在ACI中配置系統日誌並對其進行故障排除

簡介

本檔案介紹如何在思科以應用程式為中心的基礎架構(ACI)中設定、驗證系統記錄（系統日誌）以及對其進行疑難排解。 它涵蓋完整的配置工作流、使用應用程式策略基礎設施控制器(APIC)託管對象(MO)模型的程式設計驗證，以及針對APIC控制器和枝葉和主幹交換機的結構化故障排除工作流。

概觀

ACI系統日誌完全由策略驅動。與獨立Cisco NX-OS®軟體不同，ACI枝葉**logging server**或主幹交換機上沒有CLI命令。所有系統日誌配置都是通過APIC策略完成的，APIC會自動將策略推送到每個交換矩陣節點。

關鍵元件

ACI中的syslog子系統由以下託管對象構建：

- Syslog Destination Group(syslogGroup) — 所有系統日誌目標的頂級容器。它控制消息格式（ACI或NX-OS樣式）和時間戳選項。它可以包含一個或多個遠端目標、本地檔案目標和控制檯目標。
- Syslog Profile(syslogProf) — 控制組級管理狀態和傳輸協定（UDP、TCP或SSL）的目標組的子級。
- Syslog Remote Destination(syslogRemoteDest) — 表示一個遠端syslog伺服器的目標組的子級。控制用於到達伺服器的伺服器IP或主機名、埠、嚴重性過濾器、系統日誌設施和管理終端組(EPG)。
- Syslog Local File(syslogFile) — 控制將系統日誌消息寫入每個交換矩陣節點上的本地檔案的目標組/var/log/external/messages的子級。
- Syslog源(syslogSrc) — 附加到監視策略。控制傳送哪些消息型別（審計、事件、故障、會話）和最低嚴重性，以及通過關係指向目標組的syslogRsDestGroup連結。

系統日誌源連線點

ACI使用四個監控策略範圍，控制哪些節點和對象生成系統日誌消息：

- 通用監控策略monCommonPol(uni/fabric/moncommon,) — 整個交換矩陣範圍。適用於所有故障和事件的基本監控策略，可自動部署到交換矩陣中的所有節點（枝葉和主幹交換機）和所有控制器

(APIC)。涵蓋所有交換矩陣、訪問和租戶層次結構。位於Fabric > Fabric Policies > Policies > Monitoring > Common Policy。
- 交換矩陣監控策略monInfraPol(uni/infra/moninfra-default,) — 交換矩陣範圍。為交換矩陣級對象生成系統日誌：交換矩陣埠、卡、機箱元件和風扇托架。位於Fabric > Fabric Policies > Policies > Monitoring > Default。
- 訪問監控策略(monFabricPol,)uni/fabric/monfab-default — 訪問（基礎架構）範圍。為面向接入的元件生成系統日誌：接入埠、交換矩陣擴展器(FEX)裝置和虛擬機器(VM)控制器事件。位於Fabric > Access Policies > Policies > Monitoring Policies > default。
- 租戶監控策略monEPGPol(uni/tn-common/monepg-default,) — 租戶範圍。為租戶範圍對象生成系統日誌：終端組(EPG)、應用配置檔案和服務。在[Tenant] > Monitoring Policies > default的每個租戶下找到。

附註：通用監控策略是系統日誌配置的建議起點，因為它在所有層次之間提供交換矩陣範圍覆蓋，並自動部署到所有節點。交換矩陣和訪問監控策略可以配置為「公共策略」之外的其他策略，以便更精細地控制特定對象層次結構，也可以取代公共策略，將系統日誌限制在更窄的範圍。

系統日誌消息格式

當組格式設定為aci（預設值）時，ACI系統日誌消息遵循RFC 3164格式：

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

舉例來說：

```
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
```

消息正文包括受影響對象的ACI故障代碼、生命週期狀態(例如， soaking、 retaining、 cleared)、嚴重性和可分辨名稱(DN)，使消息能夠自我描述。

提供三種報文格式選項：

- aci（預設） — RFC 3164相容格式。建議用於大多數部署。
- nxos - NX-OS樣式格式。如果系統日誌平台需要NX-OS格式的消息，請使用此命令。
- 增強型日誌(APIC 5.2(8)及更高版本) — 符合RFC 5424的格式，具有包括年份的增強型時間戳。

嚴重性對映

系統日誌嚴重性欄位是一個從0（最嚴重）到7（最嚴重）的單個數字。 下表顯示了系統日誌嚴重性級別與ACI/國際電信聯盟(ITU)嚴重性術語之間的對映：

系統日誌嚴重性	ACI/ITU級別	說明
0 — 緊急	—	系統不可用
1 — 警報	嚴重	需要立即採取行動
2 — 關鍵	主要	臨界條件
3 — 錯誤	輕微	錯誤條件
4 — 警告	警告	警告條件
5 — 通知	不確定/已清除	正常但重要的情況
6 — 資訊	—	僅資訊性消息
7 — 調試	—	僅調試輸出

