ACI에서 Syslog 구성 및 문제 해결

소개

이 문서에서는 Cisco ACI(Application Centric Infrastructure)에서 시스템 로깅(syslog)을 구성, 확인 및 트러블슈팅하는 방법에 대해 설명합니다. 전체 컨피그레이션 워크플로, APIC(Application Policy Infrastructure Controller) MO(Managed-Object) 모델을 사용한 프로그래밍 방식 확인, APIC 컨트롤러와 리프 및 스파인 스위치 모두에 대한 구조화된 트러블슈팅 워크플로를 다룹니다.

개요

ACI syslog는 전적으로 정책 기반 독립형 Cisco NX-OS® 소프트웨어와 달리 ACI 리프 또는 스파인 스위치에는 **logging server** CLI 명령이 없습니다. 모든 syslog 컨피그레이션은 APIC가 모든 패브릭 노드에 자동으로 푸시하는 APIC 정책을 통해 수행됩니다.

주요 구성 요소

ACI의 syslog 하위 시스템은 다음과 같은 관리 객체로 구축됩니다.

- Syslog Destination Group (syslogGroup) — 모든 syslog 대상에 대한 최상위 컨테이너입니다. 메시지 형식(ACI 또는 NX-OS 스타일) 및 타임스탬프 옵션을 제어합니다. 하나 이상의 원격 대상, 로컬 파일 대상 및 콘솔 대상을 포함할 수 있습니다.
- Syslog 프로파일(syslogProf) — 그룹 레벨 관리 상태 및 전송 프로토콜(UDP, TCP 또는 SSL)을 제어하는 대상 그룹의 하위 항목입니다.
- Syslog Remote Destination (syslogRemoteDest) — 하나의 원격 syslog 서버를 나타내는 대상 그룹의 하위 항목입니다. 서버 IP 또는 호스트 이름, 포트, 심각도 필터, syslog 기능, 서버에 연결하는 데 사용되는 EPG(Management Endpoint Group)를 제어합니다.
- Syslog 로컬 파일(syslogFile) — 각 패브릭 노드의 로컬 파일에 syslog 메시지를 쓰는 것을 제어하는 대상 그룹/var/log/external/messages의 하위 항목입니다.
- Syslog 소스(syslogSrc) — 모니터링 정책에 연결됩니다. 어떤 메시지 유형(감사, 이벤트, 결함, 세션)과 최소 심각도를 전송할지, 관계를 통해 대상 그룹에 대한 링크를 syslogRsDestGroup 제어합니다.

Syslog 소스 첨부 지점

ACI는 syslog 메시지를 생성하는 노드 및 객체를 제어하는 네 가지 모니터링 정책 범위를 사용합니다.

- 공통 모니터링 정책(monCommonPol, uni/fabric/moncommon) — 패브릭 전반의 범위. 모든 장애 및 이벤트에 적용되고 패브릭의 모든 노드(리프 및 스파인 스위치) 및 모든 컨트롤러(APIC)에 자동으로 구축되는 기본 모니터링 정책입니다. 모든 패브릭, 액세스 및 테넌트 계층 구조에 대해 다룹니다. Fabric(패브릭) > Fabric Policies(패브릭 정책) > Policies(정책) > Monitoring(모니터링) > Common Policy(공통 정책)에서 확인할 수 있습니다.
- 패브릭 모니터링 정책(monInfraPol, uni/infra/moninfra-default) — 패브릭 범위. 패브릭 레벨 개체에 대한 syslog를 생성합니다. 패브릭 포트, 카드, 섀시 구성 요소 및 팬 트레이. Fabric(패브릭) > Fabric Policies(패브릭 정책) > Policies(정책) > Monitoring(모니터링) > default(기본값)에서 확인할 수 있습니다.
- 액세스 모니터링 정책(monFabricPol, uni/fabric/monfab-default) - 액세스(인프라) 범위. 액세스 연결 구성 요소에 대한 syslog를 생성합니다. 액세스 포트, FEX(Fabric Extender) 디바이스 및 VM(가상 머신) 컨트롤러 이벤트 Fabric(패브릭) > Access Policies(액세스 정책) > Policies(정책) > Monitoring Policies(모니터링 정책) > default(기본값)에서 확인할 수 있습니다.
- 테넌트 모니터링 정책(monEPGPol, uni/tn-common/monepg-default) — 테넌트 범위. 테넌트 범위 개체에 대한 syslog를 생성합니다. 엔드포인트 그룹(EPG), 애플리케이션 프로파일 및 서비스 [Tenant] > Monitoring Policies(모니터링 정책) > default(기본값)의 각 테넌트 아래에 있습니다.

참고: Common Monitoring Policy(공통 모니터링 정책)는 모든 계층 전반에 걸쳐 패브릭 전반의 커버리지를 제공하며 모든 노드에 자동으로 구축되기 때문에 syslog 컨피그레이션을 시작하는 것이 좋습니다. 패브릭 및 액세스 모니터링 정책은 특정 객체 계층에 대한 보다 세분화된 제어를 위해 공통 정책 외에 또는 syslog를 더 좁은 범위로 제한하기 위해 공통 정책 대신 구성할 수 있습니다.

Syslog 메시지 형식

그룹 형식이 aci로 설정된 경우 ACI syslog 메시지는 RFC 3164 형식을 따릅니다(기본값).

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

예를 들면 다음과 같습니다.

```
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
```

메시지 본문에는 ACI 결함 코드, 라이프사이클 상태(예: soaking, retaining, cleared), 심각도 및 영향을 받는 객체의 DN(Distinguished Name)이 포함되어 있으며, 이를 통해 메시지를 자체 기술할 수 있습니다.

세 가지 메시지 형식 옵션을 사용할 수 있습니다.

- aci(기본값) — RFC 3164 호환 형식. 대부분의 구축에 권장.
- nxos — NX-OS 스타일 형식 syslog 플랫폼에 NX-OS 형식의 메시지가 필요한 경우 이 옵션을 사용합니다.
- Enhanced Log(APIC 5.2(8) 이상) — 연도를 포함하는 향상된 타임스탬프가 포함된 RFC 5424 호환 형식.

심각도 매핑

syslog 심각도 필드는 0(가장 심각)부터 7(가장 심각)까지의 한 자릿수입니다. 다음 표는 syslog 심각도 수준과 ACI/ITU(International Telecommunication Union) 심각도 용어 간의 매핑을 보여줍니다 .

Syslog 심각도	ACI/ITU 레벨	설명
0 — 긴급	—	시스템을 사용할 수 없음
1 - 경고	Critical(심각)	즉각적인 조치 필요
2 - 중요	Major(중요)	위험 조건
3 — 오류	Minor(경미)	오류 상태
4 — 경고	경고	경고 조건
5 - 알림	미결정/지워짐	정상이지만 중요한 상태
6 - 정보	—	정보 메시지만
7 — 디버깅	—	디버그 출력만

전송 옵션

ACI는 원격 syslog에 대해 세 가지 전송 프로토콜을 지원합니다.

