erreichbar sind, können bei einer Netzwerkunterbrechung nicht aufgelöst werden, wenn Syslog-Meldungen generiert werden.
- Admin-Status — enabled.
- Schweregrad - information (empfohlen). Dies ist der minimale Schweregrad, der an diesen Remote-Server gesendet wird.
- Port - 514 (Standard).
- Facility (Einrichtung) local7 (Standard). Legen Sie diese Einstellung fest, um den Einrichtungswert abzugleichen, den Ihr Syslog-Server akzeptiert und weiterleitet.
- Transport — udp (Standard). Verwendung tcp für die zuverlässige Bereitstellung (APIC 5.2(3) oder höher erforderlich) oder ssl für verschlüsselten Transport (APIC 5.2(4) oder höher erforderlich und ein auf den APIC hochgeladenes Zertifikat).
- Management-EPG - Wählen Sie die Management-EPG aus, die für den Syslog-Server erreichbar ist. Für das OOB-Management: uni/tn-mgmt/mgmtp-default/oob-default. Wählen Sie für das In-Band-Management die entsprechende In-Band-EPG aus. Dieses Feld darf nicht leer sein.

Klicken Sie auf OK und dann auf Fertig stellen.

 Anmerkung: Sie können der gleichen Zielgruppe mehrere Remote-Ziele hinzufügen. Jedes Ziel kann über einen anderen Schweregrad, einen anderen Standort und ein anderes Transportprotokoll verfügen.

Schritt 3: Erstellen einer Syslog-Quelle unter der Fabric-Überwachungsrichtlinie



In diesem Schritt wird Syslog für die Fabric-Objekthierarchie konfiguriert - Fabric-Ports, Karten, Chassis-Komponenten und Lüftereinschübe. Dies ergänzt die Gemeinsame Überwachungsrichtlinie (Schritt 4) um eine hierarchiespezifische Kontrolle.

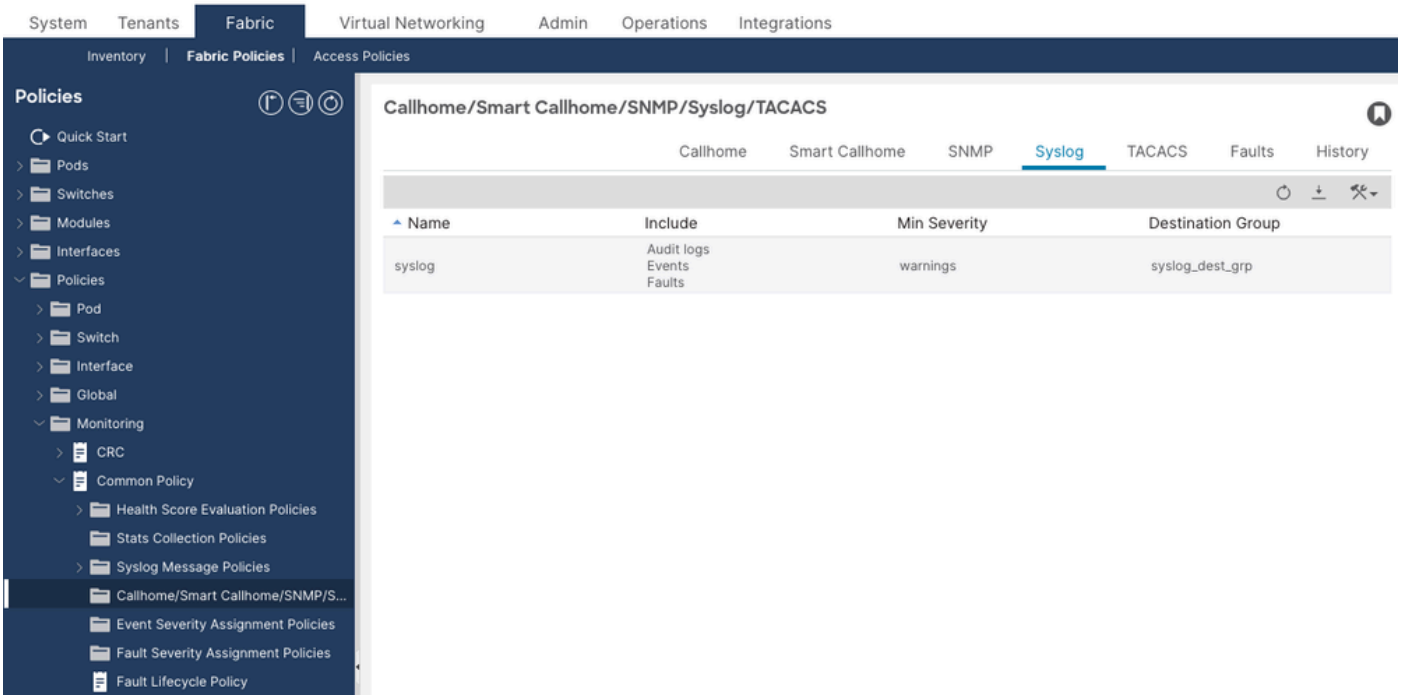
Navigieren Sie zu Fabric > Fabric Policies > Policies > Monitoring > Default > Callhome/Smart Callhome/SNMP/Syslog/TACACS.

Legen Sie im rechten Bereich Source Type (Quelltyp) auf Syslog fest. Klicken Sie auf +, um eine Syslog-Quelle zu erstellen:

- Name - Ein beschreibender Name wie Syslog-Source-Fabric.
- Min Severity (Min. Schweregrad) information (empfohlen für vollständige Abdeckung).
- Einschließen - Prüfung, Ereignisse und Fehler. Fügen Sie optional eine Sitzung für Anmelde- und Abmeldeereignisse hinzu.
- Zielgruppe — Wählen Sie die in Schritt 1 erstellte Zielgruppe aus.

Klicken Sie auf Senden.

