Syslog configureren en oplossen in ACI

Inleiding

In dit document wordt beschreven hoe u systeemlogboekregistratie (syslog) in Cisco Application Centric Infrastructure (ACI) configureert, verifieert en oplost. Het omvat de volledige configuratieworkflow, programmatische verificatie met behulp van het Application Policy Infrastructure Controller (APIC) managed-object (MO) -model en een gestructureerde workflow voor probleemoplossing voor zowel APIC-controllers als switches van bladeren en ruggengraat.

Overzicht

ACI syslog is volledig beleidsgestuurd. In tegenstelling tot de zelfstandige Cisco NX-OS®-software, zijn er geen CLI-**logging server**opdrachten op ACI-switches. Alle syslog-configuratie gebeurt via APIC-beleid dat de APIC automatisch naar elke fabric-node duwt.

Belangrijkste onderdelen

Het syslog-subsysteem in ACI is opgebouwd uit de volgende beheerde objecten:

- Syslog Destination Group (syslogGroup) — De container op het hoogste niveau voor alle syslog-bestemmingen. Het regelt de berichtindeling (ACI- of NX-OS-stijl) en tijdstempelopties. Het kan een of meer externe bestemmingen, een lokale bestandsbestemming en een consolebestemming bevatten.
- Syslog Profile (syslogProf) — Een kind van de bestemmingsgroep dat de beheerdersstatus op groepsniveau en het transportprotocol (UDP, TCP of SSL) beheert.
- Syslog Remote Destination (syslogRemoteDest) — Een kind van de bestemmingsgroep dat één externe syslog-server vertegenwoordigt. Hiermee worden de IP- of hostnaam van de server, de poort, het prioriteitsfilter, de syslog-faciliteit en de beheereindpuntgroep (EPG) die wordt gebruikt om de server te bereiken, beheerd.
- Syslog Local File (syslogFile) — Een onderliggend bestand van de bestemmingsgroep dat het schrijven van syslog-berichten naar het lokale bestand /var/log/external/messages op elke knooppunt van de fabric regelt.
- Syslog Bron (syslogSrc) — Gehecht aan een monitoringbeleid. Bepaalt welke berichttypen (audit, gebeurtenissen, fouten, sessie) en minimale ernst worden verzonden en koppelingen naar de bestemmingsgroep via een syslogRsDestGroup relatie.

Syslog-bronbevestigingspunten

ACI maakt gebruik van vier beleidsscopes voor bewaking die bepalen welke knooppunten en objecten syslog-berichten genereren:

- Gemeenschappelijk monitoringbeleid (monCommonPol, uni/fabric/moncommon) — breed toepassingsgebied. Een basisbeleid voor bewaking dat van toepassing is op alle fouten en gebeurtenissen en automatisch wordt geïmplementeerd in alle knooppunten (switches van bladeren en ruggengraat) en alle controllers (APIC's) in de stof. Omvat alle hiërarchieën voor verbindingen, toegang en huurders. Gevonden op Fabric > Fabric Policies > Policies > Monitoring > Common Policy.
- Materiaalbewakingsbeleid (monInfraPol, uni/infra/moninfra-default) — Materiaalbereik. Genereert syslog voor objecten op weefselniveau: fabric-poorten, kaarten, chassisonderdelen en ventilatorladen. Gevonden bij Fabric > Fabric Policies > Policies > Monitoring > default.
- Toegangsbewakingsbeleid (monFabricPol, uni/fabric/monfab-defaultGMP) — Reikwijdte van de toegang (infrastructuur). Genereert syslog voor componenten die toegang bieden: toegangspoorten, Fabric Extender (FEX)-apparaten en gebeurtenissen met een virtuele machine (VM)-controller. Gevonden bij Verbinding > Toegangsbeleid > Beleid > Controlebeleid > Standaard.
- Monitoringbeleid voor huurders (monEPGPol, uni/tn-common/monepg-default) — Reikwijdte huurder. Genereert syslog voor objecten met een tenant-bereik: eindpuntgroepen (EPG's), toepassingsprofielen en services. Gevonden onder elke tenant bij [Tenant] > Monitoring Policies > default.

Opmerking: het gemeenschappelijk monitoringbeleid is het aanbevolen uitgangspunt voor syslog-configuratie omdat het dekking biedt voor de hele structuur in alle hiërarchieën en automatisch wordt geïmplementeerd in alle nodes. Het Fabric and Access Monitoring Policies kan worden geconfigureerd in aanvulling op het Common Policy voor meer gedetailleerde controle over specifieke objecthiërarchieën, of in plaats van het Common Policy om syslog te beperken tot een beperkter bereik.

Syslog-berichtindeling

ACI syslog-berichten volgen de RFC 3164-indeling wanneer de groepsindeling is ingesteld op aci (de standaardwaarde):

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

Voorbeeld:

```
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
```

De berichttekst bevat de ACI-foutcode, de levenscyclusstatus (bijvoorbeeld soakingACIretaining, clearedACI), de ernst en de DN-naam van het betreffende object, waardoor berichten zichzelf beschrijven.

Er zijn drie opties voor berichtindeling beschikbaar:

- aci (standaard) — RFC 3164-compatibel formaat. Aanbevolen voor de meeste implementaties.
- nxos — NX-OS-stijl formaat. Gebruik dit als het syslog-platform berichten met NX-OS-indeling verwacht.
- Verbeterd logboek (APIC 5.2(8) en hoger) — RFC 5424-compatibel formaat met verbeterde tijdstempels die het jaar bevatten.

dichtheidsbepaling

Het syslog-ernstveld bestaat uit één cijfer van 0 (meest ernstig) tot 7 (minst ernstig). De volgende tabel toont de mapping tussen syslog-ernstniveaus en ACI / International Telecommunication Union (ITU)-ernstterminologie:

Syslog-ernst	ACI-/ITU-niveau	Beschrijving
0 — Noodsituatie	—	Systeem is onbruikbaar
1 — Waarschuwing	Critical (Kritiek)	Onmiddellijke actie vereist
2 — Kritiek	Major (Groot)	Kritieke toestand
3 — Fout	Beperkt	Foutconditie
4 — Waarschuwing	WAARSCHUWING	Waarschuwingsvoorwaarde
5 — Kennisgeving	Onbepaald / Gewist	Normale maar significante toestand
6 — Informatief	—	Alleen informatief bericht
7 — Foutopsporing	—	Alleen foutopsporingsuitvoer

Vervoeropties

ACI ondersteunt drie transportprotocollen voor remote syslog:

- UDP (standaard) — Beschikbaar in alle APIC-releases. Standaard brand-en-vergeet levering.
- TCP — Beschikbaar vanaf APIC-versie 5.2(3) en hoger. Biedt betrouwbare levering met aansluitingsgericht transport.
- SSL — Beschikbaar vanaf APIC versie 5.2(4) en hoger. Biedt versleuteld transport met behulp van TLS. Elke ACI-node (APIC of switch) fungeert als de TLS-client en initieert een uitgaande verbinding met de syslog-server. Het servercertificaat moet worden geüpload naar