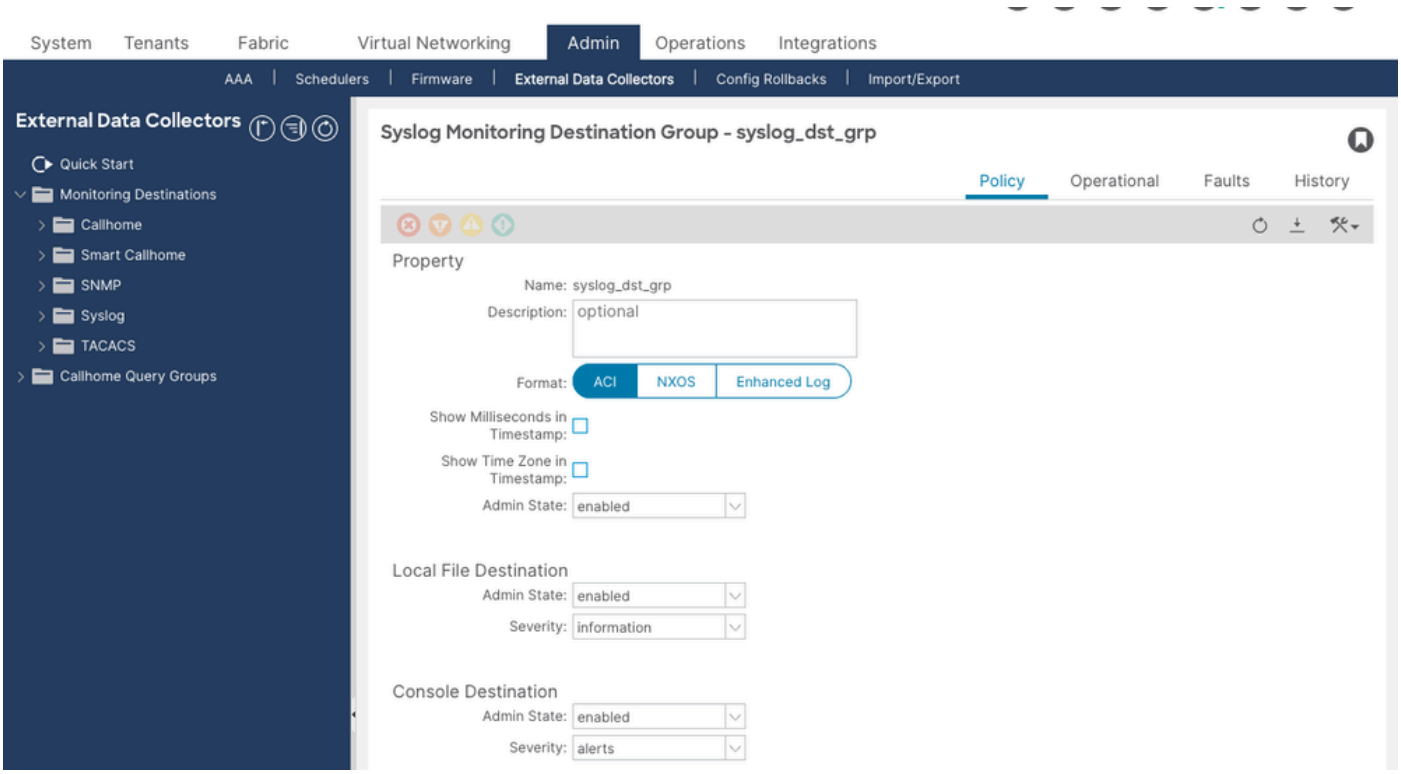
- UDP(기본값) — 모든 APIC 릴리스에서 사용 가능합니다. 표준 화재 방지 배송.
- TCP — APIC 릴리스 5.2(3) 이상에서 사용 가능합니다. 연결 지향 전송을 통해 안정적으로 전달합니다.
- SSL — APIC 릴리스 5.2(4) 이상에서 사용 가능합니다. TLS를 사용하여 암호화된 전송을 제공합니다. 각 ACI 노드(APIC 또는 스위치)는 TLS 클라이언트 역할을 하며 syslog 서버에 대한 아웃바운드 연결을 시작합니다. 서버 인증서는 Admin(관리) > AAA(AAA) > Security(보안) > Public Key Management(공개 키 관리) > Certificate Authorities(인증 기관)에서 APIC에 업로드해야 합니다.

참고: 원격 대상이 SSL 전송으로 구성되어 있고 APIC가 SSL을 지원하지 않는 릴리스로 다운그레이드된 경우 전송 프로토콜은 자동으로 UDP로 되돌아갑니다. syslog 서버가 UDP 연결도 대안으로 수락할 수 있는지 확인합니다.

설정

다음 단계에서는 ACI syslog를 처음부터 끝까지 구성합니다. APIC 컨트롤러와 리프 및 스파인 스위치에서 syslog 포워딩을 활성화하려면 모든 단계를 완료합니다.

1단계: Syslog 대상 그룹 생성



대상 그룹은 syslog 메시지가 전송되는 위치와 형식을 정의합니다. 이후 단계에서 구성된 syslog 소스가 이 그룹을 이름으로 참조하므로 먼저 이 그룹을 생성합니다.

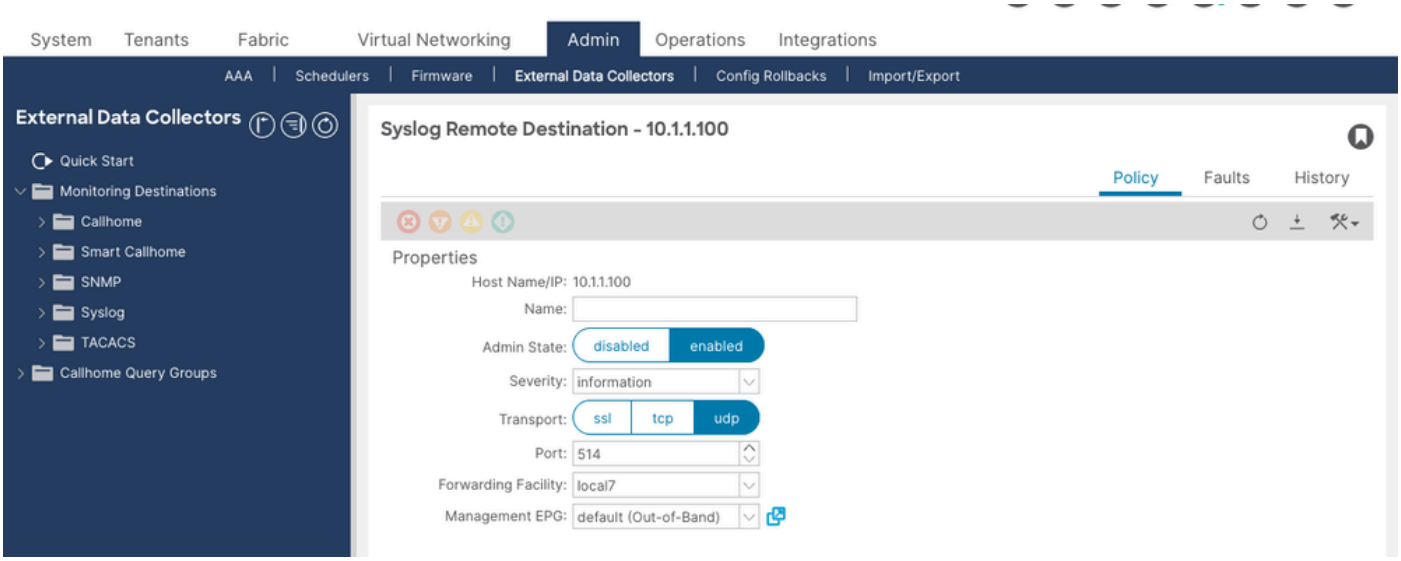
Admin(관리) > External Data Collectors(외부 데이터 수집기) > Monitoring Destinations(모니터링 대상) > Syslog로 이동합니다. Syslog를 마우스 오른쪽 버튼으로 클릭하고 Create Syslog Monitoring Destination Group(Syslog 모니터링 대상 그룹 생성)을 선택합니다.