Schritt 4: Konfigurieren der allgemeinen Überwachungsrichtlinie (systemweites Syslog)

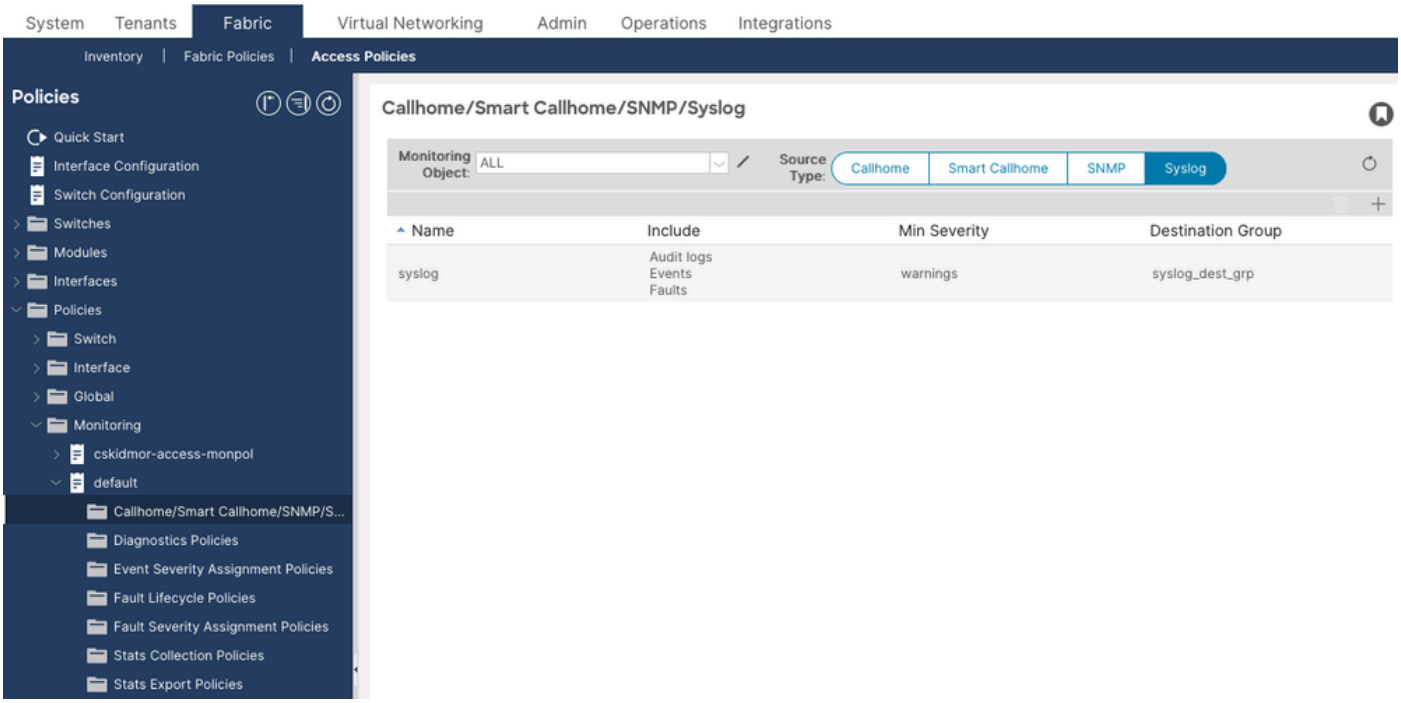


Die Common Monitoring Policy sieht eine systemweite Syslog-Abdeckung vor, die automatisch auf allen Knoten und Controllern in der Fabric bereitgestellt wird. In diesem Schritt wird die Syslog-Quelle des Systems mit der Zielgruppe verknüpft.

Navigieren Sie zu Fabric > Fabric Policies > Policies > Monitoring > Common Policy. Verknüpfen Sie im Abschnitt "Syslog" die Syslog-Quelle des Systems mit der in Schritt 1 erstellten Zielgruppe.

Die Syslog-Quelle des Common Policy-Systems verwendet den MO syslogRsSystemDestGroup bei der DN uni/fabric/moncommon/systemslsrc/rssystemDestGroup.

Schritt 5: Erstellen einer Syslog-Quelle unter der Richtlinie für die Zugriffsüberwachung



In diesem Schritt wird Syslog für die Zugriffsobjekthierarchie konfiguriert - Zugriffsports, Fabric Extender (FEX)-Geräte und VM-Controller-Ereignisse. Dies ergänzt die Gemeinsame Überwachungsrichtlinie (Schritt 4) um eine hierarchiespezifische Kontrolle.