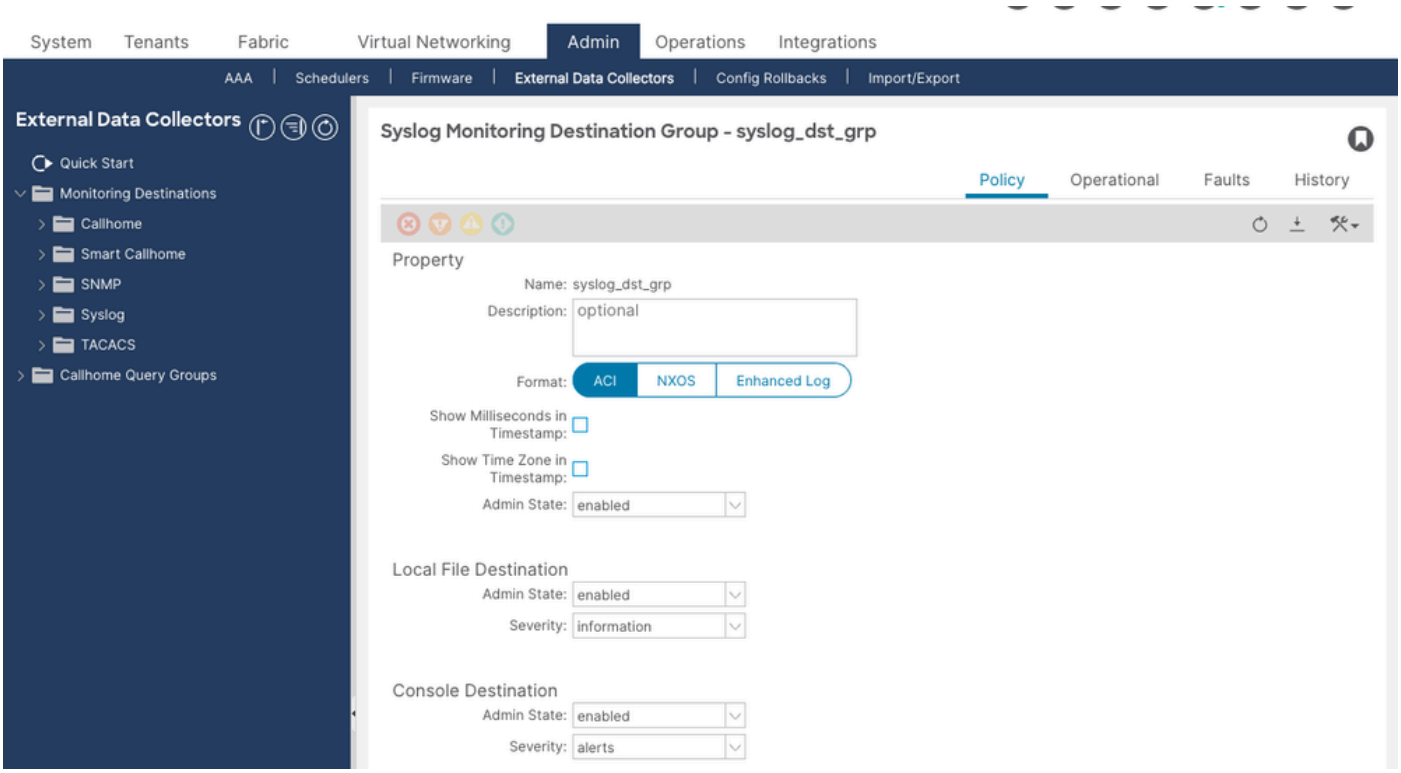
de APIC via Beheer > AAA > Beveiliging > Beheer openbare sleutel > Certificaatautoriteiten.

Opmerking: als een externe bestemming is geconfigureerd met SSL-transport en de APIC is gedegradeerd naar een release die geen SSL ondersteunt, wordt het transportprotocol automatisch teruggezet naar UDP. Zorg ervoor dat de syslog-server ook UDP-verbindingen kan accepteren als een fallback.

Configuratie

In de volgende stappen wordt de ACI-syslog van begin tot eind geconfigureerd. Voltooi alle stappen om syslog-doorsturen mogelijk te maken van zowel de APIC-controllers als de switches van het blad en de wervelkolom.

Stap 1: Maak de Syslog-bestemmingsgroep aan



De bestemmingsgroep bepaalt waar syslog-berichten worden verzonden en in welk formaat. Maak dit eerst aan, omdat de syslog-bronnen die in latere stappen zijn geconfigureerd, deze groep bij naam noemen.

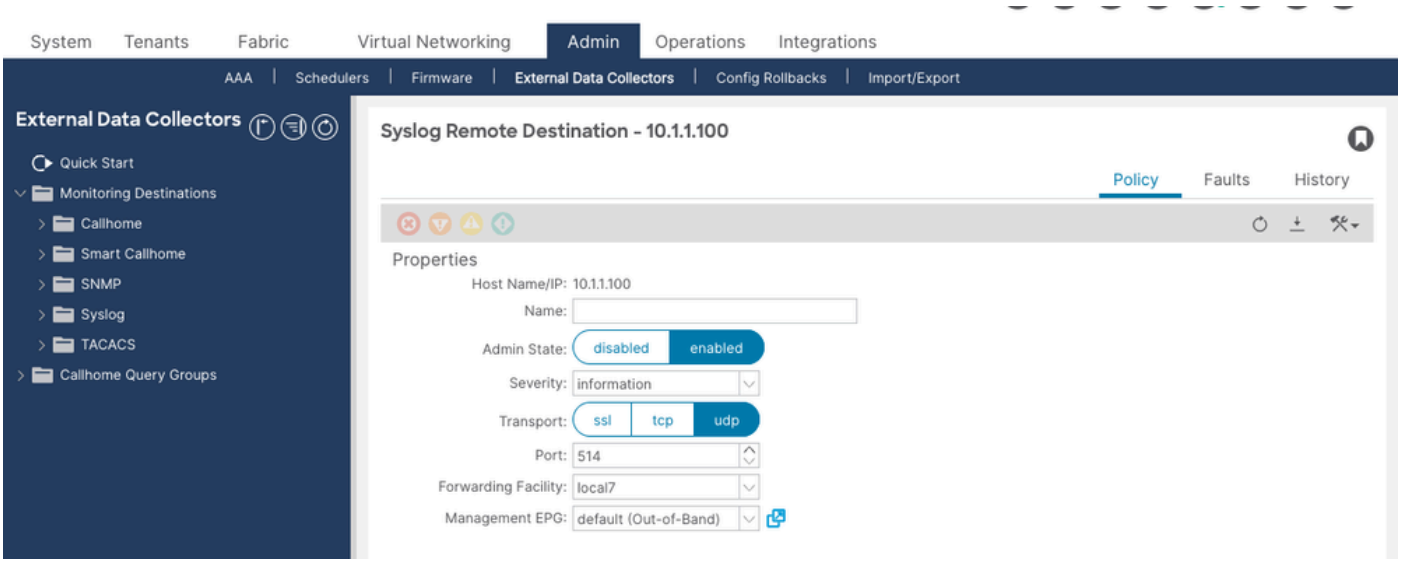
Navigeer naar Beheer > Externe gegevensverzamelaars > Bewaking van bestemmingen > Syslog. Klik met de rechtermuisknop op Syslog en selecteer Syslog Monitoring Destination Group maken.