마법사에서 첫 번째 페이지(그룹 프로필)에서 다음을 구성합니다.

- 이름 — 를 설명하는 Syslog-Dest-Group이름입니다.
- 형식 — aci (기본값, RFC 3164 호환) 또는 nxos입니다.
- 관리 상태 — enabled.
- Local File Destination Admin State — enabled (권장) 이렇게 하면 모든 패브릭 노드 /var/log/external/messages에 메시지가 기록되며 원격 서버에 연결할 수 없는 경우에도 로컬 트러블슈팅에 필수적입니다.
- 로컬 파일 대상 심각도 — information.
- Console Destination Admin State — disabled (프로덕션 환경에 권장)

Next(다음)를 클릭합니다. 두 번째 페이지에서 Create Remote Destinations(원격 대상 생성) 영역에서 +를 클릭하여 원격 syslog 서버를 추가합니다.

2단계: 원격 대상 추가



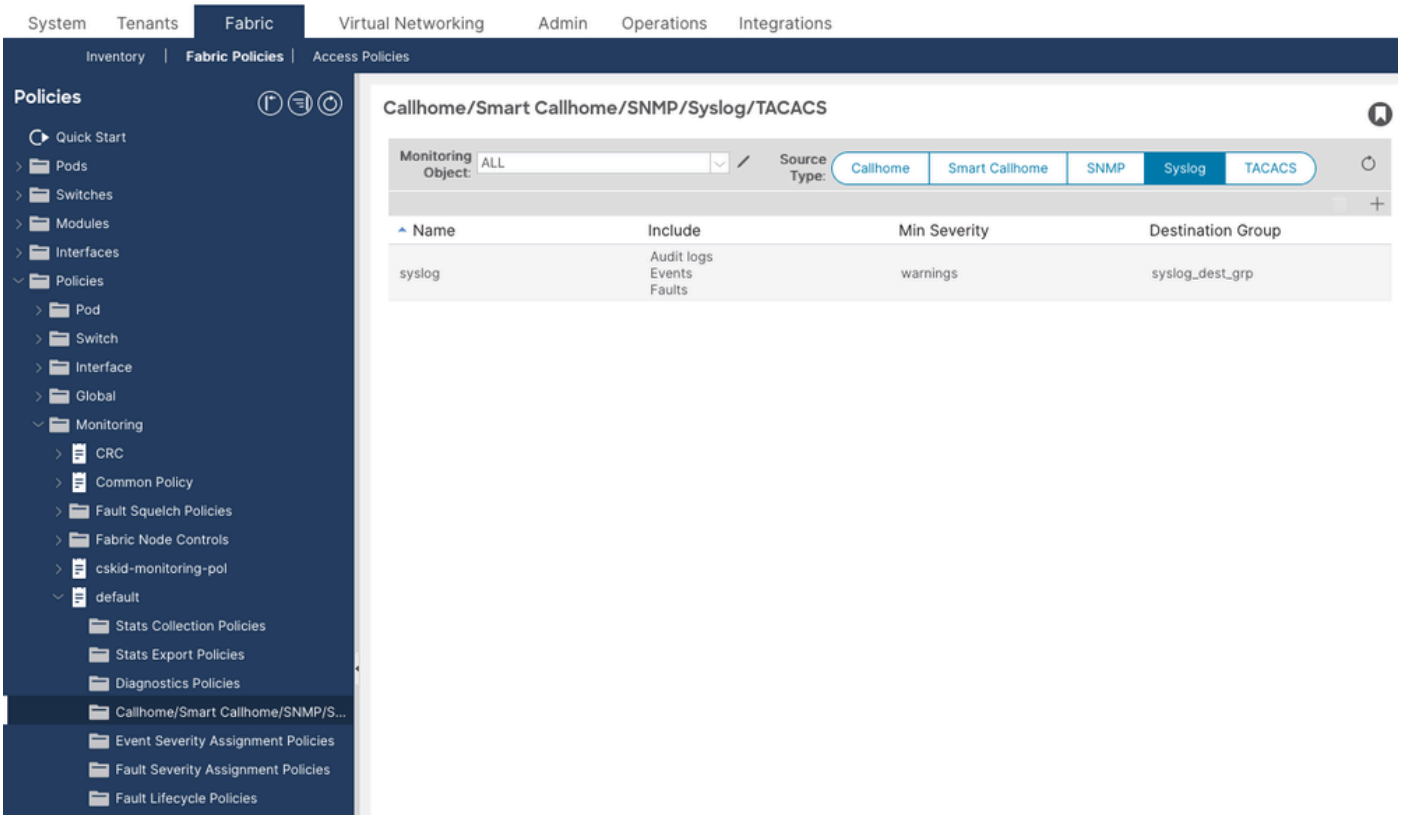
Create Syslog Remote Destination(Syslog 원격 대상 생성) 대화 상자에서 원격 syslog 서버를 구성합니다.

- 호스트 — syslog 서버의 IP 주소입니다. 호스트 이름 대신 IP 주소를 사용합니다. 호스트 이름을 사용하는 경우 OOB(Out-of-Band) 관리 인터페이스를 통해 DNS(Domain Name System) 서버에 연결할 수 있는지 확인해야 합니다. 대역 내 연결을 통해서만 연결할 수 있는 DNS 서버는 네트워크 중단 중에 syslog 메시지가 생성될 때 확인하지 못할 수 있습니다.
- 관리 상태 — enabled.
- 심각도 — information (권장). 이는 이 특정 원격 서버로 전송된 최소 심각도입니다.
- 포트 — 514 (기본값).
- 기능 — local7 (기본값). 이 값을 syslog 서버가 수락 및 라우팅하도록 구성된 기능 값과 일치하도록 설정합니다.
- 전송 — udp (기본값). 신뢰할 수 tcp 있는 전달(APIC 5.2(3) 이상 필요) 또는 암호화된 전달(APIC 5.2(4) 이상 및 APIC에 업로드된 인증서 필요)에 ssl 사용합니다.
- Management EPG — syslog 서버에 연결할 수 있는 관리 EPG를 선택합니다. OOB 관리의 경우: uni/tn-mgmt/mgmtp-default/oob-default. 대역 내 관리에서 적절한 대역 내 EPG를 선택합니다. 이 필드는 비워둘 수 없습니다.