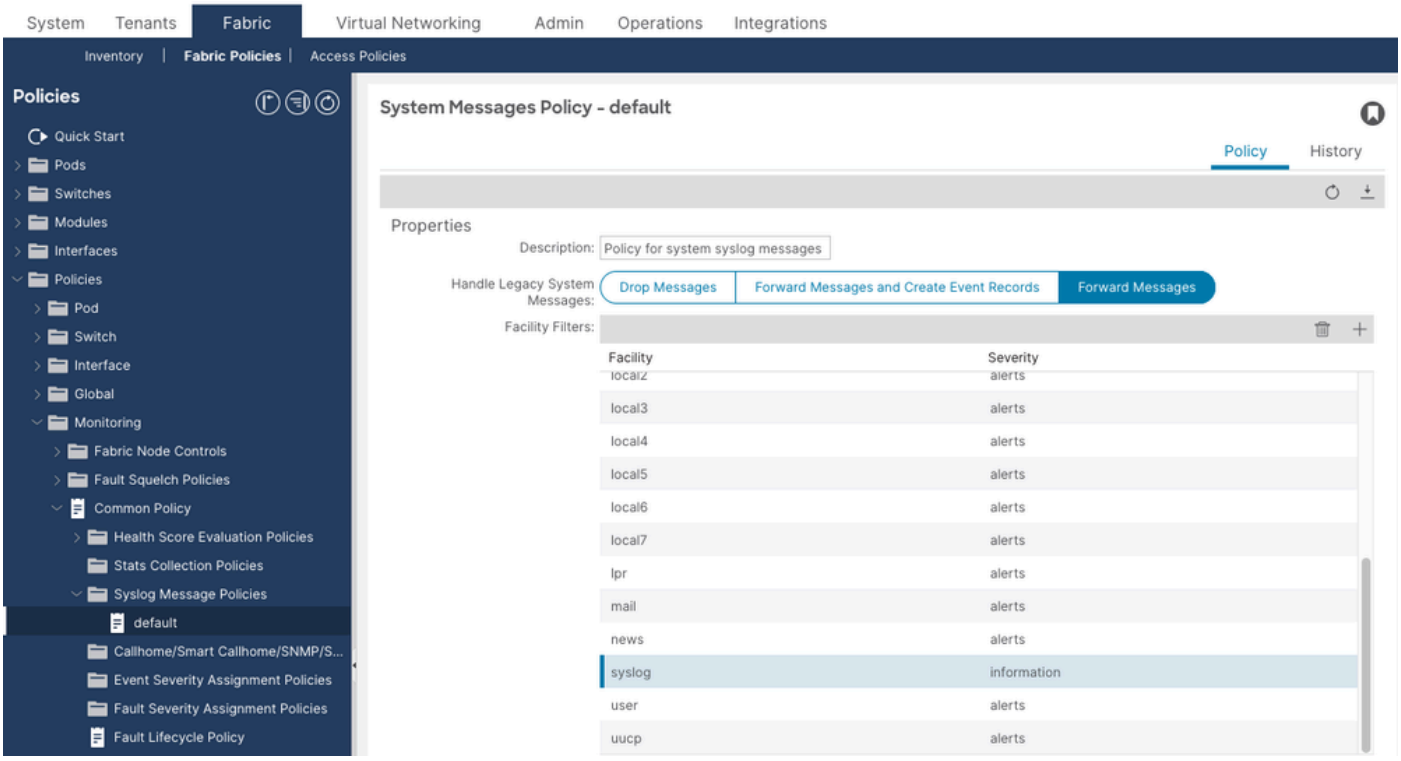
Navigieren Sie zu Fabric > Access Policies > Policies > Monitoring Policies > default > Callhome/SNMP/Syslog.

Setzen Sie den Quelltyp auf Syslog. Klicken Sie auf +, und konfigurieren Sie die gleichen Einstellungen wie in Schritt 3:

- Name - Beispiel: Syslog-Source-Access.
- Min. Schweregrad — information.
- Einschließen - Prüfung, Ereignisse und Fehler.
- Zielgruppe — Wählen Sie dieselbe Zielgruppe aus.

Klicken Sie auf Senden.

Schritt 6 (optional): Stellen Sie die Syslog-Meldungsrichtlinie für die Protokollierung von Vertragszugriffskontrolllisten ein.



Wenn im Remote-Syslog-Server zulässige oder abgelehnte Paketprotokolle (ACLLOG_PKTLOG_PERMIT / ACLLOG_PKTLOG_DENY) der Vertrags-ACLs angezeigt werden sollen, muss der Syslog-Nachrichtenfunktionsfilter auf den informativen Schweregrad gesetzt werden.

Navigieren Sie zu Fabric > Fabric-Richtlinien > Richtlinien > Überwachung > Allgemeine Richtlinie > Syslog-Nachrichtenrichtlinien > Standard. Wählen Sie in der Liste der Anlagenfilter die Syslog-Einrichtung aus, und legen Sie deren Min Severity (Min-Schweregrad) auf informationfest. Dies ist die syslogFacilityFilter MO bei DN uni/fabric/moncommon/sysmsgp/ff-syslog.

Anmerkung: Damit ACL-Zulassungs- und -Ablehnungsprotokolle den Remote-Syslog-Server erreichen, müssen vier Bedingungen erfüllt sein: (1) Die Syslog-Quelle minSev muss eine Information sein, (2) der Schweregrad des Remote-Ziels muss eine Information sein, (3) der Syslog Message Policy-Syslog-Funktionsfilter minSev muss eine Information sein, und (4) die Log-Direktive muss für den Vertragsfiltereintrag aktiviert sein. Wenn alle drei Bedingungen erfüllt sind, stammen die ACL-Protokollmeldungen vom Leaf-Switch (nicht vom APIC), sodass sie zuerst in `/var/log/external/messages` auf dem Leaf angezeigt werden. Die Protokollierungsraten für Vertrags-ACL-Pakete sind durch CoPP begrenzt: deny logs legt den Standardwert auf 500 Pakete pro Sekunde (pps) fest und erlaubt logs mit 300 pps pro Leaf.

Anmerkung: Die Verwendung der Log-Direktive für Filter in Managementverträgen wird nicht unterstützt und verursacht Fehler bei der Bereitstellung von Zoning-Regeln. Wenden Sie die Vertragsprotokollierung nur auf Verträge der Tenant-Datenebene an.

Überprüfen der Konfiguration

Überprüfen Sie die Konfiguration, bevor Sie betriebliche Probleme beheben. Die häufigste Ursache für fehlende Syslog-Meldungen ist eine falsche Konfiguration, kein Netzwerk- oder Softwarefehler.

Überprüfen der Zielgruppe und des Profils

Führen Sie **moquery -c syslogGroup** den APIC aus, um zu überprüfen, ob Zielgruppen vorhanden sind, und überprüfen Sie deren Attribute:

<#root>

```
apic1#

moquery -c syslogGroup

Total Objects shown: 1

# syslog.Group
name                 : Syslog-Dest-Group
dn                   : uni/fabric/slgroup-Syslog-Dest-Group
format               : aci                    <--- aci or nxos
includeMilliSeconds  : yes
includeTimeZone      : yes
remoteDestCount      : 1                      <--- must be ≥1; 0 means no remote dest added
```

Überprüfen Sie dann das Profil (Admin-Status auf Gruppenebene) mit **moquery -c syslogProf**:

<#root>

```
apic1#

moquery -c syslogProf

Total Objects shown: 1

# syslog.Prof
dn           : uni/fabric/slgroup-Syslog-Dest-Group/prof
adminState   : enabled    <--- must be enabled; disabled stops ALL forwarding for this group
transport    : udp
port         : 514
```

Führen Sie Folgendes aus, um nach einer Zielgruppe zu suchen, deren Profil deaktiviert ist:

<#root>

apic1#

moquery -c syslogProf -x 'query-target-filter=eq(syslogProf.adminState,"disabled")'

Das bedeutet, dass die Zielgruppe keinen Syslog-Datenverkehr weiterleitet, unabhängig vom Status des Remote-Ziel-Administrators.