傳輸選項

ACI支援三種遠端系統日誌傳輸協定：

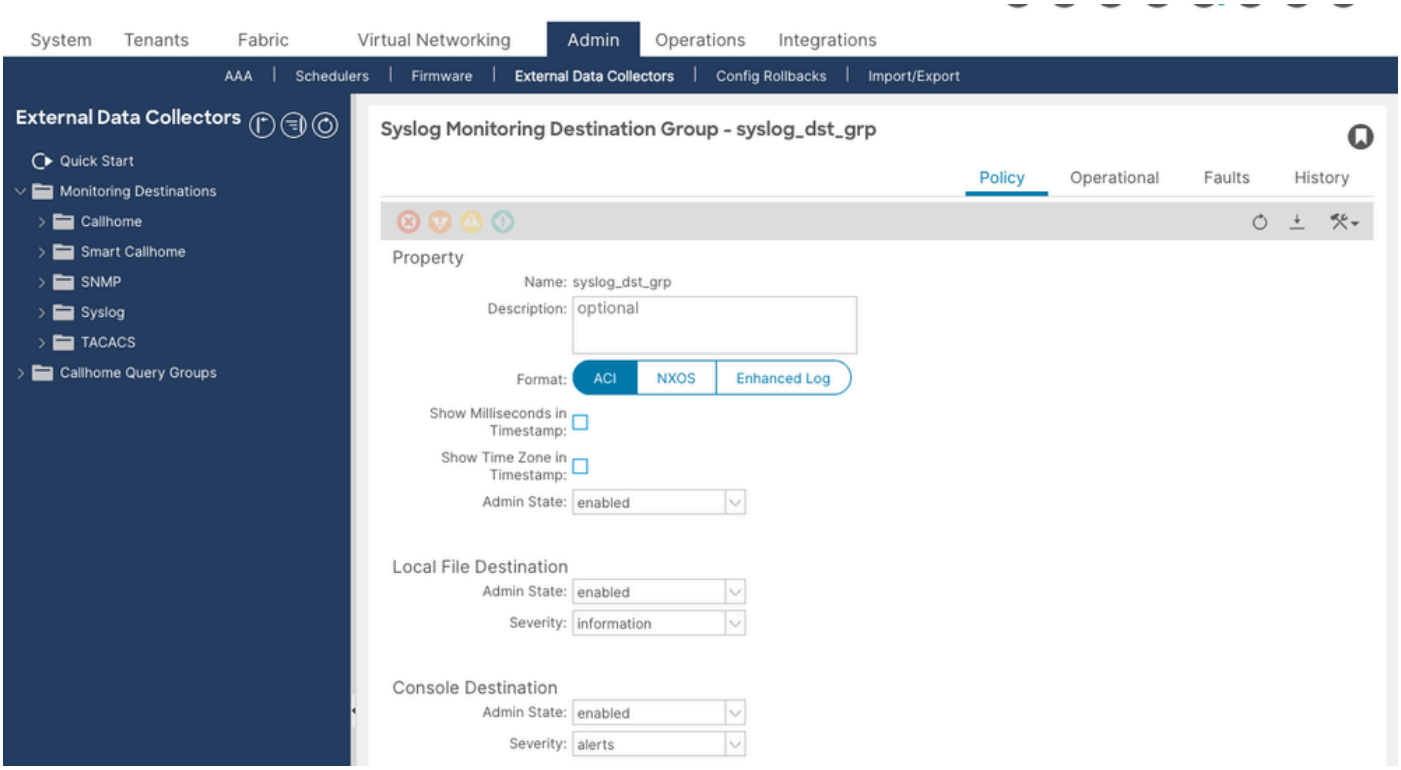
- UDP（預設） — 在所有APIC版本中可用。標準的免責交貨。
- TCP — 從APIC 5.2(3)版及更新版本提供。通過面向連線的傳輸提供可靠的傳輸。
- SSL — 從APIC 5.2(4)版及更新版本提供。使用TLS提供加密傳輸。每個ACI節點（APIC或交換機）充當TLS客戶端，並發起到系統日誌伺服器的出站連線。必須將伺服器證書上傳到APIC，地址為Admin > AAA > Security > Public Key Management > Certificate Authorities。

附註：如果遠端目標配置了SSL傳輸並且APIC降級為不支援SSL的版本，傳輸協定將自動恢復為UDP。確保系統日誌伺服器也可以接受UDP連線作為回退。

組態

以下步驟從端到端配置ACI系統日誌。完成所有步驟，以便從APIC控制器以及枝葉和主幹交換機啟用系統日誌轉發。

步驟 1:建立系統日誌目標組



目標組定義系統日誌消息的傳送位置和格式。請先建立此組，因為在後續步驟中配置的系統日誌源會按名稱引用此組。

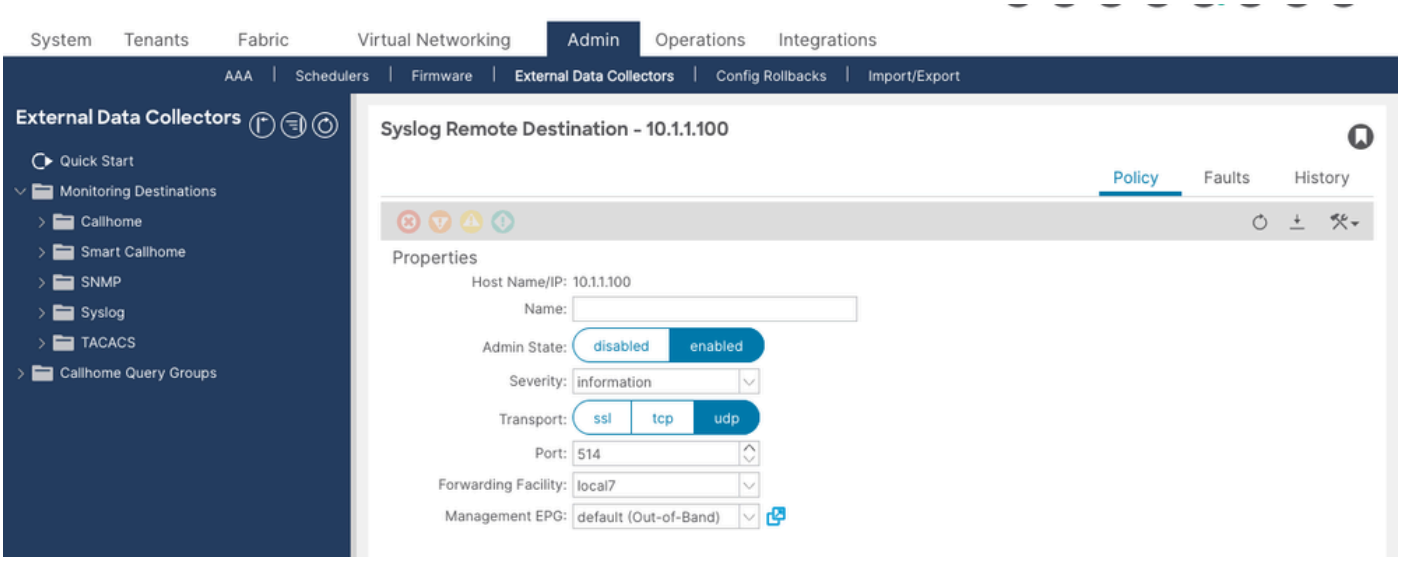
導航到Admin > External Data Collectors > Monitoring Destinations > Syslog。按一下右鍵Syslog，然後選擇Create Syslog Monitoring Destination Group。