OK(확인), Finish(마침)를 차례로 클릭합니다.

✎ 참고: 동일한 대상 그룹에 여러 원격 대상을 추가할 수 있습니다. 각 목적지는 서로 다른 심각도 임계값, 시설, 전송 프로토콜을 가질 수 있습니다.

3단계: 패브릭 모니터링 정책에서 Syslog 소스 생성



이 단계에서는 패브릭 포트, 카드, 섀시 구성 요소 및 팬 트레이와 같은 패브릭 객체 계층 구조에 대해 syslog를 구성합니다. 이는 계층별 제어로 공통 모니터링 정책(4단계)을 보완합니다.

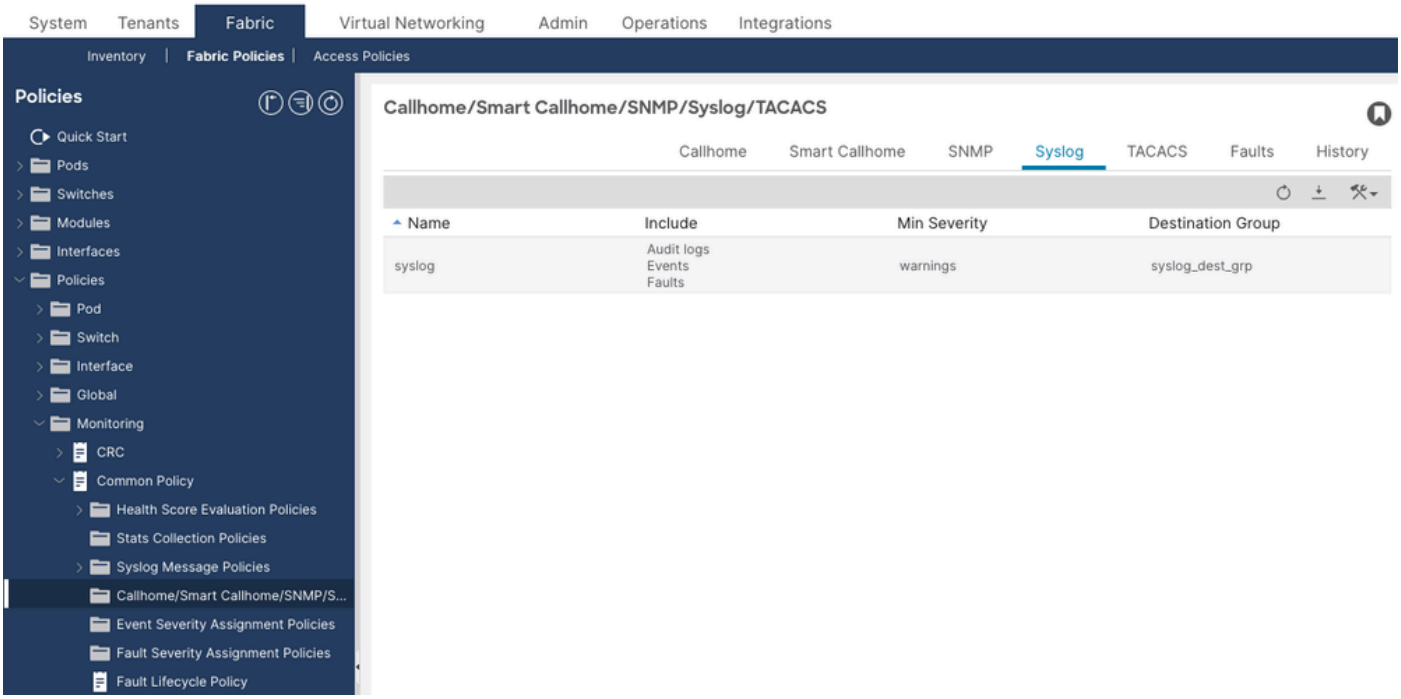
Fabric(패브릭) > Fabric Policies(패브릭 정책) > Policies(정책) > Monitoring(모니터링) > default(기본값) > Callhome/Smart Callhome/SNMP/Syslog/TACACS로 이동합니다.

오른쪽 창에서 Source Type(소스 유형)을 Syslog로 설정합니다. Syslog 소스를 생성하려면 +를 클릭합니다.

- 이름 — 를 설명하는 Syslog-Source-Fabric이름입니다.
- Min Severity — information (전체 커버리지에 권장).
- 포함 — 감사, 이벤트 및 결함을 확인합니다. 선택적으로 로그인 및 로그아웃 이벤트에 대한 세션을 추가합니다.
- 대상 그룹 — 1단계에서 생성한 대상 그룹을 선택합니다.

Submit(제출)을 클릭합니다.

4단계: 공통 모니터링 정책 구성(시스템 전체 Syslog)