Überprüfen des Remote-Ziels

Führen Sie **moquery -c syslogRemoteDest** aus, um jede Konfiguration des Remote-Servers zu überprüfen:

<#root>

apic1#

moquery -c syslogRemoteDest

```
Total Objects shown: 1

# syslog.RemoteDest
host               : 10.1.1.100
dn                 : uni/fabric/slgroup-Syslog-Dest-Group/rdst-10.1.1.100
adminState         : enabled              <--- must be enabled
epgDn              : uni/tn-mgmt/mgmtp-default/oob-default   <--- must not be empty
forwardingFacility : local7
operState          : unknown              <--- normal; ACI does not probe syslog servers
port               : 514
protocol           : udp
severity           : information          <--- lower values = less restrictive
```

Drei Attribute erfordern besondere Aufmerksamkeit:

- AdminState: muss enabledsein. Wenn diese Option deaktiviert ist, erhält dieser Remote-Server nichts.
- epgDn: darf nicht leer sein. Eine leere Zeichenfolge epgDn bedeutet, dass die Fabric nicht weiß, von welcher Schnittstelle Syslog-Datenverkehr gesendet werden soll, sodass keine Nachrichten die Fabric verlassen.
- Betriebszustand: Unbekannt: Dieser Wert wird erwartet und weist nicht auf ein Problem hin. Die ACI überprüft Syslog-Server nicht aktiv auf ihre Verfügbarkeit.

Überprüfen der Syslog-Quellen

Führen Sie **moquery -c syslogSrc** den Vorgang aus, um zu überprüfen, ob Quellen unter den richtigen Überwachungsrichtlinien vorhanden sind:

<#root>

```
apic1#

moquery -c syslogSrc


Total Objects shown: 2

# syslog.Src
dn           : uni/infra/moninfra-default/slsrc-Syslog-Source-Fabric  <--- fabric monitoring policy (fa
minSev       : information    <--- must match or be lower than remote dest severity
incl         : audit,events,faults

# syslog.Src
dn           : uni/fabric/monfab-default/slsrc-Syslog-Source-Access   <--- access monitoring policy (ac
minSev       : information
incl         : audit,events,faults
```

Bestätigen Sie, dass im Rahmen der entsprechenden Überwachungsrichtlinien Quellen vorhanden sind:

- Eine Quelle unter uni/fabric/moncommon — die gemeinsame Überwachungsrichtlinie für die Fabric-weite Abdeckung aller Knoten und Objekthierarchien.
- Eine Quelle unter uni/infra/moninfra-default - die Fabric-Überwachungsrichtlinie für Objekte auf Fabric-Ebene (Fabric-Ports, Karten, Chassis).
- Eine Quelle unter uni/fabric/monfab-default — die Zugriffsüberwachungsrichtlinie für Objekte auf Zugriffsebene (Access-Ports, FEX, VM-Controller).

Überprüfen Sie außerdem, ob die Syslog-Quelle des Systems der gemeinsamen Überwachungsrichtlinie verknüpft ist:

<#root>

```
apic1#

moquery -d uni/fabric/moncommon/systemslsrc/rssystemDestGroup


Total Objects shown: 1

# syslog.RsSystemDestGroup
dn           : uni/fabric/moncommon/systemslsrc/rssystemDestGroup
tDn          : uni/fabric/slgroup-Syslog-Dest-Group    <--- must point to your dest group
```

Wenn eine Protokollierung der Vertrags-ACL erforderlich ist, überprüfen Sie den Schweregrad des Syslog-Nachrichtenrichtlinienfilters mit **moquery -d uni/fabric/moncommon/sysmsgp/ff-syslog**:

<#root>

```
apic1#

moquery -d uni/fabric/moncommon/sysmsgp/ff-syslog

Total Objects shown: 1

# syslog.FacilityFilter
facility     : syslog
dn           : uni/fabric/moncommon/sysmsgp/ff-syslog
minSev       : information    <--- must be information for ACL logs; default is warnings
```

Überprüfen der lokalen Protokolldatei

Die lokale Datei unter /var/log/external/messages stellt die direkteste Möglichkeit dar, zu bestätigen, dass Syslog-Meldungen auf einem beliebigen Fabric-Knoten generiert werden, auch wenn ein Remote-Server nicht erreichbar ist. Überprüfen Sie dies sowohl am APIC als auch an einem Leaf-Switch:

<#root>

```
apic1#

cat /var/log/external/messages | tail -20

Apr 10 08:25:33 apic1 %LOG_LOCAL0-3-SYSTEM_MSG [F0022][soaking][inoperable][major][topology/pod-1/node-
Apr 10 08:30:02 apic1 %LOG_LOCAL0-6-SYSTEM_MSG [F0022][retaining][inoperable][cleared][topology/pod-1/n
```

<#root>

```
leaf1#

cat /var/log/external/messages | tail -20

Apr 10 09:47:14 leaf1 %LOG_LOCAL0-6-SYSTEM_MSG [E4208077][oper-state-change][info][sys/ipv4/inst/dom-Pr
Apr 10 09:51:15 leaf1 %LOG_LOCAL0-6-SYSTEM_MSG [login,session][info][subj-[uni/userext/remoteuser-admin
```

Wenn diese Datei leer ist oder auf einem Knoten nicht aktualisiert wird, werden an der Quelle keine Nachrichten generiert. Wenn die Datei Inhalt hat, der entfernte Syslog-Server jedoch keine Nachrichten empfängt, liegt das Problem in der Weiterleitung (Zielgruppe, Netzwerk oder Firewall) und nicht in der Nachrichtengenerierung.