在嚮導的第一頁（組配置檔案）上配置以下內容：

- 名稱 — 描述性名稱，如Syslog-Dest-Group。
- Format -(aci預設，RFC 3164相容)nxos或。
- 管理狀態 — enabled。
- 本地檔案目標管理狀態enabled —（推薦）。這會將消息寫入到每/var/log/external/messages個交換矩陣節點上，並且即使遠端伺服器無法訪問，此消息對於本地故障排除也至關重要。
- 本地檔案目標嚴重性 — information。
- 控制檯目標管理狀態disabled —（建議用於生產環境）。

按「Next」（下一步）。在第二頁上，按一下Create Remote Destinations區域中的+以新增遠端系統日誌伺服器。

步驟 2:新增遠端目標



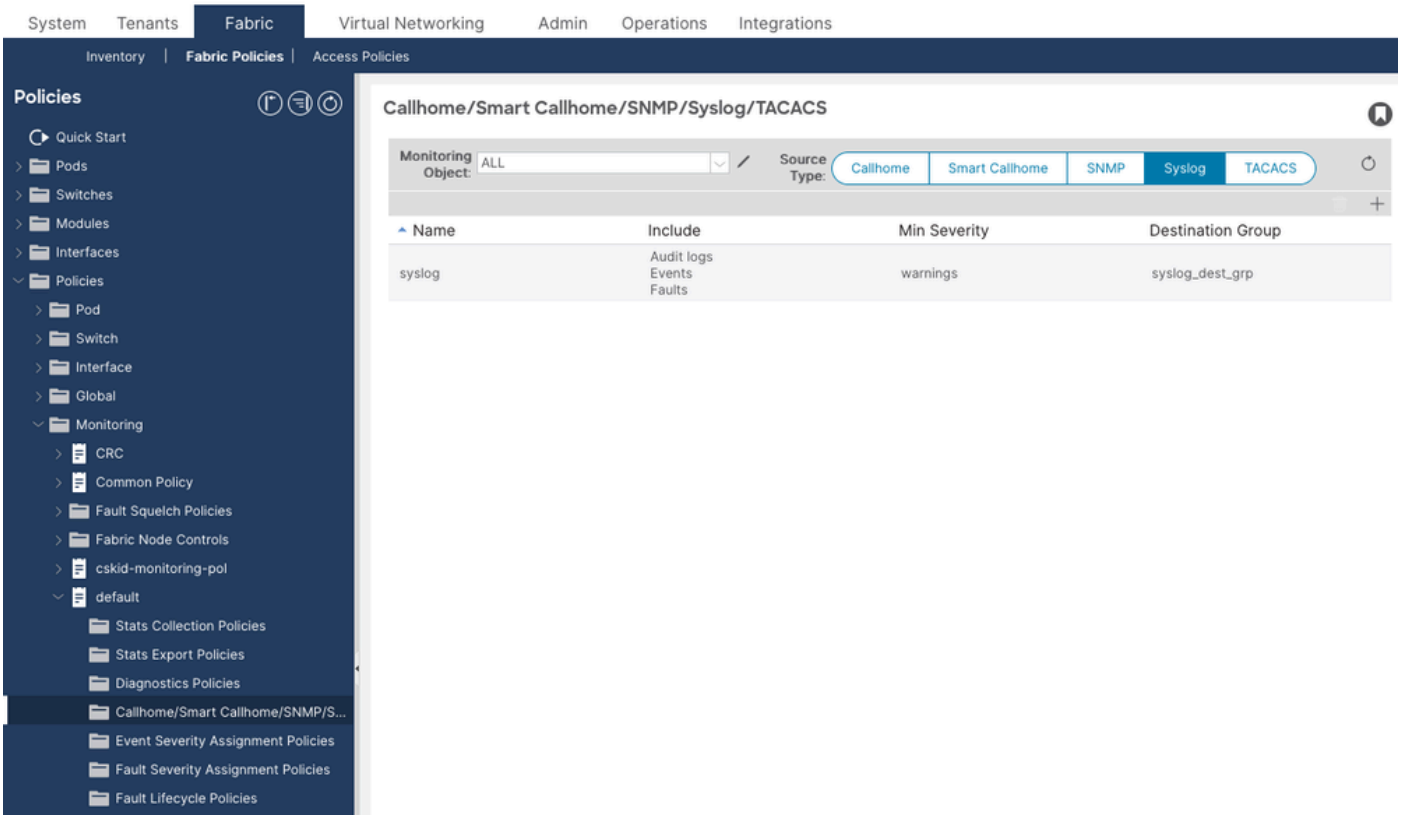
在Create Syslog Remote Destination對話方塊中配置遠端系統日誌伺服器：

