Configurazione e risoluzione dei problemi del syslog in ACI

Introduzione

In questo documento viene descritto come configurare, verificare e risolvere i problemi relativi alla registrazione del sistema (syslog) in Cisco Application Centric Infrastructure (ACI). Il documento illustra l'intero flusso di lavoro di configurazione, la verifica programmatica mediante il modello a oggetti gestiti (MO) di Application Policy Infrastructure Controller (APIC) e un flusso di lavoro strutturato per la risoluzione dei problemi sia per i controller APIC che per gli switch a foglia e dorso.

Panoramica

ACI syslog è interamente basato su policy. A differenza del software Cisco NX-OS® standalone, non sono disponibili comandi **logging server** CLI sugli switch ACI leaf o spine. Tutta la configurazione syslog viene eseguita mediante regole APIC che l'APIC trasferisce automaticamente su ogni nodo di fabric.

Componenti principali

Il sottosistema syslog in ACI è creato dai seguenti oggetti gestiti:

- Syslog Destination Group (syslogGroup): il contenitore di primo livello per tutte le destinazioni syslog. Controlla le opzioni relative al formato del messaggio (stile ACI o NX-OS) e all'indicatore orario. Può contenere una o più destinazioni remote, una destinazione file locale e una destinazione console.
- Profilo syslog (syslogProf): figlio del gruppo di destinazione che controlla lo stato amministrativo a livello di gruppo e il protocollo di trasporto (UDP, TCP o SSL).
- Destinazione remota syslog (syslogRemoteDest): figlio del gruppo di destinazione che rappresenta un server syslog remoto. Controlla l'IP o il nome host del server, la porta, il filtro di gravità, la funzione syslog e il gruppo di endpoint di gestione (EPG, Management Endpoint Group) utilizzati per raggiungere il server.
- File locale di syslog (syslogFile): figlio del gruppo di destinazione che controlla la scrittura dei messaggi di syslog nel file locale /var/log/external/messages su ciascun nodo dell'infrastruttura.
- Origine syslog (syslogSrc): associata a un criterio di monitoraggio. Controlla i tipi di messaggi (controllo, eventi, errori, sessione) e la gravità minima inviati e i collegamenti al gruppo di destinazione tramite una syslogRsDestGroup relazione.

Punti di collegamento origine Syslog

ACI utilizza quattro ambiti di criteri di monitoraggio che controllano quali nodi e oggetti generano messaggi syslog:

- Policy di monitoraggio comune (monCommonPol, uni/fabric/moncommon): ambito a livello di fabric. Criterio di monitoraggio di base che viene applicato a tutti gli errori e gli eventi e viene distribuito automaticamente in tutti i nodi (switch foglia e spine) e in tutti i controller (APIC) della struttura. Copre tutte le gerarchie di strutture, accessi e tenant. Disponibile in Fabric > Criteri fabric > Criteri > Monitoraggio > Criteri comuni.
- Criteri di monitoraggio fabric (monInfraPol, uni/infra/moninfra-default): ambito fabric. Genera syslog per gli oggetti a livello di struttura: porte fabric, schede, componenti dello chassis e alloggiamenti per ventole. Disponibile in Fabric > Criteri fabric > Criteri > Monitoraggio > Predefinito.
- Policy di monitoraggio dell'accesso (monFabricPol, uni/fabric/monfab-default) — Ambito dell'accesso (infrastruttura). Genera il syslog per i componenti di accesso: porte di accesso, dispositivi Fabric Extender (FEX) ed eventi del controller della macchina virtuale (VM). Disponibile in Fabric > Access Policies > Policies > Monitoring Policies > default (Policy di monitoraggio > Predefinito).
- Criteri di monitoraggio tenant (monEPGPol, uni/tn-common/monepg-default) - Ambito tenant. Genera il syslog per gli oggetti con ambito tenant: gruppi di endpoint (EPG), profili applicazione e servizi. Trovato sotto ogni tenant in [Tenant] > Monitoring Policies > default.

Nota: Il criterio di monitoraggio comune è il punto di partenza consigliato per la configurazione del syslog in quanto fornisce una copertura a livello di struttura in tutte le gerarchie e viene distribuito automaticamente in tutti i nodi. È possibile configurare i criteri di monitoraggio dell'infrastruttura e dell'accesso in aggiunta ai criteri comuni per un controllo più granulare su gerarchie di oggetti specifiche oppure al posto dei criteri comuni per limitare syslog a un ambito più ristretto.

Formato messaggi Syslog

I messaggi ACI syslog seguono il formato RFC 3164 quando il formato del gruppo è impostato su aci (impostazione predefinita):

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

Ad esempio:

```
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
```

Il corpo del messaggio include il codice di errore ACI, lo stato del ciclo di vita (ad esempio, soaking, retaining, cleared), la gravità e il nome distinto (DN) dell'oggetto interessato, rendendo i messaggi autodescrittivi.

Sono disponibili tre opzioni per il formato dei messaggi:

- Aci (predefinito): formato compatibile con RFC 3164. Consigliato per la maggior parte delle distribuzioni.
- nxos — Formato stile NX-OS. Utilizzare questa opzione se la piattaforma syslog prevede messaggi in formato NX-OS.
- Enhanced Log (APIC 5.2(8) e versioni successive): formato conforme alla RFC 5424 con timestamp migliorati che includono l'anno.