Überprüfen der Erreichbarkeit des Syslog-Servers

Führen Sie einen Ping vom APIC zum Syslog-Server aus, um die IP-Verfügbarkeit über das Managementnetzwerk zu überprüfen:

```
<#root>

apic1#

ping -c 3 10.1.1.100


PING 10.1.1.100 (10.1.1.100) 56(84) bytes of data.
64 bytes from 10.1.1.100: icmp_seq=1 ttl=251 time=0.8 ms
64 bytes from 10.1.1.100: icmp_seq=2 ttl=251 time=0.8 ms
64 bytes from 10.1.1.100: icmp_seq=3 ttl=251 time=0.8 ms
```

Verwenden Sie von einem Leaf- oder Spine-Switch aus die `IP-Leitung` mit dem `-V-`Flag, um die VRF-Instanz festzulegen. Verwenden Sie `Management` für Out-of-Band oder `mgmt:inb` für In-Band, je nachdem, welche Management-EPG dem Syslog-Ziel zugewiesen ist:

```
<#root>

leaf1#

iping -V management 10.1.1.100


PING 10.1.1.100 (10.1.1.100): 56 data bytes
64 bytes from 10.1.1.100: icmp_seq=0 ttl=59 time=1.324 ms
64 bytes from 10.1.1.100: icmp_seq=1 ttl=59 time=0.622 ms

--- 10.1.1.100 ping statistics ---
2 packets transmitted, 2 packets received, 0.00% packet loss
round-trip min/avg/max = 0.622/0.973/1.324 ms
```

```
<#root>

leaf1#

iping -V mgmt:inb 10.1.1.100


PING 10.1.1.100 (10.1.1.100): 56 data bytes
64 bytes from 10.1.1.100: icmp_seq=0 ttl=58 time=0.833 ms
64 bytes from 10.1.1.100: icmp_seq=1 ttl=58 time=0.608 ms

--- 10.1.1.100 ping statistics ---
2 packets transmitted, 2 packets received, 0.00% packet loss
round-trip min/avg/max = 0.608/0.72/0.833 ms
```

Ein erfolgreicher Ping bestätigt die IP-Erreichbarkeit, bestätigt jedoch nicht, dass der UDP- oder TCP-Port 514 zulässig ist. Internet Control Message Protocol (ICMP) und Syslog verwenden unterschiedliche Protokolle.

Fehlerbehebung

Triage-Workflow

Verwenden Sie die folgende Entscheidungsstruktur, wenn Syslog-Meldungen nicht auf dem Remote-Server eingehen:

```
No messages at remote syslog server
│
├─ Step 1: Check /var/log/external/messages on APIC and a leaf
│   ├─ File is EMPTY or not updating
│   │   → No messages are being generated at the source. Proceed to configuration checks:
│   │     - Is a syslogSrc configured and linked to the destination group?
│   │     - Is minSev set to information?
│   │     - Does incl include audit, events, and faults?
│   │
│   └─ File HAS CONTENT (messages are generating locally)
│       → Problem is in forwarding to the remote server. Continue to Step 2.
│
├─ Step 2: Check syslogProf adminState
│   └─ adminState = disabled → Enable it. This stops ALL forwarding from this group.
│
├─ Step 3: Check syslogRemoteDest adminState
│   └─ adminState = disabled → Enable it. This stops messages to this specific server.
│
├─ Step 4: Check syslogRemoteDest epgDn
│   └─ epgDn is empty → Set the correct Management EPG (OOB or in-band).
│
├─ Step 5: Verify network reachability
│   Run on the APIC: ping -c 3 10.1.1.100
│   ├─ ping FAILS → routing/firewall issue; verify OOB routing table and firewall rules
│   └─ ping SUCCEEDS → IP reachable; check firewall for UDP/TCP port 514 specifically

Messages from some nodes or object hierarchies are missing
└─ Check Common Policy — is it linked to the destination group?
    └─ Verify: moquery -d uni/fabric/moncommon/systemslsrc/rssystemDestGroup
    └─ Not linked → Configure Common Policy (Step 4) for fabric-wide coverage
    └─ Also check Fabric and Access policy sources for hierarchy-specific coverage

Messages arrive but important events are missing
└─ Check syslogSrc minSev AND syslogRemoteDest severity
    └─ Both must be information for full coverage; the more restrictive of the two applies
```

Gängige Szenarien

Szenario 1: Keine Syslog-Meldungen auf dem Remote-Server empfangen

Problem: Die Syslog-Zielgruppe und das Remote-Ziel sind konfiguriert, es werden jedoch keine Meldungen an den Remote-Server gesendet. Die lokale Datei /var/log/external/messages auf dem APIC und den Switches enthält aktuelle Einträge.

Konfigurationsprüfung:

<#root>

```
apic1#

moquery -c syslogRemoteDest

# syslog.RemoteDest
host       : 10.1.1.100
adminState : disabled    <--- PROBLEM: remote destination is disabled
epgDn      : uni/tn-mgmt/mgmtp-default/oob-default
```

Ursache: Der Status des Remote-Ziel-Administrators lautet disabled. Dies kann passieren, wenn das Ziel erstellt, aber versehentlich deaktiviert wurde, oder wenn es während der Wartung deaktiviert und nie wieder aktiviert wurde.

Lösung: Navigieren Sie zu Admin > External Data Collectors > Monitoring Destinations > Syslog > [Gruppenname] > Remote Destinations > [Server]. Bearbeiten Sie das Remote-Ziel, und setzen Sie den Admin State auf enabled (aktiviert).