- 主機 — 系統日誌伺服器的IP地址。使用IP地址而非主機名。如果使用主機名，必須確保通過帶外(OOB)管理介面可以訪問域名系統(DNS)伺服器。當網路中斷期間生成系統日誌消息時，只能通過帶內連線訪問的DNS伺服器可能無法解析。
- 管理狀態 — enabled。
- 嚴重性—information（推薦）。 這是傳送到此特定遠端伺服器的最低嚴重性。
- Port - 514（預設）。
- 設施 - local7（預設）。 將其設定為與您的系統日誌伺服器配置為接受和路由的設施值相匹配。
- Transport -(udp預設)。 用於tcp可靠傳輸(需要APIC 5.2(3)或更高版本)或加密傳輸(需要APIC 5.2(4)或更高版本以及上傳到APIC的證書ssl)。
- 管理EPG — 選擇可訪問系統日誌伺服器的管理EPG。對於OOB管理：uni/tn-mgmt/mgmtp-default/oob-default.對於帶內管理，請選擇適當的帶內EPG。此欄位不能為空。

按一下「OK」，然後「Finish」。

附註：可以將多個遠端目標新增到同一個目標組。每個目標可以有不同的嚴重性閾值、設施和傳輸協定。

步驟 3:在交換矩陣監控策略下建立系統日誌源



此步驟配置交換矩陣對象分層結構的系統日誌 — 交換矩陣埠、卡、機箱元件和風扇托架。這使用特定於層次的控制對通用監視策略（步驟4）進行補充。

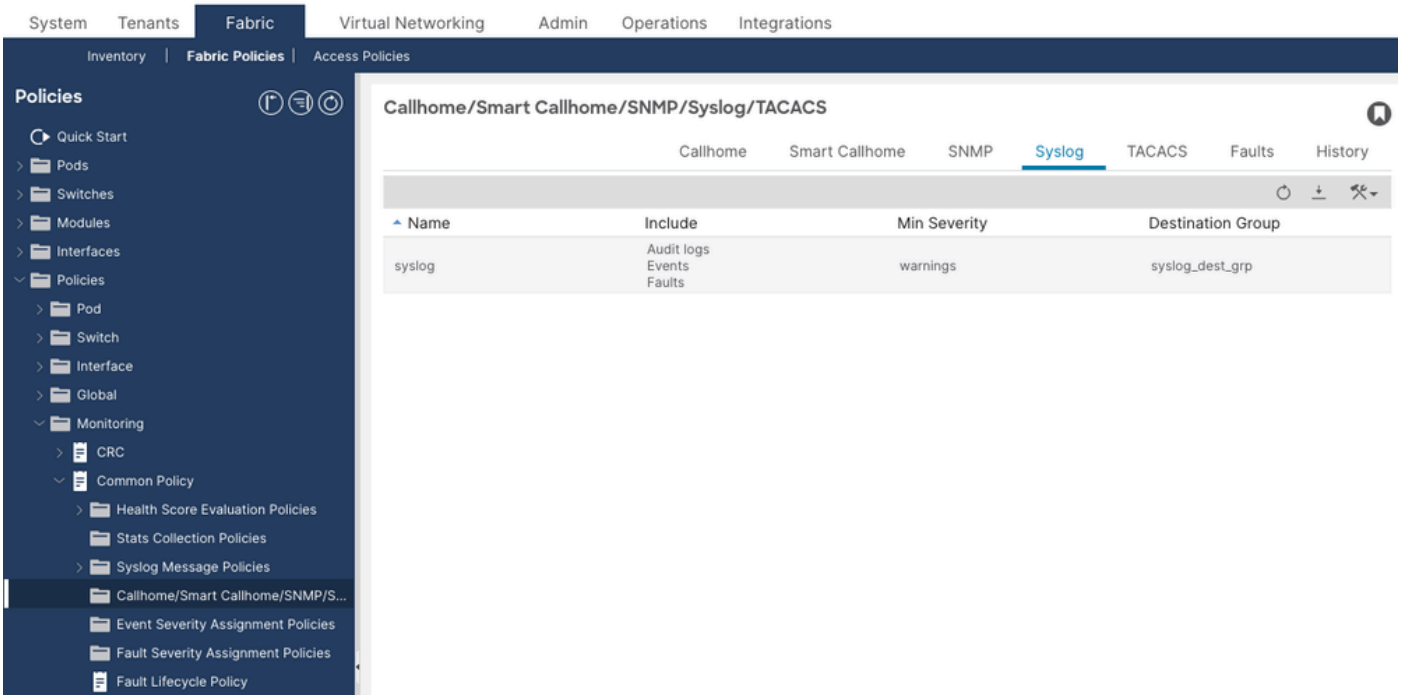
導航到Fabric > Fabric Policies > Policies > Monitoring > Default > Callhome/Smart Callhome/SNMP/Syslog/TACACS。

在右窗格中，將Source Type設定為Syslog。按一下+以建立系統日誌源：

- 名稱 — 描述性名稱，如Syslog-Source-Fabric。
- 最小嚴重性—information（建議用於完全覆蓋）。
- Include — 檢查audit、events和faults。（可選）為登入和註銷事件新增session。
- 目標組 — 選擇在步驟1中建立的目標組。