Configureer in de wizard het volgende op de eerste pagina (groepsprofiel):

- Naam - Een beschrijvende naam zoals Syslog-Dest-Groupca.
- Formaat — aci (standaard, compatibel met RFC 3164) of nxosformaat.
- Administratieve staat — enabled.
- Beheerdersstatus voor lokale bestandsbestemming — enabled (aanbevolen). Dit schrijft berichten naar elke /var/log/external/messages fabric node en is essentieel voor lokale probleemoplossing, zelfs wanneer een externe server onbereikbaar is.
- Bestandsdoel voor lokaal gebruik — information.
- Console Bestemmingsstatus — disabled (aanbevolen voor productieomgevingen).

Klik op Next (Volgende). Klik op de tweede pagina op + in het gebied Externe bestemmingen maken om een externe syslog-server toe te voegen.

Stap 2: Een externe bestemming toevoegen



Configureer de externe syslog-server in het dialoogvenster Externe bestemming voor syslog maken:

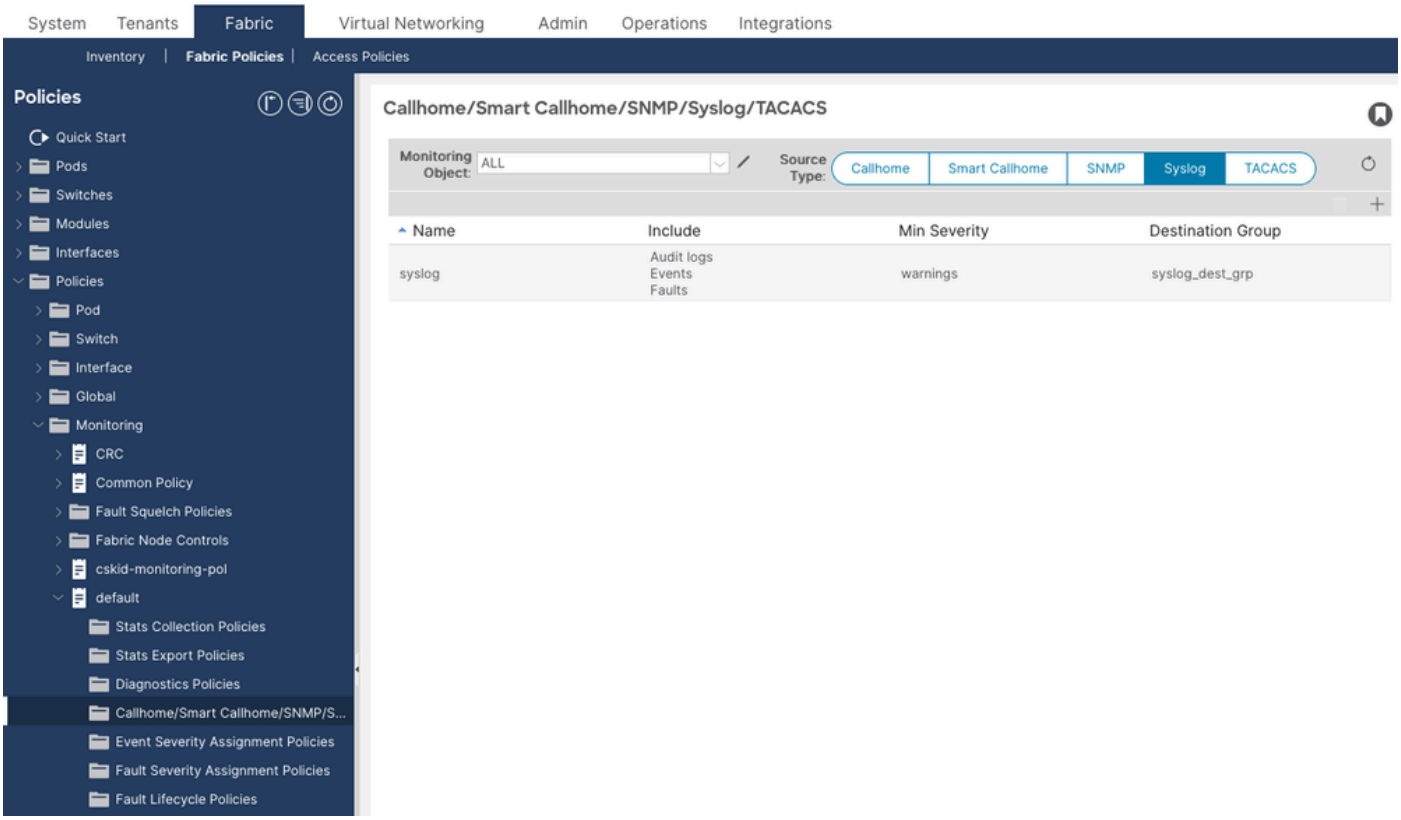
- Host — IP-adres van de syslog-server. Gebruik een IP-adres in plaats van een hostnaam. Als u een hostnaam gebruikt, moet u ervoor zorgen dat de DNS-server (Domain Name System) bereikbaar is via de out-of-band beheerinterface (OOB). DNS-servers die alleen bereikbaar zijn via in-band connectiviteit kunnen niet worden opgelost wanneer syslog-berichten worden gegenereerd tijdens een netwerkonderbreking.
- Administratieve staat — enabled.
- Ernst — information (aanbevolen). Dit is de minimale ernst die naar deze specifieke externe server wordt verzonden.
- Poort — 514 (standaard).

- Faciliteit — local7 (standaard). Stel dit in op de faciliteitswaarde die uw syslog-server kan accepteren en routeren.
- Vervoer — udp (standaard). Gebruik tcp voor betrouwbare levering (vereist APIC 5.2(3) of later), of voor versleuteld transport (vereist APIC 5.2(4) of later en een certificaat ssl dat is geüpload naar de APIC).
- EPG-beheer — Selecteer de EPG-beheer die toegankelijk is voor de syslog-server. Voor OOB-beheer: uni/tn-mgmt/mgmtp-default/oob-default. Voor in-band beheer selecteert u de juiste in-band EPG. Dit veld mag niet leeg zijn.