Szenario 2: Syslog-Zielgruppenprofil ist deaktiviert

Problem: Es werden keine Nachrichten von einem Knoten weitergeleitet, obwohl der Administrator-Status für das Remote-Ziel aktiviert ist.

Konfigurationsprüfung:

<#root>

```
apic1#

moquery -c syslogProf -x 'query-target-filter=eq(syslogProf.adminState,"disabled")'

Total Objects shown: 1

# syslog.Prof
```

```
dn           : uni/fabric/slgroup-Syslog-Dest-Group/prof
adminState   : disabled    <--- PROBLEM: group profile is disabled
transport    : udp
```

Ursache: Der syslogProf Admin-Status steuert die gesamte Zielgruppe. Wenn sie deaktiviert ist, werden unabhängig von den einzelnen Remote-Zielstatus keine Nachrichten von einem Knoten weitergeleitet.

Lösung: Navigieren Sie zu Admin > External Data Collectors > Monitoring Destinations > Syslog > [Gruppenname]. Bearbeiten Sie das Profil, und setzen Sie den Admin State auf enabled (Aktiviert).

Szenario 3: Ereignisse fehlen — Gemeinsame Überwachungsrichtlinie nicht verknüpft

Problem: Syslog-Meldungen von einigen Knoten oder Objekthierarchien erreichen den Remote-Server nicht, obwohl eine Syslog-Quelle in der Fabric- oder Zugriffsüberwachungsrichtlinie konfiguriert ist.

Konfigurationsprüfung:

<#root>

```
apic1#

moquery -d uni/fabric/moncommon/systemslsrc/rssystemDestGroup

Total Objects shown: 0
```

Die Syslog-Quelle des Systems der allgemeinen Überwachungsrichtlinie ist nicht mit der Zielgruppe verknüpft.

Ursache: Die Common Monitoring Policy (uni/fabric/moncommon) sorgt für eine Fabric-weite Syslog-Abdeckung in allen Hierarchien und wird automatisch auf allen Knoten und Controllern bereitgestellt. Andernfalls werden nur Ereignisse weitergeleitet, die mit den spezifischen Hierarchien der Fabric- oder Zugriffsüberwachungsrichtlinien übereinstimmen. Die Fabric-Überwachungsrichtlinie (uni/infra/moninfra-default) deckt Objekte auf Fabric-Ebene ab, und die Zugriffsüberwachungsrichtlinie (uni/fabric/monfab-default) deckt Objekte auf Access-Ebene ab, bietet aber keine der beiden Methoden die von der Common Policy angebotene Fabric-weite Abdeckung.

Lösung: Navigieren Sie zu Fabric > Fabric Policies > Policies > Monitoring > Common Policy.

Verknüpfen Sie im Abschnitt Syslog die Syslog-Quelle des Systems mit der Zielgruppe. Überprüfen Sie mit **moquery -d uni/fabric/moncommon/systemslsrc/rssystemDestGroup** , ob die tDn auf Ihre Zielgruppe zeigt.

Szenario 4: Schweregrad zu restriktiv - erwartete Nachrichten fehlen

Problem: Einige Nachrichten erreichen den Syslog-Server, aber es fehlen Informationsereignisse, Überwachungsprotokolleinträge oder Sitzungsanmeldeereignisse. Es werden nur kritische und größere Störungen gesehen.

Konfigurationsprüfung:

<#root>

```
apic1#

moquery -c syslogSrc

# syslog.Src
dn       : uni/fabric/monfab-default/slsrc-Syslog-Source-Fabric
minSev   : warnings    <--- PROBLEM: only warnings and above are sent; info events filtered out
incl     : faults      <--- PROBLEM: audit and events are not included
```

<#root>

```
apic1#

moquery -c syslogRemoteDest

# syslog.RemoteDest
host     : 10.1.1.100
severity : warnings    <--- PROBLEM: remote dest severity also too restrictive
```

Ursache: Die Syslog-Filterung tritt an zwei Punkten auf: Quelle (minSev) und Remote-Ziel (severity). Nur Nachrichten, die beide Filter passieren, werden weitergeleitet. Wenn einer der Werte oben eingestellt ist, informationwerden Informationsmeldungen verworfen.

Lösung: Bearbeiten Sie die Syslog-Quelle, und legen Sie den Min Severity-Wert auf Informationen fest, und überprüfen Sie Audit, Ereignisse und Fehler im Feld Include (Einschließen). Bearbeiten Sie das Remote-Ziel, und legen Sie den Schweregrad auf Informationen fest.

Szenario 5: Keine Verwaltungs-EPG für Remote-Ziel zugewiesen

Problem: Auf dem Remote-Server werden keine Syslog-Meldungen empfangen. Die Zielgruppe ist aktiviert, das Remote-Ziel ist aktiviert, und die lokale Protokolldatei enthält Inhalt.

Konfigurationsprüfung:

<#root>

```
apic1#

moquery -c syslogRemoteDest

# syslog.RemoteDest
host       : 10.1.1.100
adminState : enabled
epgDn      :             <--- PROBLEM: Management EPG is empty
```

Ursache: Ohne Management-EPG wissen der APIC und die Switches nicht, welche physische Schnittstelle zum Senden von Syslog-Meldungen verwendet werden soll. Nachrichten werden generiert, können aber nicht weitergeleitet werden.

Lösung: Bearbeiten Sie das Remote-Ziel, und wählen Sie die entsprechende Management-EPG aus. Wählen Sie für das OOB-Management uni/tn-mgmt/mgmtp-default/oob-default. Wählen Sie für das In-Band-Management die entsprechende In-Band-EPG aus.

Szenario 6: Falsche Management-EPG (In-Band und Out-of-Band)

Problem: Syslog-Meldungen kommen gelegentlich oder nur von einigen Knoten an. Der Syslog-Server ist nur über die OOB-Verwaltung erreichbar, aber das Remote-Ziel verweist auf die In-Band-EPG.