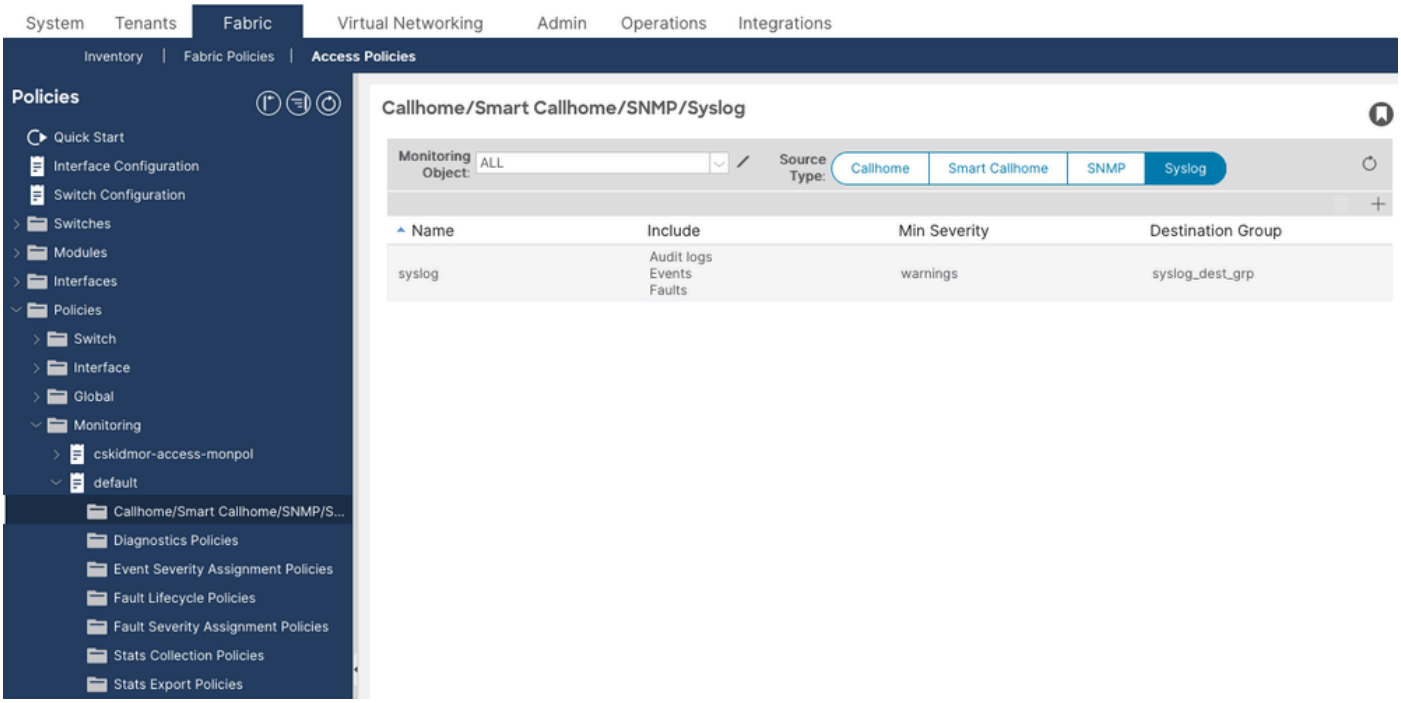


공통 모니터링 정책은 패브릭의 모든 노드 및 컨트롤러에 자동으로 구축되는 시스템 전체의 syslog 범위를 제공합니다. 이 단계에서는 시스템 syslog 소스를 대상 그룹에 연결합니다.

Fabric(패브릭) > Fabric Policies(패브릭 정책) > Policies(정책) > Monitoring(모니터링) > Common Policy(공통 정책)로 이동합니다. Syslog 섹션에서 시스템 syslog 소스를 1단계에서 생성한 대상 그룹에 연결합니다.

공통 정책 시스템 syslog 소스는 DN에서 MO를 syslogRsSystemDestGroup 사용합니다 uni/fabric/moncommon/systemslsrc/rssystemDestGroup.

5단계: 액세스 모니터링 정책에서 Syslog 소스 생성



이 단계에서는 액세스 객체 계층(액세스 포트, FEX(Fabric Extender) 디바이스, VM(가상 머신) 컨트롤러 이벤트)에 대해 syslog를 구성합니다. 이는 계층별 제어로 공통 모니터링 정책(4단계)을 보완합니다.

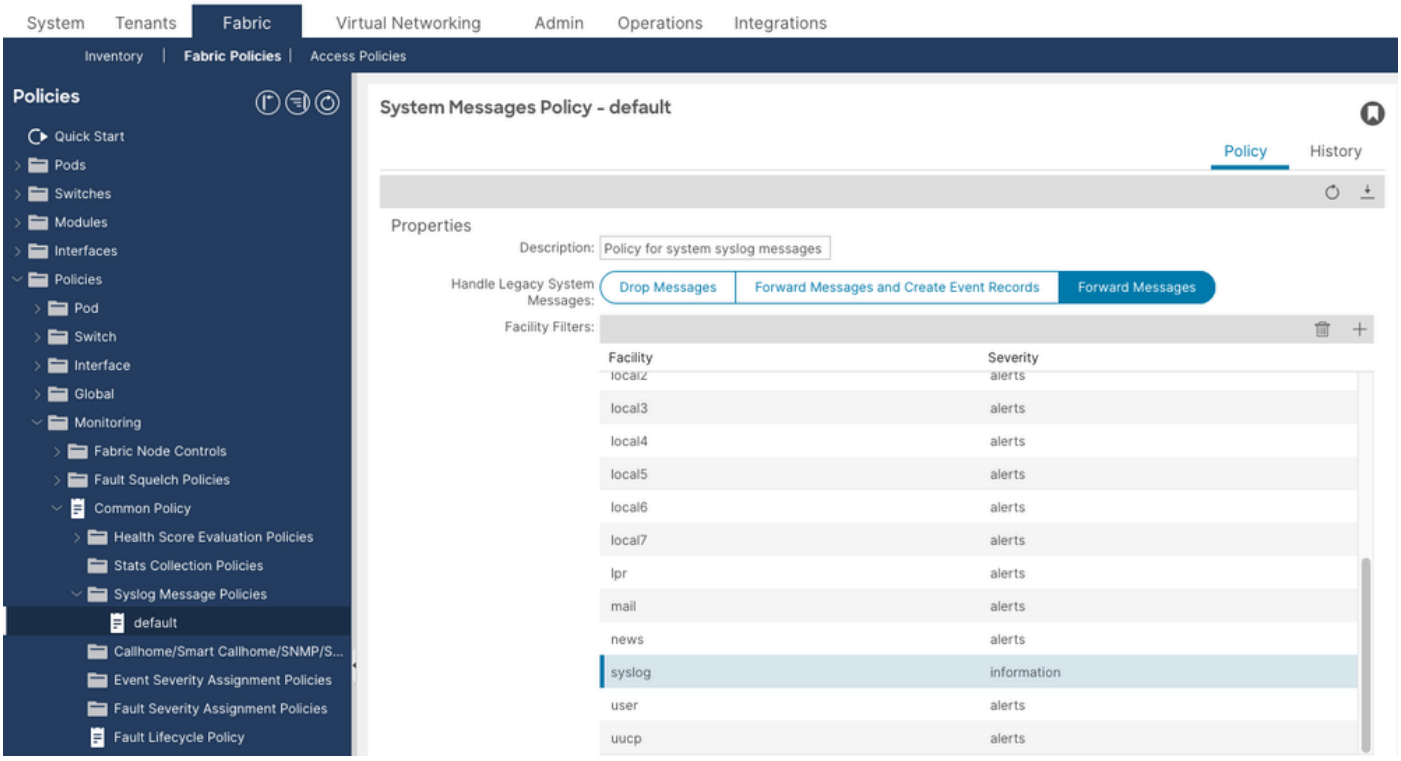
Fabric(패브릭) > Access Policies(액세스 정책) > Policies(정책) > Monitoring Policies(모니터링 정책) > default(기본값) > Callhome/SNMP/Syslog로 이동합니다.

Source Type(소스 유형)을 Syslog로 설정합니다. +를 클릭하고 3단계와 동일한 설정을 구성합니다.

- 이름 — 예: Syslog-Source-Access입니다.
- 최소 심각도 — information.
- 포함 — 감사, 이벤트 및 결함을 확인합니다.
- 대상 그룹 — 동일한 대상 그룹을 선택합니다.

Submit(제출)을 클릭합니다.

6단계(선택 사항): 계약 ACL 로깅에 대한 Syslog 메시지 정책 조정



원격 syslog 서버에 계약 ACL 허용 또는 거부 패킷 로그(ACLLOG_PKTLOG_PERMIT / ACLLOG_PKTLOG_DENY)가 나타나도록 하려면 syslog 메시지 기능 필터를 정보 심각도로 설정해야 합니다.

Fabric(패브릭) > Fabric Policies(패브릭 정책) > Policies(정책) > Monitoring(모니터링) > Common Policy(공통 정책) > Syslog Message Policies(Syslog 메시지 정책) > default(기본값)로 이동합니다. Facility filter(기능 필터) 목록에서 syslog 기능을 선택하고 Min Severity(최소 심각도)를 information설정합니다. DN의 syslogFacilityFilter MO입니다uni/fabric/moncommon/sysmsgp/ff-syslog.