Klik op OK en vervolgens op Voltooien.

Opmerking: u kunt meerdere externe bestemmingen toevoegen aan dezelfde bestemmingsgroep. Elke bestemming kan een andere prioriteitsdrempel, faciliteit en transportprotocol hebben.

Stap 3: Maak een Syslog-bron aan onder het beleid voor fabrieksbewaking



Met deze stap wordt syslog geconfigureerd voor de hiërarchie van het fabric-object: fabric-poorten, kaarten, chassisonderdelen en ventilatorladen. Dit vormt een aanvulling op het gemeenschappelijk monitoringbeleid (stap 4) met een hiërarchische specifieke controle.

Navigeer naar Fabric > Fabric Policies > Policies > Monitoring > default > Callhome/Smart

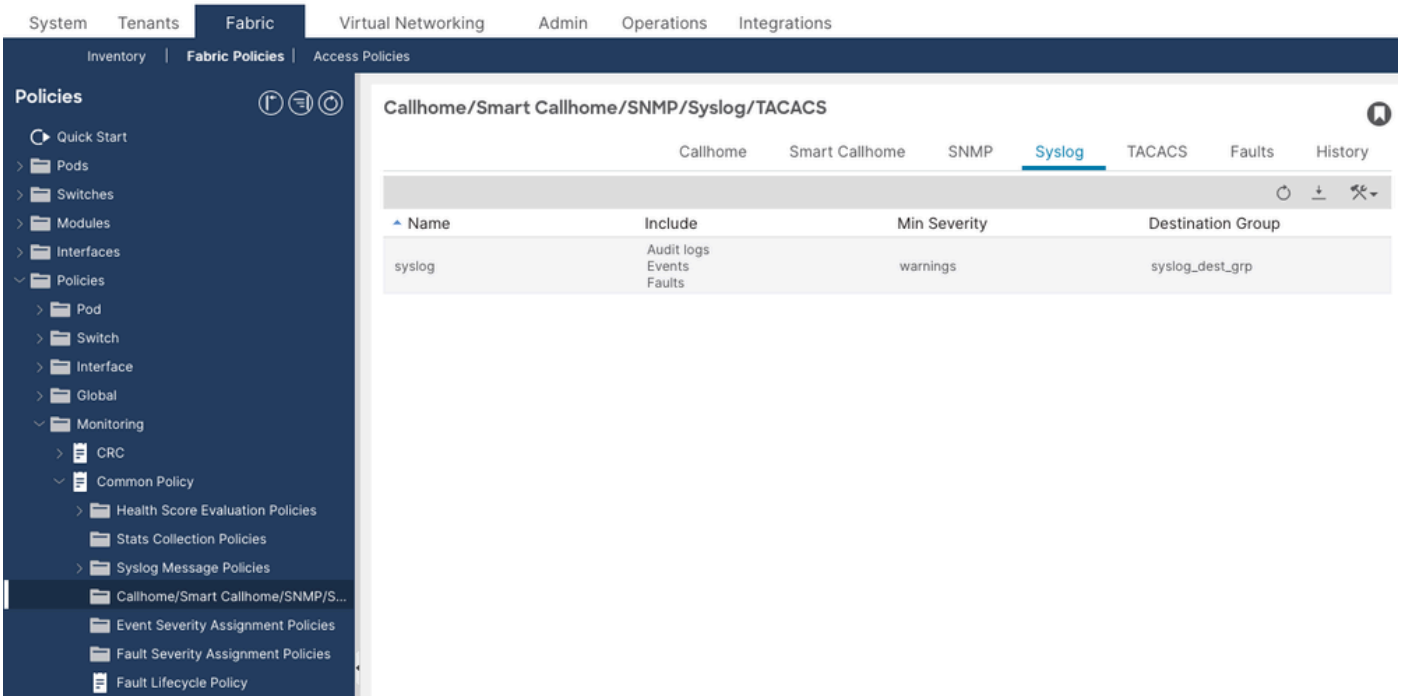
Callhome/SNMP/Syslog/TACACS.

Stel in het rechterdeelvenster het brontype in op syslog. Klik + om een syslog-bron te maken:

- Naam - Een beschrijvende naam zoals Syslog-Source-Fabricca.
- Minimale ernst — information (aanbevolen voor volledige dekking).
- Opnemen — Controle van audit, gebeurtenissen en fouten. Optioneel sessie toevoegen voor aanmeldings- en afmeldingsgebeurtenissen.
- Groep verwijderen — Selecteer de bestemmingsgroep die is gemaakt in stap 1.

Klik op Indienen.

Stap 4: Configureer het gemeenschappelijk monitoringbeleid (Systeembrede syslog)