Konfigurationsprüfung:

<#root>

```
apic1#

moquery -c syslogRemoteDest

# syslog.RemoteDest
host       : 10.1.1.100
epgDn      : uni/tn-mgmt/mgmtp-default/inb-In-Band    <--- in-band EPG selected
```

Wenn der Syslog-Server nur über das OOB-Netzwerk erreichbar ist, führt die In-Band-EPG dazu, dass Meldungen von der In-Band-Schnittstelle stammen, die den Server nicht erreichen kann.

Lösung: Bearbeiten Sie das Remote-Ziel, und ändern Sie die Management-EPG in uni/tn-mgmt/mgmtp-default/oob-default. Überprüfen Sie mithilfe **ping -c 3 10.1.1.100** des APIC-Bash, ob der OOB erreichbar ist.

Szenario 7: Firewall blockiert Syslog-Datenverkehr

Problem: Die lokale Protokolldatei enthält Inhalt sowohl auf dem APIC als auch auf den Leaf-Knoten. Die Konfiguration ist korrekt, das ICMP-Ping an den Syslog-Server ist erfolgreich, es werden jedoch keine Meldungen an den Server gesendet.

Betriebsprüfung: Führen Sie einen Ping vom APIC zum Syslog-Server aus, um die IP-Erreichbarkeit zu überprüfen:

<#root>

```
apic1#

ping -c 3 10.1.1.100

PING 10.1.1.100 (10.1.1.100) 56(84) bytes of data.
64 bytes from 10.1.1.100: icmp_seq=1 ttl=251 time=0.8 ms
64 bytes from 10.1.1.100: icmp_seq=2 ttl=251 time=0.8 ms
64 bytes from 10.1.1.100: icmp_seq=3 ttl=251 time=0.8 ms
```

Ping erfolgreich, aber Syslog-Meldungen kommen nicht an. ICMP (Ping) verläuft erfolgreich, während der UDP-Port 514 blockiert wird.

Ursache: Eine Firewall oder ACL zwischen dem Managementnetzwerk und dem Syslog-Server blockiert den UDP-Port 514 (oder TCP 514, wenn TCP-Transport konfiguriert ist). ICMP und UDP sind unabhängig - durch ICMP-Übertragung wird nicht bestätigt, dass UDP 514 zulässig ist. Darüber hinaus sendet jedes Leaf und jede Spine Syslog direkt von der eigenen OOB-IP-Adresse. Eine Firewall, die nur die APIC OOB-IPs zulässt, verwirft Syslog-Pakete, die von Switch-Knoten stammen.

Lösung: Überprüfen Sie, ob die Firewall den UDP-/TCP-Port 514 aus dem OOB-IP-Adressbereich aller Fabric-Knoten zulässt, einschließlich aller APICs, aller Leaf-Switches und aller Spine-Switches. Eine Paketerfassung auf dem Syslog-Server bestätigt, ob UDP 514-Pakete eintreffen.

Szenario 8: ACL-Vertrags: Protokolle zulassen/verweigern nicht vorhanden

Problem: Contract-Allow- oder -Deny-Packet-Logs (ACLLOG_PKTLOG_PERMIT/) ACLLOG_PKTLOG_DENYkommen nicht beim Syslog-Server an.

Konfigurationsprüfung:

1. Stellen Sie sicher, dass der Schweregrad der Syslog-Quelle informationlautet:
   <#root>

   ```
   apic1#

   moquery -c syslogSrc

   # syslog.Src
   minSev : information    <--- must be information; any higher value drops ACL logs
   ```

2. Überprüfen Sie, ob der Schweregrad des Remote-Ziels information:
   <#root>

   ```
   apic1#

   moquery -c syslogRemoteDest

   # syslog.RemoteDest
   severity : information    <--- must be information
   ```

3. Stellen Sie sicher, dass der Schweregrad des Syslog-Nachrichtenrichtlinienfilters information:
   <#root>

   ```
   apic1#

   moquery -d uni/fabric/moncommon/sysmsgp/ff-syslog

   # syslog.FacilityFilter
   facility : syslog
   minSev   : information    <--- must be information; default is warnings which drops ACL logs
   ```

4. Überprüfen Sie, ob die Protokollanweisung für den Vertragsfilter aktiviert ist. Navigieren Sie zu Tenants > [Tenant] > Contracts > [contract] > Subjects > [subject] > Filters (Tenants > [Tenant] > Verträge), und bestätigen Sie, dass in der Spalte Directions (Richtlinien) das Protokoll für den entsprechenden Filtereintrag angezeigt wird.
5. Vergewissern Sie sich, dass auf dem Leaf-Switch ACL-Protokolle generiert werden (ACL-Protokolle stammen vom Leaf, nicht vom APIC):
   <#root>

   ```
   leaf1#

   show logging ip access-list internal packet-log deny
   ```

   <#root>

   ```
   leaf1#
   ```

```
cat /var/log/external/messages | grep ACLLOG | tail -20
```

Wenn keine ACLLOG Einträge angezeigt werden, löst die log-Direktive keine Protokollgenerierung auf dem Leaf aus. Dies kann auf eine falsch konfigurierte Vertragsanweisung hinweisen, darauf, dass kein übereinstimmender Datenverkehr den Vertrag erreicht oder dass Pakete bei der CoPP-Ratenbegrenzung verworfen werden, bevor sie protokolliert werden.

Ursache: Der Schweregrad des Vertrags-ACL-Protokolls ist informational (Syslog-Ebene 6). Wenn ein Filter in der Syslog-Kette - Quelle minSev, Remote-Ziel severityoder Syslog Message Policy Facility-Filter (syslogFacilityFilter at uni/fabric/moncommon/sysmsgp/ff-syslog) - oben festgelegt ist, werden informationdie ACL-Protokollmeldungen ohne Nachfrage verworfen, bevor sie den Fabric-Knoten verlassen.