按一下「Submit」。

步驟 4:配置通用監控策略（系統範圍的系統日誌）

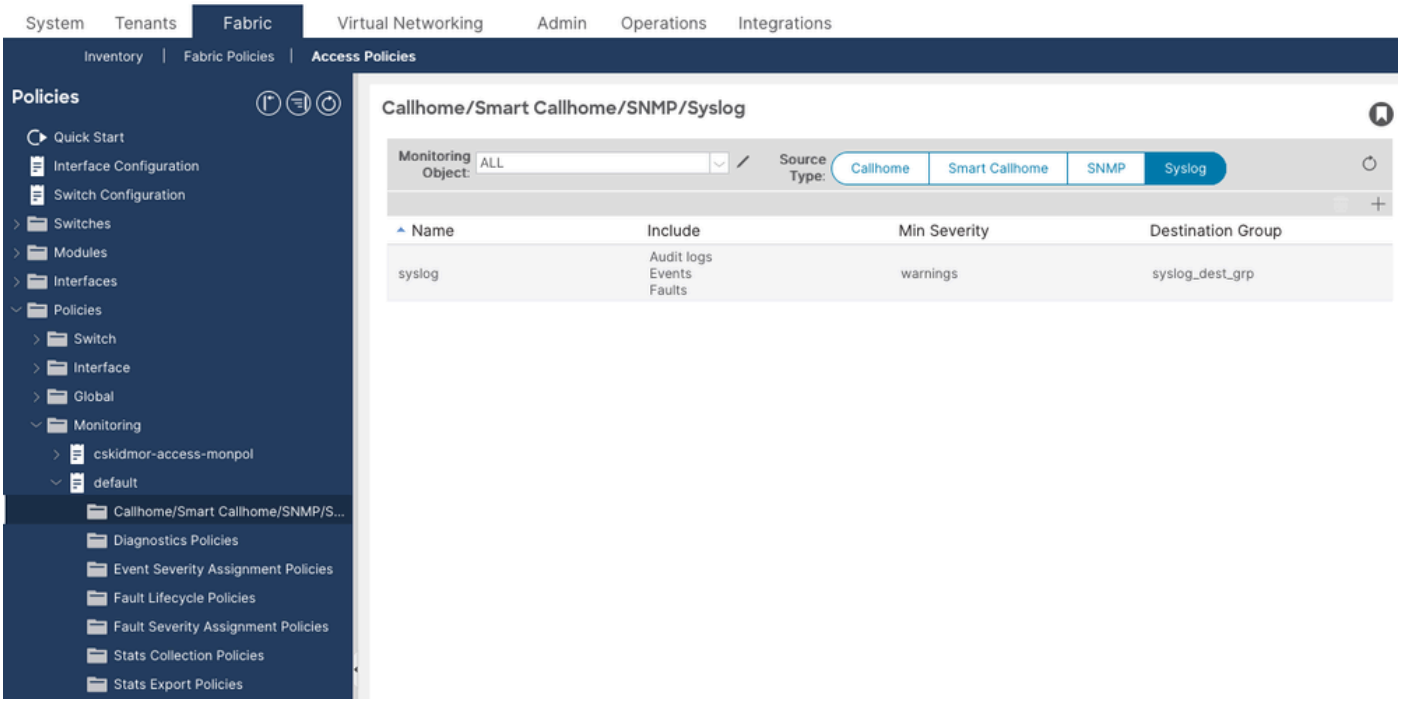


通用監控策略提供系統範圍的系統日誌覆蓋範圍，系統日誌覆蓋範圍會自動部署到交換矩陣中的所有節點和控制器。此步驟將系統系統日誌源連結到目標組。

導航到Fabric > Fabric Policies > Policies > Monitoring > Common Policy。在Syslog部分下，將系統syslog源連結到步驟1中建立的目標組。

公共策略系統syslog源使用DN$_{\text{syslogRsSystemDestGroup}}$上的$_{\text{uni/fabric/moncommon/systemslsrc/rssystemDestGroup}}$MO。

步驟 5:在訪問監視策略下建立系統日誌源



此步驟配置訪問對象分層結構的系統日誌 — 訪問埠、交換矩陣擴展器(FEX)裝置和虛擬機器(VM)控制器事件。這使用特定於層次的控制對通用監視策略（步驟4）進行補充。

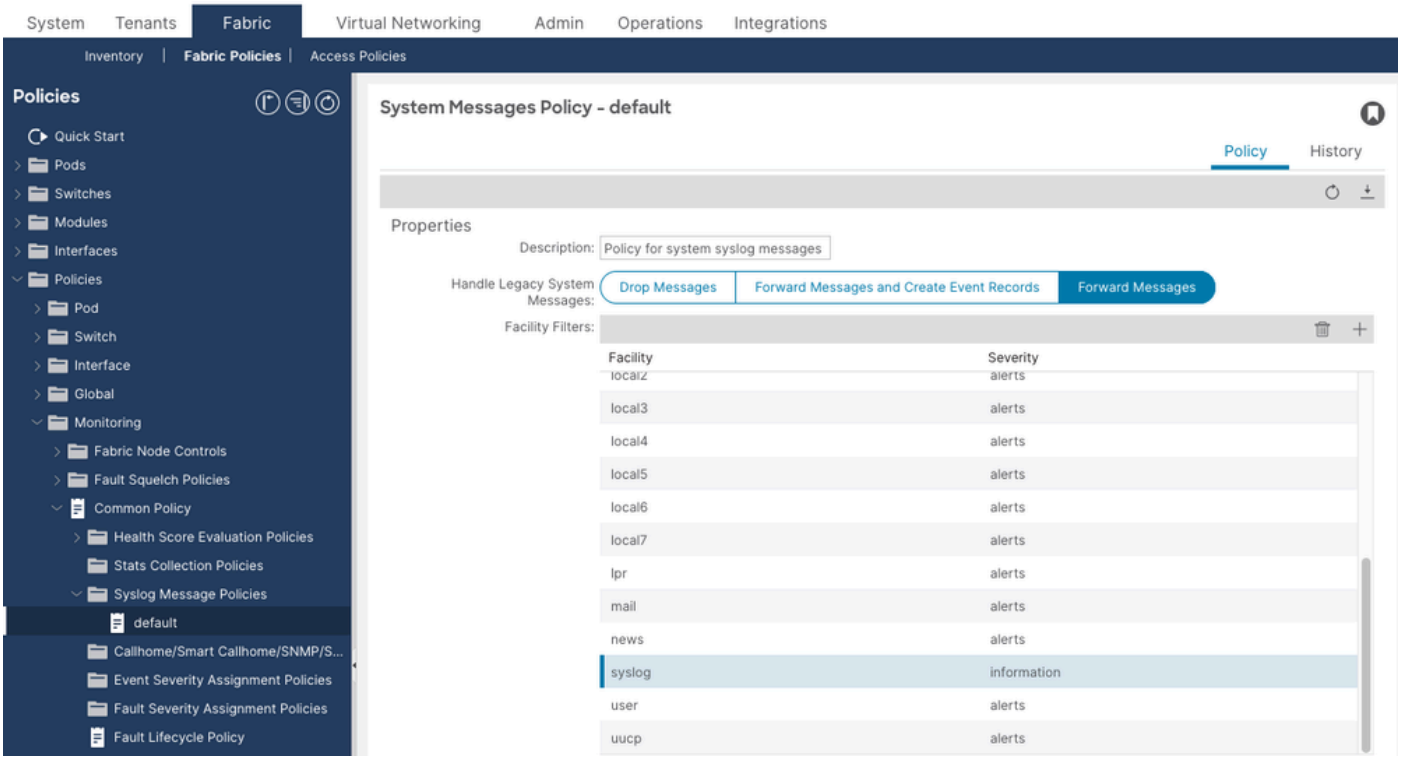
導航到Fabric > Access Policies > Policies > Monitoring Policies > default > Callhome/SNMP/Syslog。