참고: 계약 ACL 허용 및 거부 로그가 원격 syslog 서버에 도달하려면 다음 네 가지 조건이 모두 충족되어야 합니다. (1) syslog 소스 minSev는 정보여야 하고, (2) 원격 대상 심각도는 정보여야 하며, (3) Syslog 메시지 정책 syslog 기능 필터 minSev는 정보여야 하고, (4) LogDirective는 계약 필터 항목에서 활성화되어야 합니다. 이 세 가지 조건이 모두 충족되면 ACL 로그 메시지는 APIC이 아닌 leaf 스위치에서 시작하므로 leaf의 `/var/log/external/messages`에 먼저 나타납니다. 계약 ACL 패킷 로그 속도는 CoPP에 의해 제한됩니다. deny logs는 기본적으로 500pps(packets per second)이고 permit logs는 기본적으로 leaf당 300pps입니다.

참고: 관리 계약의 필터에 Log 지시어를 사용하는 것은 지원되지 않으며 조닝 규칙 구축 실패를 유발합니다. 테넌트 데이터 플레인 계약에만 계약 로깅을 적용합니다.

구성 확인

운영 문제를 트러블슈팅하기 전에 컨피그레이션을 확인합니다. syslog 메시지가 누락되는 가장 일반적인 근본 원인은 네트워크 또는 소프트웨어 결함이 아니라 컨피그레이션 잘못입니다.

대상 그룹 및 프로필 확인

대상 그룹**moquery -c syslogGroup**이 존재하는지 확인하고 해당 특성을 확인하기 위해 APIC에서 실행합니다.

<#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
```

그런 다음 프로파일(그룹 레벨 관리자 상태)을 다음과 같이 **moquery -c syslogProf**확인합니다.

<#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
```

프로필이 비활성화된 대상 그룹을 찾으려면 다음을 실행합니다.

<#root>

```
apic1#
```

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

따라서 대상 그룹이 원격 대상 관리자 상태와 상관없이 어떤 syslog 트래픽도 전달하지 않습니다.

원격 대상 확인

실행**moquery -c syslogRemoteDest**을 실행하여 각 원격 서버 컨피그레이션을 확인합니다.

<#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
```

다음과 같은 세 가지 특성에 각별한 주의가 필요합니다.

- 관리자 상태: 이어야 합니다enabled. 비활성화하면 이 특정 원격 서버에 아무것도 수신되지 않습니다.
- epgDn: 비워둘 수 없습니다. 공백은 epgDn 패브릭이 어떤 인터페이스에서 syslog 트래픽을 전송할지 모르기 때문에 패브릭 외부로 전송되는 메시지가 없음을 의미합니다.
- 작동 상태: 알 수 없음: 이 값은 예상되며 문제를 나타내지 않습니다. ACI는 syslog 서버에 연결할 수 있는지 적극적으로 조사하지 않습니다.

Syslog 소스 확인

실행**moquery -c syslogSrc**을 실행하여 소스가 올바른 모니터링 정책에 있는지 확인합니다.

<#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
```

소스가 적절한 모니터링 정책에 있는지 확인합니다.

- 모든 노드 uni/fabric/moncommon 및 모든 객체 계층의 패브릭 전반에서 적용할 수 있는 공통 모니터링 정책의 소스.
- 아래의 소스 uni/infra/moninfra-default — 패브릭 레벨 객체(패브릭 포트, 카드, 섀시)에 대한 패브릭 모니터링 정책.
- 액세스 레벨 uni/fabric/monfab-default 객체(액세스 포트, FEX, VM 컨트롤러)에 대한 액세스 모니터링 정책 아래의 소스.

또한 공통 모니터링 정책 시스템 syslog 소스가 연결되었는지 확인합니다.

```
<#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
```

계약 ACL 로깅이 필요한 경우 Syslog Message Policy 기능 필터 심각도를 다음과 같이 **moquery -d uni/fabric/moncommon/sysmsgp/ff-syslog**확인합니다.

```
<#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
```

로컬 로그 파일 확인

의 로컬 파일/var/log/external/messages은 원격 서버에 연결할 수 없는 경우에도 어떤 패브릭 노드에서도 syslog 메시지가 생성되고 있는지 확인하는 가장 직접적인 방법입니다. APIC 및 leaf 스위치에서 모두 확인합니다.

<#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
```

이 파일이 비어 있거나 노드에서 업데이트되지 않으면 소스에서 메시지가 생성되지 않습니다. 파일에 컨텐트가 있지만 원격 syslog 서버가 메시지를 수신하지 않는 경우, 메시지 생성이 아니라 전달(대상 그룹, 네트워크 또는 방화벽)에 문제가 있습니다.

Syslog 서버에 대한 연결 확인

APIC에서 syslog 서버로 ping을 실행하여 관리 네트워크를 통한 IP 연결성을 확인합니다.

<#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
```

리프 또는 스파인 스위치에서 -V 플래그가 포함된 iping을 사용하여 VRF를 지정합니다. syslog 대상에 할당된 관리 EPG에 따라 대역 외 관리 또는 대역 내 관리:inb를 사용합니다.

<#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
```

성공적인 ping은 IP 연결성을 확인하지만 UDP 또는 TCP 포트 514가 허용되는지 확인하지는 않습니다. ICMP(Internet Control Message Protocol)와 syslog는 서로 다른 프로토콜을 사용합니다.

문제 해결

분류 워크플로

syslog 메시지가 원격 서버에 도착하지 않을 경우 다음 진단트리를 사용합니다.

```
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
```

일반적인 시나리오

시나리오 1: 원격 서버에서 수신된 Syslog 메시지 없음

문제/장애: syslog 대상 그룹 및 원격 대상이 구성되었지만 원격 서버에 메시지가 도착하지 않습니다. APIC 및 스위치/var/log/external/messages의 로컬 파일에는 최근 항목이 들어 있습니다.

컨피그레이션 확인:

<#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
```

근본 원인: 원격 대상 관리자 상태는 입니다disabled. 이는 대상이 생성되었지만 실수로 비활성화된 상태로 남아 있거나, 유지 관리 중에 비활성화되었지만 다시 활성화되지 않은 경우 발생할 수 있습니다.

해결책: Admin(관리) > External Data Collectors(외부 데이터 수집기) > Monitoring Destinations(모니터링 대상) > Syslog > [group name] > Remote Destinations(원격 대상) > [server](서버)로 이동합니다. 원격 대상을 편집하고 Admin State(관리 상태)를 enabled(활성화됨)로 설정합니다.

시나리오 2: Syslog 대상 그룹 프로필이 비활성화되었습니다.

문제/장애: 원격 대상 관리 상태가 활성화되었더라도 어떤 노드에서도 메시지가 전달되지 않습니다.