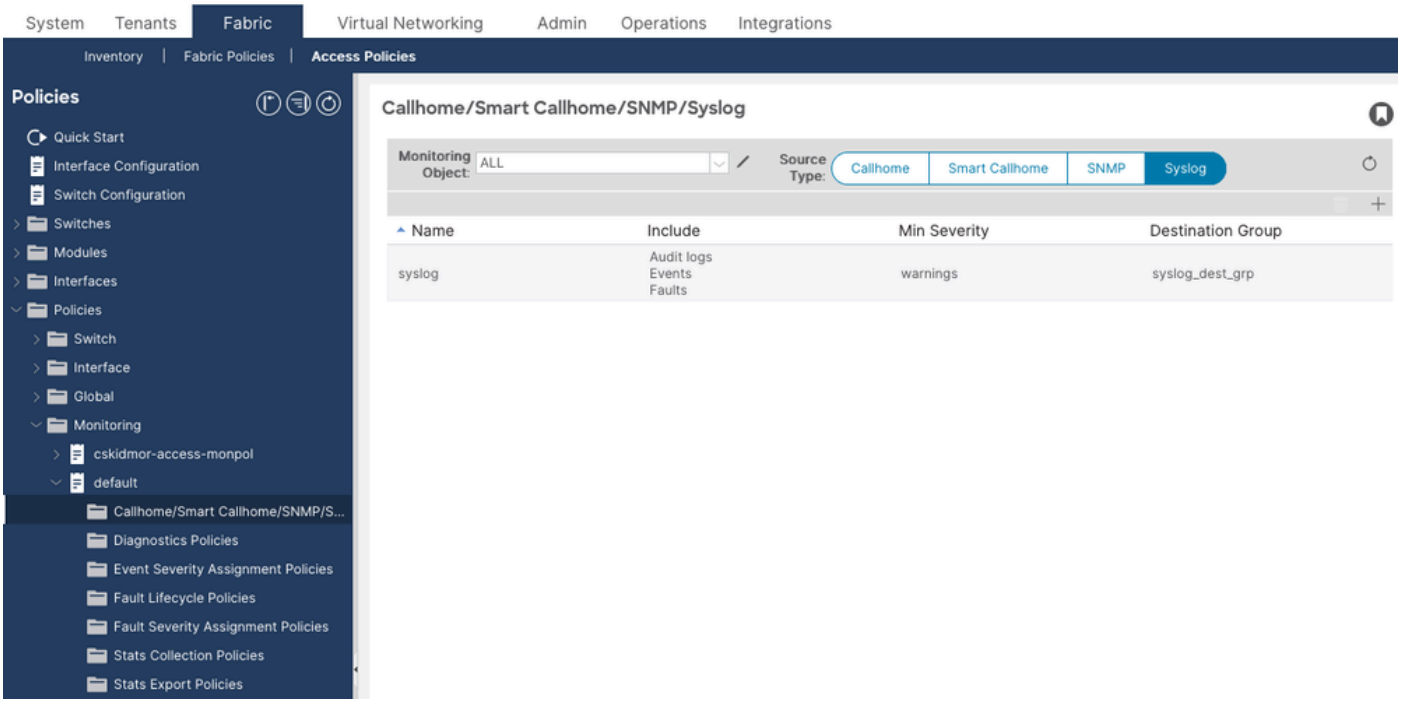


Het gemeenschappelijk monitoringbeleid biedt systeembrede syslog-dekking die automatisch wordt geïmplementeerd op alle knooppunten en controllers in de fabric. Deze stap koppelt de syslog-bron van het systeem aan de bestemmingsgroep.

Navigeer naar Fabric > Fabric Policies > Policies > Monitoring > Common Policy. Koppel onder de sectie Syslog de systeemsyslog-bron aan de bestemmingsgroep die is gemaakt in stap 1.

De Syslog-bron van het Common Policy-systeem gebruikt de MO syslogRsSystemDestGroup bij uni/fabric/moncommon/systemslsrc/rssystemDestGroupDN.

Stap 5: Maak een Syslog-bron aan onder het toegangscontrolebeleid



Met deze stap wordt syslog geconfigureerd voor de hiërarchie van het toegangsobject: toegangspoorten, Fabric Extender-apparaten (FEX-apparaten) en gebeurtenissen in de VM-controller (virtuele machine). Dit vormt een aanvulling op het gemeenschappelijk monitoringbeleid (stap 4) met een hiërarchische specifieke controle.

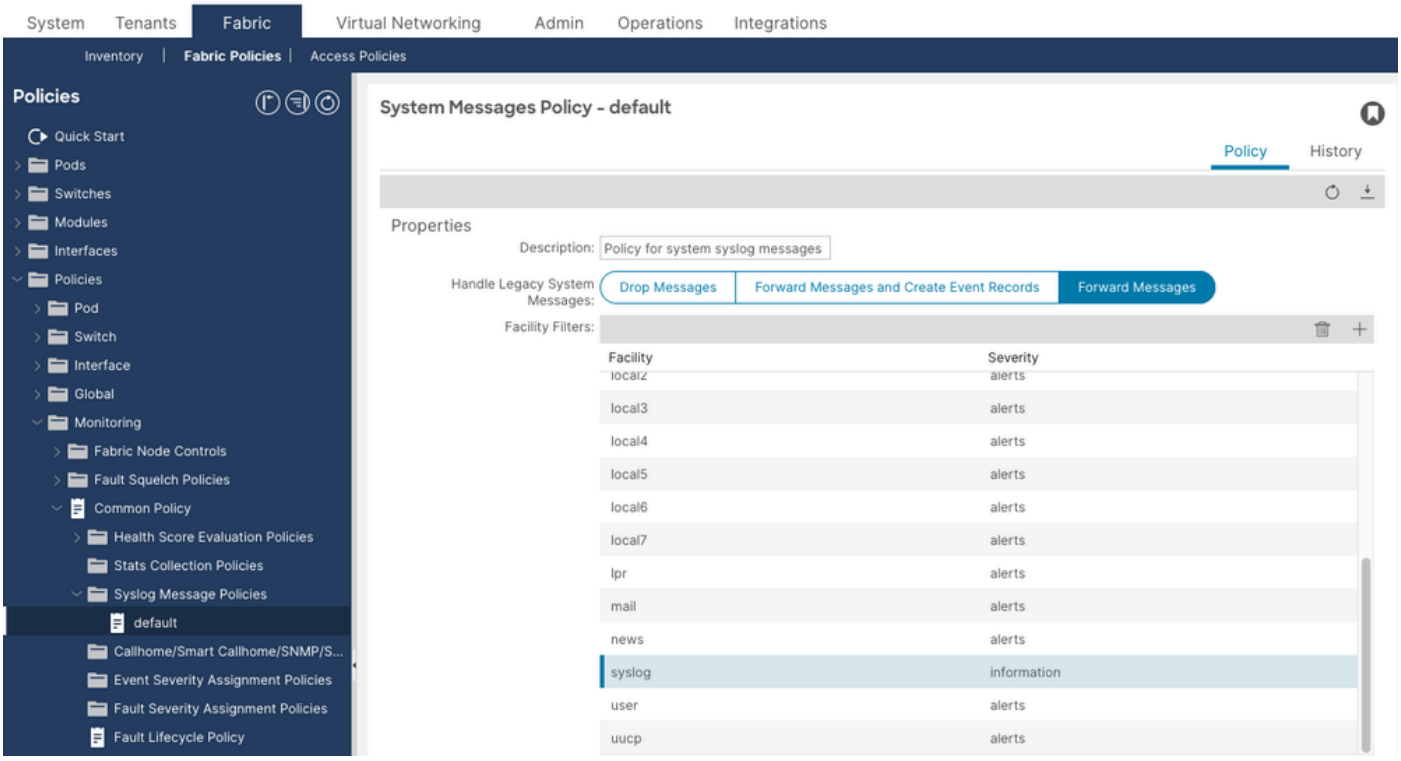
Navigeer naar Fabric > Toegangsbeleid > Beleid > Controlebeleid > Standaard > Callhome/SNMP/Syslog.

Stel het brontype in op Syslog. Klik + en configureer dezelfde instellingen als in stap 3:

- Naam, bijvoorbeeld Syslog-Source-Accessca.
- Minimale ernst — information.
- Opnemen — Controle van audit, gebeurtenissen en fouten.
- Desinfecteergroep — Selecteer dezelfde bestemmingsgroep.

Klik op Indienen.

Stap 6 (optioneel): pas het Syslog-berichtenbeleid voor ACL-logboekregistratie aan



Als u een contract ACL-vergunning nodig hebt of pakketlogboeken (ACLLOG_PKTLOG_PERMIT / ACLLOG_PKTLOG_DENY) wilt weigeren om op de externe syslog-server te worden weergegeven, moet het syslog-berichtenfaciliteitsfilter worden ingesteld op informatieve ernst.