將Source Type設定為Syslog。按一下「+」，然後設定與步驟3相同的設定：

- 名稱 — 例如Syslog-Source-Access。
- 最小嚴重性 — information。
- Include — 檢查audit、events和faults。
- 目標組 — 選擇相同的目標組。

按一下「Submit」。

第6步（可選）：調整合約ACL日誌記錄的系統日誌消息策略



如果您需要合約ACL permit或deny packet logs(ACLLOG_PKTLOG_PERMIT / ACLLOG_PKTLOG_DENY)顯示在遠端系統日誌伺服器中，則系統日誌消息工具過濾器必須設定為資訊性嚴重。

導航到Fabric > Fabric Policies > Policies > Monitoring > Common Policy > Syslog Message Policies > default。在設施過濾器清單中，選擇syslog設施，並將其Min Severity設定為information。這是DN的syslogFacilityFilterMO地uni/fabric/moncommon/sysmsgp/ff-syslog位。

附註：若要使合約ACL允許和拒絕日誌到達遠端系統日誌伺服器，必須滿足四個條件：(1)系統日誌源minSev必須是資訊,(2)遠端目標嚴重性必須是資訊,(3)系統日誌消息策略syslog設施過濾器minSev必須為資訊,(4)必須在合約過濾器條目上啟用Log指令。當滿足所有三個條件時，ACL日誌消息來自枝葉交換機（不是來自APIC），因此它們首先出現在枝葉交換機上的/var/log/external/messages中。合約ACL資料包日誌速率受CoPP的限制：deny logs預設為500 packets per second(pps),permit logs預設為300 pps per leaf。

附註：不支援在管理合約中對篩選器使用Log指令，這將導致分割槽規則部署失敗。僅將合約日誌記錄應用於租戶資料平面合約。

驗證設定

在排除任何操作問題之前驗證配置。缺少系統日誌消息的最常見根本原因是配置錯誤，而不是網路或軟體故障。

驗證目標組和配置檔案

在APIC**moquery -c syslogGroup**上運行以確認目標組存在並檢查其屬性：

<#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
```

然後使用以下命令驗證配置檔案(組級別管理狀態**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
```

若要查詢其配置檔案被禁用的任何目標組，請運行：

<#root>

```
apic1#

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

此處的結果表示無論遠端目標管理狀態如何，目標組都不會轉發任何系統日誌流量。

驗證遠端目的地

運行**moquery -c syslogRemoteDest**以驗證每個遠端伺服器配置：

<#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
```

需要特別注意以下三個屬性：

- adminState:一定是enabled的。如果禁用，則此特定遠端伺服器不會收到任何內容。
- epgDn:不能為空。空表示epgDn交換矩陣不知道從哪個介面傳送系統日誌流量，因此沒有消息離開交換矩陣。
- operState:未知:該值應為預期值，並不表示存在問題。ACI不會主動探測系統日誌伺服器的可達性。

驗證系統日誌源

運行**moquery -c syslogSrc**以確認源存在於正確的監控策略下：

<#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
```

確認在相應的監視策略下存在源：

- 下面的uni/fabric/moncommon源 — 通用監控策略，用於覆蓋整個交換矩陣的所有節點和所有對象層次結構。
- 下的源 — uni/infra/moninfra-default交換矩陣監控策略，用於交換矩陣級對象（交換矩陣埠、卡、機箱）。
- A source under uni/fabric/monfab-default- the Access Monitoring Policy for access-level objects(access ports， FEX， VM controllers)。

此外，驗證是否已連結通用監視策略系統syslog源：

<#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
```

如果需要協定ACL記錄，請使用以下命令驗證系統日誌消息策略工具過濾器嚴重**moquery -d uni/fabric/moncommon/sysmsgp/ff-syslog**性：

<#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
```

驗證本地日誌檔案

上的本地檔案/var/log/external/messages是確認系統日誌消息正在任何交換矩陣節點上生成的最直接方式，即使無法訪問遠端伺服器也是如此。在APIC和枝葉交換機上檢查它：

```
<#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
```

如果此檔案為空或未在節點上更新，則不會在源生成消息。如果檔案包含內容，但遠端系統日誌伺服器沒有接收消息，則問題在於轉發（目標組、網路或防火牆），而不是消息生成。

驗證與系統日誌伺服器的可達性

從APIC ping syslog伺服器，以驗證管理網路上的IP可達性：