컨피그레이션 확인:

<#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
```

근본 원인: 관리 syslogProf 상태는 전체 대상 그룹을 제어합니다. 비활성화되면 개별 원격 대상 상태에 관계없이 어떤 노드에서도 메시지가 전달되지 않습니다.

해결책: Admin(관리) > External Data Collectors(외부 데이터 수집기) > Monitoring Destinations(모니터링 대상) > Syslog > [group name](그룹 이름)으로 이동합니다. 프로필을 수정하고 Admin State(관리 상태)를 enabled(활성화됨)로 설정합니다.

시나리오 3: 누락된 이벤트 - 공통 모니터링 정책이 연결되지 않음

문제/장애: Syslog 소스가 패브릭 또는 액세스 모니터링 정책에 구성되어 있어도 일부 노드 또는 개체 계층의 Syslog 메시지가 원격 서버에 도달하지 않습니다.

컨피그레이션 확인:

<#root>

```
apic1#

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

Total Objects shown: 0
```

공통 모니터링 정책 시스템 syslog 소스가 대상 그룹에 연결되어 있지 않습니다.

근본 원인: 공통 모니터링 정책(uni/fabric/moncommon)은 모든 계층 전반에 걸쳐 패브릭 전반의 syslog 적용 범위를 제공하며 모든 노드 및 컨트롤러에 자동으로 구축됩니다. 이 명령이 없으면 특정 패브릭 또는 액세스 모니터링 정책 계층과 일치하는 이벤트만 전달됩니다. Fabric Monitoring Policy(uni/infra/moninfra-default)는 Fabric 레벨 object를, Access Monitoring Policy(uni/fabric/monfab-default)는 Access 레벨 object를 다루지만, Common Policy가 제공하는 Fabric 차원의 커버리지는 모두 제공하지 않습니다.

해결책: Fabric(패브릭) > Fabric Policies(패브릭 정책) > Policies(정책) > Monitoring(모니터링) > Common Policy(공통 정책)로 이동합니다. Syslog 섹션에서 시스템 syslog 소스를 대상 그룹에 연결합니다. 에서 **moquery -d uni/fabric/moncommon/systemslsrc/rssystemDestGroup** 가 대상 그룹을 tDn 가리키는지 확인합니다.

시나리오 4: 심각도가 너무 제한적임 - 필요한 메시지가 누락됨

문제/장애: 일부 메시지는 syslog 서버에 도착하지만 정보 이벤트, 감사 로그 항목 또는 세션 로그인 이벤트가 누락됩니다. 중대한 결함만 표시됩니다.

컨피그레이션 확인:

<#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
```

근본 원인: Syslog 필터링은 다음 두 지점에서 발생합니다. 소스(minSev) 및 원격 대상(severity)입니다. 두 필터를 모두 통과하는 메시지만 전달됩니다. 둘 중 하나가 위information에 설정된 경우 정보 메시지가 삭제됩니다.

해결책: syslog 소스를 편집하고 Min Severity(최소 심각도)를 정보로 설정하고 Include(포함) 필드에서 audit, events(이벤트), faults(결함)를 확인합니다. 원격 대상을 수정하고 심각도를 정보로 설정합니다.

시나리오 5: 원격 대상에 할당된 관리 EPG 없음

문제/장애: 원격 서버에서 syslog 메시지를 수신하지 않습니다. 대상 그룹이 활성화되고, 원격 대상이 활성화되며, 로컬 로그 파일에 내용이 있습니다.

컨피그레이션 확인:

<#root>

```
apic1#
```

moquery -c syslogRemoteDest

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

근본 원인: 관리 EPG가 없으면 APIC와 스위치는 syslog 메시지를 전송하기 위해 어떤 물리적 인터페이스를 사용해야 하는지 알지 못합니다. 메시지가 생성되지만 전달할 수 없습니다.

해결책: 원격 대상을 수정하고 적절한 관리 EPG를 선택합니다. OOB 관리에서 을 선택합니다uni/tn-mgmt/mgmtp-default/oob-default. 대역 내 관리에서 적절한 대역 내 EPG를 선택합니다.

시나리오 6: 잘못된 관리 EPG(대역 내/대역 외)

문제/장애: Syslog 메시지는 간헐적으로 도착하거나 일부 노드에서만 도착합니다. syslog 서버는 OOB 관리를 통해서만 연결할 수 있지만 원격 대상이 대역 내 EPG를 참조합니다.

컨피그레이션 확인:

```
<#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
```

OOB 네트워크를 통해서만 syslog 서버에 연결할 수 있는 경우 대역 내 EPG는 메시지가 대역 내 인터페이스에서 소싱되며 서버에 연결할 수 없게 됩니다.

해결책: 원격 대상을 수정하고 관리 EPG를 로 uni/tn-mgmt/mgmtp-default/oob-default변경합니다. APIC **ping -c 3 10.1.1.100** 베이스에서 를 확인하여 OOB 연결성을 확인합니다.

시나리오 7: 방화벽 차단 Syslog 트래픽

문제/장애: 로컬 로그 파일에는 APIC 및 리프 노드 모두에 콘텐츠가 있으며, 컨피그레이션이 올바르고, syslog 서버에 대한 ICMP ping이 성공하지만, 서버에 어떤 메시지도 도착하지 않습니다.

운영 확인: IP 연결성을 확인하기 위해 APIC에서 syslog 서버로 ping을 실행합니다.

```
<#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
```

Ping은 성공하지만 syslog 메시지는 도착하지 않습니다. UDP 포트 514가 차단된 상태에서 ICMP(ping)가 통과합니다.

근본 원인: 관리 네트워크와 syslog 서버 간의 방화벽 또는 ACL이 UDP 포트 514(또는 TCP 전송이 구성된 경우 TCP 514)를 차단하고 있습니다. ICMP 및 UDP는 독립적입니다. — ICMP 전달은 UDP 514가 허용됨을 확인하지 않습니다. 또한 각 leaf 및 spine은 자체 OOB IP 주소에서 직접 syslog를 전송합니다. APIC OOB IP만 허용하는 방화벽은 스위치 노드에서 시작되는 syslog 패킷을 삭제합니다.

해결책: 방화벽에서 모든 APIC, 모든 leaf 스위치, 모든 spine 스위치를 포함한 모든 패브릭 노드의 OOB IP 주소 범위에서 UDP/TCP 포트 514를 허용하는지 확인합니다. syslog 서버의 패킷 캡처는 UDP 514 패킷이 도착하는지 확인합니다.

시나리오 8: 계약 ACL 허용/거부 로그가 도착하지 않음

문제/장애: 계약 허용 또는 거부 패킷 로그(ACLLOG_PKTLOG_PERMIT / ACLLOG_PKTLOG_DENY)가 syslog 서버에 도착하지 않습니다.