Lösung: Legen Sie minSev auf information der Syslog-Quelle fest, legen Sie severity auf information dem Remote-Ziel fest, stellen Sie den syslog Anlagenfilter minSev auf information unter Common Policy > Syslog Message Policies > default ein, bestätigen Sie, dass die Log-Direktive auf dem Vertragsfilter aktiviert ist, und stellen Sie sicher, dass die Firewall den Syslog-Datenverkehr von den OOB-IP-Adressen desLeaf-Switches zulässt, nicht nur von den APIC-IPs, da ACL-Protokolle vom Switch.

Szenario 9: Syslog wird nach dem Umbenennen der Zielgruppe beendet

Problem: Syslog-Meldungen gelangen nicht mehr zum Remote-Server, nachdem der Name der Syslog-Zielgruppe geändert wurde. Eine Änderung des Hafens oder der Anlage verursacht dieses Problem nicht. Durch Deaktivieren und erneutes Aktivieren der Richtlinie wird die Nachrichtenübermittlung nicht fortgesetzt.

Ursache: Dies ist ein bekannter Softwarefehler. Siehe Cisco Bug-ID CSCwj23752. Durch das Umbenennen der Zielgruppe wird die interne Syslog-Weiterleitungszuordnung aufgehoben. Sie wurde in APIC Version 6.0(6) und höher behoben.

Lösung: Upgrade auf APIC Version 6.0(6c) oder höher Löschen Sie als Problemumgehung für die betroffenen Versionen die umbenannte Zielgruppe, und erstellen Sie sie mit dem gewünschten Namen neu, und ordnen Sie dann die Syslog-Quellen erneut zu.

Szenario 10: Übermäßiges Syslog verursacht Langsamkeit der APIC-GUI

Problem: Die APIC-GUI wird langsam, und die CPU-Auslastung des APIC ist hoch. Dies kann auftreten, wenn die Protokollierung von Vertrags-ACLs während des normalen Betriebs aktiviert bleibt, wodurch eine große Menge an Syslog-Informationsmeldungen generiert wird, die in Objekte in der APIC-Datenbank konvertiert eventRecord werden.

Ursache: Wenn der Schweregrad der Common Policy Syslog Message Policy (Common-Policy-Syslog-Meldungsrichtlinie) auf information festgelegt ist, generiert jede informative Syslog-Meldung, einschließlich der ACL-Protokolle mit hohem Volumen, einen Fehler eventRecord im APIC. Dies kann die APIC-Datenbank überlasten und zu verlangsamten Benutzeroberflächen führen.

Lösung:

- Deaktivieren Sie die Protokollierung von Vertrags-ACLs während des normalen Betriebs. Aktivieren Sie diese Option nur während der Problembehebungs- oder Wartungsfenster.
- Wenn die ACL-Protokollierung aktiviert bleiben muss, setzen Sie den Schweregrad der Syslog-Nachrichtenrichtlinie auf alertsFabric > Fabric Policies > Policies > Monitoring > Common Policy > Syslog Message Policies > default. Auf diese Weise wird verhindert, dass Syslog-Informationsmeldungen in Ereignisse umgewandelt werden, während gleichzeitig ihre Weiterleitung an den Remote-Syslog-Server möglich ist.
- Geräuschhafte Ereigniscodes, die für den Betrieb nicht nützlich sind, können abgefangen werden. Ein Ereigniscode kann gelöscht werden, um zu verhindern, dass er Ereignisdatensätze generiert, ohne die Syslog-Weiterleitung zu beeinträchtigen.

Bekannte Fehler

Die folgenden bekannten Softwarefehler haben Auswirkungen auf die ACI-Syslog-Funktionalität:

- Cisco Bug-ID CSCwj23752: Durch Umbenennen der Syslog-Zielgruppe wird die Syslog-Übermittlung beendet. Behoben in APIC Version 6.0(6c) und höher.

Eskalationskriterien

Holen Sie technischen Support ein, und wenden Sie sich an das Cisco TAC, wenn:

- Syslog-Meldungen werden /var/log/external/messages lokal auf Fabric-Knoten angezeigt, Zielgruppen- und Remote-Ziel-Admin-Zustände sind beide enabledgegeben, die Management-EPG ist korrekt, die Netzwerkerreichbarkeit wurde bestätigt (Ping- und Firewall-Prüfung bestanden), aber die Meldungen erreichen den Remote-Server immer noch nicht.
- Syslog-Meldungen kommen von einigen Fabric-Knoten, aber nicht von anderen, ohne Unterschied in der Konfiguration, was auf eine Inkonsistenz bei der Richtlinienbereitstellung hindeutet.
- Das Zielgruppenprofil oder Remote-Ziel wurde erneut aktiviert, aber die Nachrichten werden nach der Konfigurationsänderung nicht innerhalb weniger Minuten fortgesetzt.
- Nach einem APIC-Upgrade sind keine Syslog-Meldungen mehr eingegangen, was auf einen potenziellen Softwarefehler hindeutet.

Zu erfassende Daten vor dem Öffnen eines TAC-Tickets:

- Bedarfsgerechter technischer Support durch den betroffenen APIC und einen betroffenen Leaf-Knoten.
- Ausgabe von `moquery -c syslogGroup`, `moquery -c syslogProf`, `moquery -c syslogRemoteDest`und `moquery -c syslogSrc` vom APIC.
- Ausgabe von `moquery -d uni/fabric/moncommon/systemslsrc/rssystemDestGroup` , um den Link zur gemeinsamen Richtlinie zu überprüfen.
- Schwanz `/var/log/external/messages` eines APIC und eines betroffenen Leaf.
- Paketerfassung vom Syslog-Server, die bestätigt, ob UDP-/TCP 514-Pakete von Fabric-OOB-Adressen ankommen.

Referenzen

- Cisco APIC Basic Konfigurationsleitfaden, Version 6.1(x) - Verwaltung
- Leitfaden zu Cisco ACI-Systemmeldungen
- Managementleitfaden für Cisco ACI-Fehler, -Ereignisse und -Systemmeldungen
- Cisco ACI-Vertragsleitfaden - Whitepaper
- Fehlerbehebung in einer langsamen APIC-GUI

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.