Navigeer naar Fabric > Fabric Policies > Policies > Monitoring > Common Policy > Syslog Message Policies > default. Selecteer in de lijst met faciliteitsfilters de syslog-faciliteit en stel de Min. ernst in op informationinstelbaar. Dit is de syslogFacilityFilter MO bij uni/fabric/moncommon/sysmsgp/ff-syslogDN.

Opmerking: Als u ACL-machtigingen en -weigeringslogboeken wilt gebruiken om de externe syslog-server te bereiken, moet aan vier voorwaarden worden voldaan: (1) de syslog-bron `minSev-informatie moet bevatten, (2) de ernst van de externe bestemming moet informatie zijn, (3) het Syslog-berichtenbeleid syslog-faciliteitsfilter minSev moet informatie bevatten en (4) de` Log-richtlijn moet zijn ingeschakeld op de contractfiltervermelding. Wanneer aan alle drie de voorwaarden is voldaan, komen ACL-logberichten van de switch van het blad (niet van de APIC), zodat ze eerst in `/var/log/external/berichten` op het blad verschijnen. Contract ACL-pakketlogboeksnelheden zijn beperkt door CoPP: ontken logs standaard tot 500 pakketten per seconde (pps) en sta logs standaard toe tot 300 pps per blad.

Opmerking: het gebruik van de logboekrichtlijn voor filters in beheercontracten wordt niet ondersteund en veroorzaakt een fout bij de implementatie van de zoneringsregel. Contractregistratie alleen toepassen op contracten voor huurdersdata-plane.

De configuratie verifiëren

Controleer de configuratie voordat u operationele problemen oplost. De meest voorkomende hoofdoorzaak van ontbrekende syslog-berichten is een verkeerde configuratie, geen netwerk- of softwarefout.

Controleer de bestemmingsgroep en het profiel

Voer **moquery -c syslogGroup** de APIC uit om te bevestigen dat er doelgroepen bestaan en controleer hun kenmerken:

```
<#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
```

Controleer vervolgens het profiel (beheerdersstatus op groepsniveau) met **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
```

Om een doelgroep te vinden waarvan het profiel is uitgeschakeld, voert u het volgende uit:

<#root>

```
apic1#

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

Een resultaat hier betekent dat de bestemmingsgroep geen syslog-verkeer doorstuurt, ongeacht de beheerdersstatus van de externe bestemming.

Verifieer de externe bestemming

Uitvoeren **moquery -c syslogRemoteDest** om elke configuratie van de externe server te controleren:

<#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
```

Drie attributen vereisen speciale aandacht:

- adminState: moet enabledzijn. Als deze optie is uitgeschakeld, ontvangt deze specifieke externe server niets.
- epgDn: mag niet leeg zijn. Een lege epgDn verbinding betekent dat de verbinding niet weet van welke interface syslog-verkeer moet worden verzonden, dus er verlaten geen berichten de verbinding.
- operState: onbekend: deze waarde wordt verwacht en geeft geen probleem aan. ACI onderzoekt syslog-servers niet actief op bereikbaarheid.

Controleer de Syslog-bronnen

Uitvoeren **moquery -c syslogSrc** om te bevestigen dat bronnen bestaan onder het juiste controlebeleid:

```
<#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
```

Bevestig dat er bronnen bestaan onder het juiste monitoringbeleid:

- Een bron onder uni/fabric/moncommon — het gemeenschappelijk monitoringbeleid, voor dekking van alle knooppunten en alle objecthiërarchieën voor de gehele structuur.
- Een bron onder uni/infra/moninfra-default — het beleid voor de bewaking van verbindingen, voor objecten op weefselniveau (weefselpoorten, kaarten, chassis).
- Een bron onder uni/fabric/monfab-default — het beleid voor toegangsbewaking, voor objecten op toegangsniveau (toegangspoorten, FEX, VM-controllers).

Controleer ook of het systeem voor gemeenschappelijk monitoringbeleid syslog-bron is gekoppeld:

```
<#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
```

Als de ACL-logboekregistratie van het contract vereist is, controleert u de ernst van het Syslog Message Policy-filter met **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
```

Verifieer het lokale logbestand

/var/log/external/messages Het lokale bestand in is de meest directe manier om te bevestigen dat syslog-berichten worden gegenereerd op elke fabric-node, zelfs wanneer een externe server niet bereikbaar is. Controleer het op zowel de APIC als een 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
```

Als dit bestand leeg is of niet wordt bijgewerkt op een node, worden er geen berichten gegenereerd aan de bron. Als het bestand inhoud heeft, maar de externe syslog-server geen berichten ontvangt, is het probleem bij het doorsturen (bestemmingsgroep, netwerk of firewall), niet bij het genereren van berichten.

Bereikbaarheid van de Syslog-server controleren

Voer een ping uit van de APIC naar de syslog-server om de IP-bereikbaarheid via het beheernetwerk te controleren:

```
<#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
```

Gebruik `piping` met de switch `-V` om de VRF aan te geven, vanaf een blad of de ruggengraat. Gebruik `beheer` voor out-of-band of `management:inb` voor in-band, afhankelijk van welke beheer-EPG is toegewezen aan de syslog-bestemming:

```
<#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
```

Een succesvolle ping bevestigt de bereikbaarheid van IP, maar bevestigt niet dat UDP- of TCP-

poort 514 is toegestaan. Internet Control Message Protocol (ICMP) en syslog gebruiken verschillende protocollen.

Probleemoplossing

Triage-workflow

Gebruik de volgende beslisboom wanneer syslog-berichten niet aankomen op de externe server:

```
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
```

Gemeenschappelijke scenario's

Scenario 1: Geen Syslog-berichten ontvangen op externe server

Probleem: De syslog-bestemmingsgroep en externe bestemming zijn geconfigureerd, maar er komen geen berichten op de externe server. Het lokale bestand /var/log/external/messages op de APIC en switches bevat recente vermeldingen.

Configuratiecontrole:

<#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
```

Hoofdoorzaak: De beheerdersstatus van de externe bestemming is disabledgewijzigd. Dit kan gebeuren als de bestemming is gemaakt maar per ongeluk uitgeschakeld is gebleven, of als deze tijdens onderhoud is uitgeschakeld en nooit opnieuw is ingeschakeld.

Oplossing: Navigeer naar Beheer > Externe gegevensverzamelaars > Controle van bestemmingen > Syslog > [groepsnaam] > Externe bestemmingen > [server]. Bewerk de externe bestemming en stel de beheerdersstatus in op ingeschakeld.

Scenario 2: Syslog-doelgroepprofiel is uitgeschakeld

Probleem: er worden geen berichten doorgestuurd vanaf een node, ook al is de beheerdersstatus van de externe bestemming ingeschakeld.