```
<#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
```

在枝葉或主幹交換機上，使用帶-V標誌的iping來指定VRF。將management用於帶外或將mgmt:inb用於

帶內，具體取決於將哪個管理EPG分配給syslog目標：

```
<#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
```

成功的ping操作可確認IP可達性，但不確認是否允許UDP或TCP埠514。網際網路控制訊息通訊協定(ICMP)和系統日誌使用不同的通訊協定。

疑難排解

分類工作流

當系統日誌消息未到達遠端伺服器時，請使用以下診斷樹：

```
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
```

常見方案

案例 1:遠端伺服器未收到系統日誌消息

問題:已配置系統日誌目標組和遠端目標，但沒有消息到達遠端伺服器。APIC和交換機 /var/log/external/messages上的本地檔案包含最新條目。

配置檢查：

<#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
```

根本原因：遠端目標管理狀態為disabled。如果目標已建立但無意中處於禁用狀態，或者目標在維護期間被禁用且從未重新啟用，則可能會發生這種情況。

解決方案：導航到Admin > External Data Collectors > Monitoring Destinations > Syslog > [group name] > Remote Destinations > [server]。編輯遠端目標並將Admin State設定為enabled。

案例 2:Syslog目標組配置檔案已禁用

問題:即使啟用了遠端目標管理狀態，也不會從任何節點轉發任何消息。

配置檢查：

<#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
```

根本原因：管理syslogProf狀態控制整個目標組。禁用後，無論各個遠端目標狀態如何，都不會從任何節點轉發任何消息。

解決方案：導航到Admin > External Data Collectors > Monitoring Destinations > Syslog > [group name]。編輯配置檔案並將Admin State設定為enabled。

案例 3:缺少事件 — 未連結公共監視策略

問題:來自某些節點或對象層次的系統日誌消息無法到達遠端伺服器，即使在「交換矩陣」或「訪問監視策略」下配置了系統日誌源。

配置檢查：

<#root>

```
apic1#
```

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

Total Objects shown: 0
```

通用監視策略系統syslog源未連結到目標組。

根本原因：通用監控策略(uni/fabric/moncommon)提供所有層次結構的交換矩陣範圍系統日誌覆蓋範圍，並自動部署到所有節點和控制器。如果沒有它，則僅轉發與特定結構或訪問監控策略層次結構匹配的事件。交換矩陣監控策略(uni/infra/moninfra-default)涵蓋交換矩陣級對象，訪問監控策略(uni/fabric/monfab-default)涵蓋訪問級對象，但兩者均不提供通用策略提供的交換矩陣範圍覆蓋。

解決方案：導航到Fabric > Fabric Policies > Policies > Monitoring > Common Policy。在Syslog部分下，將系統syslog源連結到目標組。驗證是**moquery -d uni/fabric/moncommon/systemslsrc/rssystemDestGroup**否指向tDn您的目標組。

案例 4:嚴重性過於嚴格 — 缺少預期消息

問題:有些消息到達系統日誌伺服器，但缺少資訊性事件、審計日誌條目或會話登入事件。僅發現嚴重和重大故障。

配置檢查：

<#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
```

根本原因：系統日誌過濾發生在兩點：源(minSev)和遠端目標(severity)。 僅轉發通過兩個過濾器的郵件。如果以上任一選項設定，information資訊性消息將被丟棄。

解決方案：編輯syslog源並將Min Severity設定為資訊，然後在Include欄位中選中audit、events、faults。編輯遠端目標並將Severity設定為資訊。

案例 5:未向遠端目標分配管理EPG

問題:遠端伺服器未收到任何系統日誌消息。目標組已啟用，遠端目標已啟用，並且本地日誌檔案包含內容。

配置檢查：

<#root>

```
apic1#

moquery -c syslogRemoteDest

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

根本原因：如果沒有管理EPG，APIC和交換機不知道使用哪個物理介面來傳送系統日誌消息。消息已生成，但無法轉發。

解決方案：編輯遠端目標，選擇適當的管理EPG。對於OOB管理，請選擇uni/tn-mgmt/mgmtp-default/oob-default。對於帶內管理，請選擇適當的帶內EPG。

案例 6:管理EPG錯誤（帶內與帶外）

問題:系統日誌消息間歇地或僅從某些節點到達。系統日誌伺服器只能通過OOB管理訪問，但遠端目標引用帶內EPG。

配置檢查：

<#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
```

如果只能通過OOB網路訪問Syslog伺服器，則帶內EPG會導致消息來自無法到達伺服器的帶內介面。

解決方案：編輯遠端目標並將Management EPG更改為uni/tn-mgmt/mgmtp-default/oob-default。從APIC bash**ping -c 3 10.1.1.100**驗證以確認OOB可達性。

案例 7:防火牆阻止系統日誌流量

問題:本地日誌檔案在APIC和枝葉節點上都有內容，配置正確，對syslog伺服器執行ICMP ping成功，但沒有消息到達伺服器。

操作檢查：從APIC對syslog伺服器運行ping以驗證IP可達性：

<#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成功，但系統日誌消息未到達。ICMP(ping)通過，而UDP埠514被阻止。

根本原因：管理網路和syslog伺服器之間的防火牆或ACL正在阻止UDP埠514（如果配置了TCP傳輸，則為TCP 514）。ICMP和UDP是獨立的 — ICMP傳遞不確認允許UDP 514。此外，每個枝葉和主幹直接從自己的OOB IP地址傳送系統日誌。僅允許APIC OOB IP的防火牆會丟棄來自交換機節點的syslog資料包。

解決方案：驗證防火牆是否允許UDP/TCP埠514來自所有交換矩陣節點的OOB IP地址範圍，包括所有APIC、所有枝葉交換機和所有主幹交換機。系統日誌伺服器上的資料包捕獲確認UDP 514資料包是否到達。

案例 8:合約ACL允許/拒絕日誌未到達

問題:合約permit或deny資料包日誌ACLLOG_PKTLOG_PERMIT(/ACLLOG_PKTLOG_DENY)未到達系統日誌伺服器。

配置檢查：

1. 驗證系統日誌源嚴重性是information否：
   <#root>

   ```
   apic1#