컨피그레이션 확인:

1. syslog 소스 심각도가 다음과 같은지 information확인합니다.
   <#root>

   ```
   apic1#

   moquery -c syslogSrc

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

2. 원격 대상 심각도가 다음과 같은지 information확인합니다.
   <#root>

   ```
   apic1#

   moquery -c syslogRemoteDest

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

3. Syslog 메시지 정책 기능 필터 심각도가 다음과 같은지 information확인합니다.
   <#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. 계약 필터에서 log 지시어가 활성화되었는지 확인합니다. Tenants(테넌트) > [tenant](테넌트) > Contracts(계약) > [contract](계약) > Subjects(주체) > [subject] > Filters(필터)로 이동하고 Directives(지시어) 열에 관련 필터 항목에 대한 로그가 표시되는지 확인합니다.
5. ACL 로그가 리프 스위치에서 생성되고 있는지 확인합니다(ACL 로그는 APIC가 아니라 leaf에서 생성됨).
   <#root>

   ```
   leaf1#

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

   <#root>

   ```
   leaf1#

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

   항목이 ACLLOG 나타나지 않으면 log 지시어는 leaf에서 로그 생성을 트리거하지 않습니다. 이는 잘못 구성된 계약 지시문, 일치하는 트래픽이 계약에 도달하지 않음 또는 CoPP 속도 제한 기능이 로깅되기 전에 패킷을 삭제하는 것임을 나타낼 수 있습니다.

근본 원인: 계약 ACL 로그 심각도 수준은 informational (syslog 수준 6)입니다. 소스, 원격 대상 또는 Syslog minSevMessage Policy 기능 필터(syslogFacilityFilter)severity를 위uni/fabric/moncommon/sysmsgp/ff-syslog에 설정한 경우 ACL 로그 메시지는 패브릭 노드information를 벗어나기 전에 자동으로 삭제됩니다.

해결책: syslog 소스minSev에서 information 로 설정하고, 원격 대상 severity information 에서 로 설정하고, syslog minSev 시설 필터를 Common Policy(공통 정책) > Syslog Message Policies(Syslog 메시지 정책) > default(기본값)에서 information 로 설정하고, Log 지시어가 계약 필터에서 활성화되었는지 확인하고, ACL 로그가 스위치에서 전송되므로 방화벽이 APIC IP뿐 아니라 leaf 스위치 OOB IP 주소에서 syslog 트래픽을 허용하는지 확인합니다.

시나리오 9: 대상 그룹 이름 변경 후 Syslog 중지

문제/장애: syslog 대상 그룹의 이름이 변경된 후 syslog 메시지가 원격 서버에 도착하지 않습니다. 포트 또는 시설을 변경해도 이 문제가 발생하지 않습니다. 정책을 비활성화하고 다시 활성화하면 메시지 전달이 재개되지 않습니다.

근본 원인: 이는 알려진 소프트웨어 결함입니다. Cisco 버그 ID CSCwj23752를 참조하십시오. 대상

그룹의 이름을 변경하면 내부 syslog 전달 연결이 끊어집니다. APIC 릴리스 6.0(6) 이상에서 고정됩니다.

해결책: APIC 릴리스 6.0(6c) 이상으로 업그레이드합니다. 영향을 받는 버전에 대한 해결 방법으로 이름이 변경된 대상 그룹을 삭제하고 원하는 이름으로 다시 생성한 다음 syslog 소스를 다시 연결합니다.

시나리오 10: APIC GUI 지연을 유발하는 과도한 Syslog

문제/장애: APIC GUI가 느려지고 APIC CPU 사용률이 높습니다. 이 문제는 일반 작업 중에 계약 ACL 로깅이 활성화된 상태로 남아 있어 APIC 데이터베이스의 객체로 변환되는 대량의 정보 syslog 메시지가 생성되는 eventRecord 경우 발생할 수 있습니다.

근본 원인: Common Policy Syslog Message Policy(공통 정책 Syslog 메시지) Policy severity(정책 심각도)가 로 설정된 information경우, 모든 정보 syslog 메시지(대용량 ACL 로그 포함)는 APIC에서 를 eventRecord 생성합니다. 이로 인해 APIC 데이터베이스가 마비되고 GUI 속도가 느려질 수 있습니다.

해결책:

- 정상 작동 중에 계약 ACL 로깅을 비활성화합니다. 문제 해결 또는 유지 관리 기간 동안에만 이 기능을 활성화합니다.
- ACL 로깅을 활성화 상태로 유지해야 하는 경우 Fabric(패브릭) > Fabric Policies(패브릭 정책) > Policies(정책) > Monitoring(모니터링) > Common Policy(공통 정책) > Syslog Message Policies(Syslog 메시지 정책) > default(기본값)alerts에서 Syslog Message Policy(Syslog 메시지 정책 심각도)를 로 설정합니다. 이렇게 하면 정보 syslog 메시지가 이벤트로 변환되지 않도록 하는 동시에 원격 syslog 서버로 전달되지 않도록 할 수 있습니다.
- 운영상 유용하지 않은 노이즈 이벤트 코드를 삭제합니다. 이벤트 코드는 syslog 전달에 영향을 주지 않고 이벤트 레코드를 생성하지 못하도록 억지됩니다.

알려진 버그

다음과 같은 알려진 소프트웨어 결함은 ACI syslog 기능에 영향을 미칩니다.

- Cisco 버그 ID CSCwj23752 — syslog 대상 그룹의 이름을 변경하면 syslog 전달이 중지됩니다. APIC 릴리스 6.0(6c) 이상에서 수정되었습니다.

에스컬레이션 기준

다음과 같은 경우 기술 지원을 수집하고 Cisco TAC에 문의하십시오.

- Syslog 메시지는 패브릭 노드에서 로컬로 /var/log/external/messages 표시되고, 대상 그룹 및 원격 대상 관리 상태가 둘 다 enabled되며, 관리 EPG가 올바르고, 네트워크 연결이 확인되지만(ping 및 방화벽 검사 통과) 메시지는 원격 서버에 도착하지 않습니다.
- Syslog 메시지는 일부 패브릭 노드에서 도착하지만 다른 패브릭 노드에서는 도착하지 않으며, 이들 간의 컨피그레이션 차이가 없으므로 정책 구축의 불일치를 시사합니다.
- 대상 그룹 프로필 또는 원격 대상이 다시 활성화되었지만 구성 변경 후 몇 분 내에 메시지가 다시 시작되지 않습니다.
- APIC 업그레이드 후 Syslog 메시지 도착이 중지되어 잠재적 소프트웨어 결함이 예상됩니다.

TAC 케이스를 열기 전에 수집할 데이터:

- 영향을 받는 APIC 및 영향을 받는 1개의 리프 노드의 온디맨드 기술 지원
- APIC의 moquery -c syslogGroup, moquery -c syslogProf, moquery -c syslogRemoteDest및 moquery -c syslogSrc 의 출력.
- 공통 정책 링크moquery -d uni/fabric/moncommon/systemslsrc/rssystemDestGroup를 확인하는 의 출력입니다.
- APIC 및 영향을 받는 leaf의 /var/log/external/messages tail of.
- UDP/TCP 514 패킷이 패브릭 OOB 주소에서 도착하는지 확인하는 syslog 서버의 패킷 캡처.

참조

- Cisco APIC 기본 컨피그레이션 가이드, 릴리스 6.1(x) — 관리
- Cisco ACI 시스템 메시지 참조 설명서
- Cisco ACI 결함, 이벤트 및 시스템 메시지 관리 가이드
- Cisco ACI 계약 가이드 백서
- 느린 APIC GUI 문제 해결

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.