Configuratiecontrole:

<#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
```

Hoofdoorzaak: De syslogProf beheerdersstatus bepaalt de gehele bestemmingsgroep. Wanneer het is uitgeschakeld, worden er geen berichten doorgestuurd vanaf een node, ongeacht de individuele externe bestemmingsstatus.

Oplossing: Navigeer naar Beheer > Externe gegevensverzamelaars > Bewakingsbestemmingen > Syslog > [groepsnaam]. Bewerk het profiel en stel de beheerdersstatus in op Ingeschakeld.

Scenario 3: ontbrekende gebeurtenissen — gemeenschappelijk monitoringbeleid niet gekoppeld

Probleem: Syslog-berichten van sommige knooppunten of objecthiërarchieën bereiken de externe server niet, hoewel een syslog-bron is geconfigureerd onder het beleid voor controle van verbindingen of toegang.

Configuratiecontrole:

<#root>

```
apic1#

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

Total Objects shown: 0
```

Het Syslog-bronsysteem van het gemeenschappelijk toezichtsbeleid is niet gekoppeld aan de bestemmingsgroep.

Hoofdoorzaak: het gemeenschappelijk monitoringbeleid (uni/fabric/moncommonCommon Monitoring Policy) biedt dekking voor de hele structuur van syslog in alle hiërarchieën en wordt automatisch geïmplementeerd in alle knooppunten en controllers. Zonder deze optie worden alleen gebeurtenissen doorgestuurd die overeenkomen met de specifieke hiërarchieën van de structuur of het toegangscontrolebeleid. Het structuurbewakingsbeleid (uni/infra/moninfra-defaultFabric Monitoring Policy) heeft betrekking op objecten op weefselniveau en het toegangsbewakingsbeleid (Access Monitoring Policyuni/fabric/monfab-default) heeft betrekking op objecten op toegangsniveau, maar biedt geen van beide de dekking op weefselniveau die het gemeenschappelijk beleid biedt.

Oplossing: Navigeer naar Fabric > Fabric Policies > Policies > Monitoring > Common Policy. Koppel onder de sectie Syslog de systeemsyslog-bron aan de bestemmingsgroep. Verifieer met

moquery -d uni/fabric/moncommon/systemslsrc/rssystemDestGroup dat het object tDn naar uw bestemmingsgroep wijst.

Scenario 4: Te restrictieve ernst — Verwachte berichten ontbreken

Probleem: sommige berichten komen op de syslog-server aan, maar er ontbreken informatiegebeurtenissen, logboekvermeldingen voor audits of gebeurtenissen voor het aanmelden voor sessies. Er worden alleen kritieke en grote fouten gezien.

Configuratiecontrole:

<#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
```

Hoofdoorzaak: Syslog-filtering vindt plaats op twee punten: de bron (minSev) en de externe bestemming (severity). Alleen berichten die beide filters passeren worden doorgestuurd. Als een van beide hierboven is informationingesteld, worden informatieve berichten verwijderd.

Oplossing: bewerk de syslog-bron en stel Min. ernst in op informatie, en controleer audit, gebeurtenissen, fouten in het veld Opnemen. Bewerk de externe bestemming en stel de prioriteit in op informatie.

Scenario 5: Geen EPG-beheer toegewezen aan externe bestemming

Probleem: er worden geen syslog-berichten ontvangen op de externe server. De bestemmingsgroep is ingeschakeld, de externe bestemming is ingeschakeld en het lokale logbestand bevat inhoud.

Configuratiecontrole:

<#root>

```
apic1#

moquery -c syslogRemoteDest

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

Root Cause: Zonder een Management EPG weten de APIC en switches niet welke fysieke interface ze moeten gebruiken om syslog-berichten te verzenden. Berichten worden gegenereerd, maar kunnen niet worden doorgestuurd.

Oplossing: Bewerk de externe bestemming en selecteer de juiste EPG voor beheer. Voor OOB-beheer selecteert uni/tn-mgmt/mgmtp-default/oob-defaultu. Voor in-band beheer selecteert u de juiste in-band EPG.

Scenario 6: Wrong Management EPG (In-Band vs Out-of-Band)

Probleem: Syslog-berichten komen af en toe of alleen van sommige knooppunten. De syslog-server is alleen bereikbaar via OOB-beheer, maar de externe bestemming verwijst naar de in-band EPG.

Configuratiecontrole:

<#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
```

Als de syslog-server alleen bereikbaar is via het OOB-netwerk, resulteert de in-band EPG in berichten die afkomstig zijn van de in-band-interface, die de server niet kan bereiken.

Oplossing: Bewerk de externe bestemming en wijzig de beheer-EPG in uni/tn-mgmt/mgmtp-default/oob-defaultBewerken. Verifieer met **ping -c 3 10.1.1.100** vanuit de APIC-bash om de bereikbaarheid van OOB te bevestigen.

Scenario 7: Firewall blokkeert Syslog-verkeer

Probleem: het lokale logbestand bevat inhoud op zowel APIC- als bladknooppunten, de configuratie is correct, ICMP-ping naar de syslog-server is geslaagd, maar er komen geen berichten op de server aan.

Operationele controle: Voer een ping uit van de APIC naar de syslog-server om de IP-bereikbaarheid te controleren:

<#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 slaagt, maar syslog-berichten komen niet aan. ICMP (ping) gaat door terwijl UDP-poort 514 wordt geblokkeerd.

Hoofdoorzaak: een firewall of ACL tussen het beheernetwerk en de syslog-server blokkeert UDP-poort 514 (of TCP 514 als TCP-transport is geconfigureerd). ICMP en UDP zijn onafhankelijk — het doorgeven van ICMP bevestigt niet dat UDP 514 is toegestaan. Bovendien stuurt elk blad en elke ruggengraat syslog rechtstreeks vanaf zijn eigen OOB IP-adres. Een firewall die alleen de APIC OOB IP's toestaat, laat syslog-pakketten vallen die afkomstig zijn van switch-knooppunten.

Oplossing: Controleer of de firewall UDP/TCP-poort 514 toestaat vanuit het OOB IP-adresbereik van alle knooppunten van de stof — inclusief alle APIC's, alle switches van bladeren en alle switches van de wervelkolom. Een pakketopname op de syslog-server bevestigt of UDP 514-pakketten aankomen.

Scenario 8: Contract ACL-vergunning / Deny-logs komen niet aan

Probleem: Contract permit of deny packet logs (ACLLOG_PKTLOG_PERMIT/ ACLLOG_PKTLOG_DENY) komen niet aan op de syslog server.