   moquery -c syslogSrc

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

2. 驗證遠端目標嚴重性是information否：
   <#root>

   ```
   apic1#

   moquery -c syslogRemoteDest

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

3. 驗證Syslog Message Policy工具過濾器嚴重性是information否：
   <#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. 驗證已在合約篩選器上啟用log指令。導航到Tenants > [tenant] > Contracts > [contract] > Subjects > [subject] > Filters，然後確認Directions列顯示相關過濾器條目的log。
5. 驗證是否正在枝葉交換機上生成ACL日誌（ACL日誌源自枝葉，而不是APIC）：
   <#root>

   ```
   leaf1#

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

   <#root>

   ```
   leaf1#
   ```

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

如果未顯ACLLOG示任何條目，則log指令不會觸發枝葉上的日誌生成。這可能表示合約指令配置錯誤、沒有匹配流量進入合約，或CoPP速率限制在記錄資料包之前丟棄資料包。

根本原因：合約ACL日誌嚴重級別為informational（系統日誌級別6）。 如果系統日誌鏈中的任何過濾器(源minSevseverity過濾器、遠端目標過濾器或系統日誌消息策略工具過濾器(syslogFacilityFilter at uni/fabric/moncommon/sysmsgp/ff-syslog))設定在上面，則ACL日誌消息會在離開交換矩陣節點之前被靜默丟棄information。

解決方案：在syslog源上設定為minSev information，在遠端目標上設定為severityinformationsyslog minSev，在Common Policy > Syslog Message Policies > default下將設施過濾器設定為information，確認已在合約過濾器上啟用Log指令，並驗證防火牆是否允許來自枝葉交換機OOB IP地址(而不僅僅是APIC IP)的系統日誌流量，因為ACL日誌是從交換機傳送的。

案例 9:重新命名目標組後Syslog停止

問題:更改系統日誌目標組的名稱后，系統日誌消息停止到達遠端伺服器。更改埠或設施不會導致此問題。禁用和重新啟用該策略不會恢復郵件傳送。

根本原因：這是一個已知的軟體缺陷。請參閱思科錯誤ID CSCwj23752。重新命名目標組會破壞內部系統日誌轉發關聯。已在APIC 6.0(6)及更新版本中修復。

解決方案：升級到APIC 6.0(6c)版或更高版本。作為受影響版本的解決方法，請刪除重新命名的目標組並使用所需的名稱重新建立它，然後重新關聯系統日誌源。

案例 10:過多系統日誌導致APIC GUI緩慢

問題:APIC GUI變慢，並且APIC CPU利用率高。如果在正常操作期間啟用合約ACL日誌記錄，生成大量資訊性syslog消息並將其轉換為APIC資料庫中的對象，就可能會發生這種情況eventRecord。

根本原因：當Common Policy Syslog Message Policy severity設定為information時，每個資訊系統日誌消息（包括高容量ACL日誌）都會在APICeventRecord中生成。這可能會使APIC資料庫不堪重負並導致GUI速度緩慢。

解決方案：

- 在正常操作期間禁用合約ACL日誌記錄。僅在故障排除或維護時段啟用它。
- 如果ACL日誌記錄必須保持啟用狀態，請將Syslog消息策略嚴重性設定為alertsFabric > Fabric

Policies > Policies > Monitoring > Common Policy > Syslog Message Policies > default。這可以防止將資訊性系統日誌消息轉換為事件，同時仍允許將其轉發到遠端系統日誌伺服器。
- 壓制操作上無用的雜訊事件代碼。可以對事件代碼執行靜默處理，以防止它生成事件記錄，而不會影響系統日誌轉發。

已知錯誤

以下已知軟體缺陷影響ACI系統日誌功能：

- 思科錯誤ID CSCwj23752 — 重新命名系統日誌目標組會停止系統日誌傳送。已在APIC 6.0(6c)及更高版本中修復。

升級標準

在以下情況下，收集技術支援並聯絡Cisco TAC:

- /var/log/external/messages系統日誌消息在本地交換矩陣節點上顯示，目標組和遠端目標管理狀態都為enabled，管理EPG正確，網路可達性得到確認（ping和防火牆檢查通過），但消息仍然沒有到達遠端伺服器。
- 系統日誌消息來自一些交換矩陣節點，而不是其他交換矩陣節點，它們之間的配置沒有差異，這表明策略部署不一致。
- 目標組配置檔案或遠端目標已重新啟用，但消息不會在配置更改的幾分鐘內恢復。
- APIC升級後，系統日誌消息停止到達，表明可能存在軟體缺陷。

開啟TAC案例之前要收集的資料：

- 來自受影響的APIC和一個受影響枝葉節點的按需技術支援。
- APICmoquery -c syslogGroup、 moquery -c syslogProf和moquery -c syslogRemoteDest的moquery -c syslogSrc輸出。
- 的輸出moquery -d uni/fabric/moncommon/systemslsrc/rssystemDestGroup，用於檢驗Common Policy鏈路。
- 來自/var/log/external/messagesAPIC和受影響枝葉的尾部。
- 來自系統日誌伺服器的資料包捕獲，確認UDP/TCP 514資料包是否從交換矩陣OOB地址到達。

參考資料

- 思科APIC基本配置指南6.1(x)版 — 管理
- 思科ACI系統消息參考指南
- 思科ACI故障、事件和系統消息管理指南

- 思科ACI合約指南白皮書
- 排除速度慢的APIC GUI故障

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。