Configuratiecontrole:

1. Controleer of de bronernst van de syslog informationals volgt is:
   <#root>

   ```
   apic1#

   moquery -c syslogSrc

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

2. Controleer of de ernst van de externe bestemming informationis:
   <#root>

   ```
   apic1#

   moquery -c syslogRemoteDest

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

3. Controleer of de ernst van het Syslog Message Policy-filter informationals volgt is:
   <#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. Controleer of de logboekrichtlijn is ingeschakeld in het contractfilter. Navigeer naar Huurders > [tenant] > Contracten > [contract] > Onderwerpen > [subject] > Filters en bevestig dat de kolom Richtlijnen log toont voor de relevante filtervermelding.
5. Controleer of er ACL-logs worden gegenereerd op de switch van het blad (ACL-logs zijn afkomstig van het blad, niet van de APIC):
   <#root>

   ```
   leaf1#

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

<#root>

leaf1#

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

Als er geen ACLLOG vermeldingen worden weergegeven, wordt met de logrichtlijn geen logboekgeneratie op het blad geactiveerd. Dit kan wijzen op een verkeerd geconfigureerde contractrichtlijn, dat geen overeenkomend verkeer het contract raakt of dat CoPP-tariefbeperking pakketten laat vallen voordat ze worden geregistreerd.

Hoofdoorzaak: Contract ACL log prioriteitsniveau is informational (syslog niveau 6). Als een filter in de syslog-keten - bron minSev, externe bestemming severityof het Syslog Message Policy-filter (syslogFacilityFilter bij uni/fabric/moncommon/sysmsgp/ff-syslog) - hierboven is ingesteld, worden de ACL-logboekberichten stilletjes weggelaten voordat ze de fabric-node verlaten information.

Oplossing: Instellen minSev op information op de syslog-bron, instellen severity op information op de externe bestemming, het syslog faciliteitsfilter instellen minSev op information onder Gemeenschappelijk beleid > Syslog Berichtbeleid > standaard, bevestigen dat de logboekrichtlijn is ingeschakeld op het contractfilter en controleren of de firewall het syslog-verkeer toestaat vanaf de OB IP-adressen van de leaf-switch , niet alleen de APIC IP's, omdat ACL-logs worden verzonden vanaf de switch.

Scenario 9: Syslog stopt na het hernoemen van de bestemmingsgroep

Probleem: Syslog-berichten komen niet meer aan op de externe server nadat de naam van de bestemmingsgroep van syslog is gewijzigd. Het veranderen van de haven of faciliteit veroorzaakt dit probleem niet. Als u het beleid uitschakelt en opnieuw inschakelt, wordt de berichtlevering niet hervat.

Root Cause: Dit is een bekend softwarefout. Zie Cisco bug ID CSCwj23752. Het hernoemen van de bestemmingsgroep breekt de interne syslog forwarding associatie. Het is vastgelegd in APIC versie 6.0(6) en hoger.

Oplossing: Upgrade naar APIC versie 6.0(6c) of hoger. Als een tijdelijke oplossing voor getroffen versies, verwijdert u de hernoemde bestemmingsgroep en maakt u deze opnieuw met de gewenste naam en koppelt u de syslog-bronnen opnieuw.

Scenario 10: Overmatige syslog veroorzaakt APIC GUI traagheid

Probleem: de APIC GUI wordt traag en het APIC CPU-gebruik is hoog. Dit kan gebeuren wanneer de ACL-logboekregistratie van het contract is ingeschakeld tijdens normale bewerkingen, waardoor een groot volume aan informatieve syslog-berichten wordt gegenereerd die worden

geconverteerd naar eventRecord objecten in de APIC-database.

Hoofdoorzaak: wanneer de ernst van het gemeenschappelijk beleidssyslog-berichtenbeleid is ingesteld op informationSyslog, genereert elk informatief syslog-bericht — inclusief ACL-logs met een hoog volume — een eventRecord fout in de APIC. Dit kan de APIC-database overweldigen en vertraging van de GUI veroorzaken.

Oplossing:

- Schakel ACL-logboekregistratie uit tijdens normale bewerkingen. Schakel het alleen in tijdens het oplossen van problemen of tijdens onderhoudsvensters.
- Als ACL-logboekregistratie ingeschakeld moet blijven, stelt u de ernst van het Syslog-berichtenbeleid in op alerts Fabric > Fabric Policies > Policies > Monitoring > Common Policy > Syslog Message Policies > default. Dit voorkomt dat informatieve syslog-berichten worden geconverteerd naar gebeurtenissen, terwijl ze nog steeds kunnen worden doorgestuurd naar de externe syslog-server.
- Ruis wegnemen van gebeurteniscodes die niet operationeel bruikbaar zijn. Een gebeurteniscode kan worden gesquelched om te voorkomen dat deze gebeurtenisrecords genereert zonder het doorsturen van syslog te beïnvloeden.

Bekende bugs

De volgende bekende softwaredefecten hebben invloed op de functionaliteit van de ACI-syslog:

- Cisco bug ID CSCwj23752 — De syslog-bestemmingsgroep hernoemen stopt de syslog-levering. Vast in APIC versie 6.0(6c) en hoger.

Escalatiecriteria

Verzamel technische ondersteuning en schakel Cisco TAC in wanneer:

- Syslog-berichten worden lokaal weergegeven in /var/log/external/messages enabledfabric-knooppunten, de bestemmingsgroep en de beheerdersstatus voor externe bestemmingen zijn beide, de beheer-EPG is correct, de bereikbaarheid van het netwerk is bevestigd (ping- en firewallcontrolepas), maar berichten komen nog steeds niet aan op de externe server.
- Syslog-berichten komen van sommige fabric-knooppunten, maar niet van andere, zonder verschil in configuratie tussen deze knooppunten, wat wijst op een inconsistentie in beleidsimplementatie.
- Het doelgroepprofiel of de externe bestemming is opnieuw ingeschakeld, maar berichten worden niet binnen enkele minuten na de configuratiewijziging hervat.

- Syslog-berichten kwamen niet meer aan na een APIC-upgrade, wat wijst op een mogelijk softwaredefect.

Gegevens die moeten worden verzameld voordat een TAC-zaak wordt geopend:

- On-demand technische ondersteuning van de getroffen APIC en één getroffen bladknooppunt.
- Uitvoer van `moquery -c syslogGroup`, `moquery -c syslogProf`, `moquery -c syslogRemoteDest`en `moquery -c syslogSrc` van de APIC.
- Output van `moquery -d uni/fabric/moncommon/systemslsrc/rssystemDestGroup` de controle van de koppeling met het gemeenschappelijk beleid.
- Staart van `/var/log/external/messages` zowel een APIC als een aangedaan blad.
- Packet capture van de syslog-server om te bevestigen of UDP/TCP 514-pakketten afkomstig zijn van fabric-OOB-adressen.

Referenties

- Cisco APIC Basic Configuration Guide, versie 6.1(x) — Beheer
- Naslaggids voor Cisco ACI-systeemberichten
- Cisco ACI Faults, Events, and System Messages Management Guide
- Cisco ACI-contractgids — Whitepaper
- Problemen met een trage APIC-GUI oplossen

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.