Mapping di gravità

Il campo della gravità del syslog è una cifra singola compresa tra 0 (massima gravità) e 7 (minima gravità). La tabella seguente mostra la mappatura tra i livelli di gravità del syslog e la terminologia di severità ACI / International Telecommunication Union (ITU):

Gravità syslog	Livello ACI/ITU	Descrizione
0 — emergenza	—	Il sistema è inutilizzabile
1 — avviso	Critico	Necessaria azione immediata
2 — critico	Importante	Condizione critica
3 — errore	Minor (Minore)	Condizione di errore
4 — avvertenza	Avviso	Condizione di avviso
5 — notifica	Indeterminato/Cancellato	Condizione normale ma significativa
6 — informativo	—	Solo messaggio informativo
7 — debug	—	Solo output di debug

Opzioni di trasporto

ACI supporta tre protocolli di trasporto per syslog remoto:

- UDP (predefinito): disponibile in tutte le versioni APIC. Consegna standard senza rischi.
- TCP: disponibile da APIC versione 5.2(3) e successive. Distribuzione affidabile con trasporto orientato alla connessione.
- SSL: disponibile da APIC versione 5.2(4) e successive. Fornisce il trasporto crittografato tramite TLS. Ogni nodo ACI (APIC o switch) funge da client TLS e avvia una connessione in

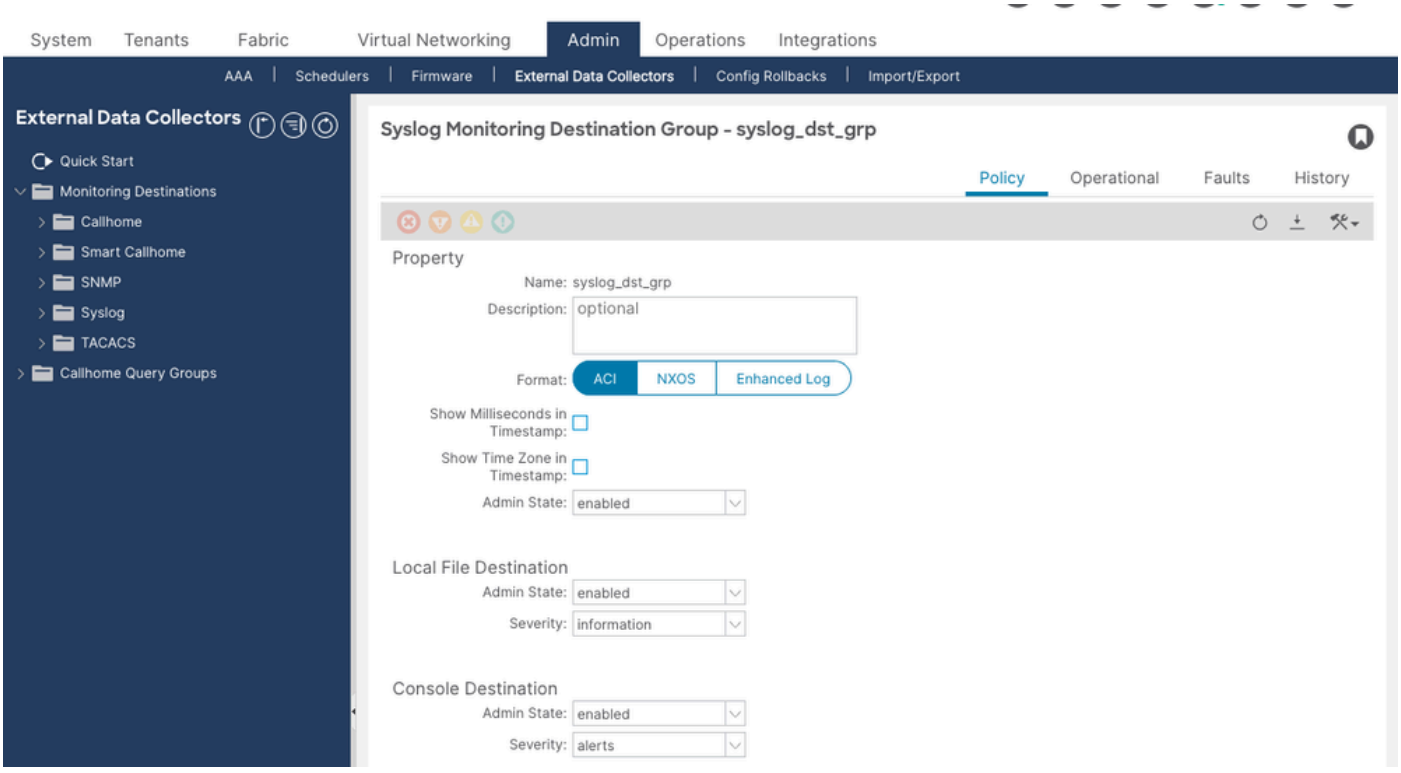
uscita al server syslog. Il certificato del server deve essere caricato nell'APIC selezionando Admin > AAA > Security > Public Key Management > Certificate Authorities.

Nota: Se una destinazione remota è configurata con il trasporto SSL e l'APIC viene aggiornato a una versione che non supporta SSL, il protocollo di trasporto viene automaticamente ripristinato a UDP. Assicurarsi che il server syslog possa accettare anche le connessioni UDP come fallback.

Configurazione

La procedura seguente consente di configurare il syslog ACI da un'estremità all'altra. Completare tutti i passaggi per abilitare l'inoltro syslog dai controller APIC e dagli switch a forma di foglia e di spine.

Passaggio 1: Creazione del gruppo di destinazione Syslog



Il gruppo di destinazione definisce dove vengono inviati i messaggi syslog e in quale formato. Creare innanzitutto questo gruppo, poiché le origini syslog configurate nei passaggi successivi fanno riferimento a questo gruppo per nome.

Passare ad Amministrazione > Raccoglitori di dati esterni > Destinazioni di controllo > Syslog. Fare clic con il pulsante destro del mouse su Syslog e selezionare Create Syslog Monitoring

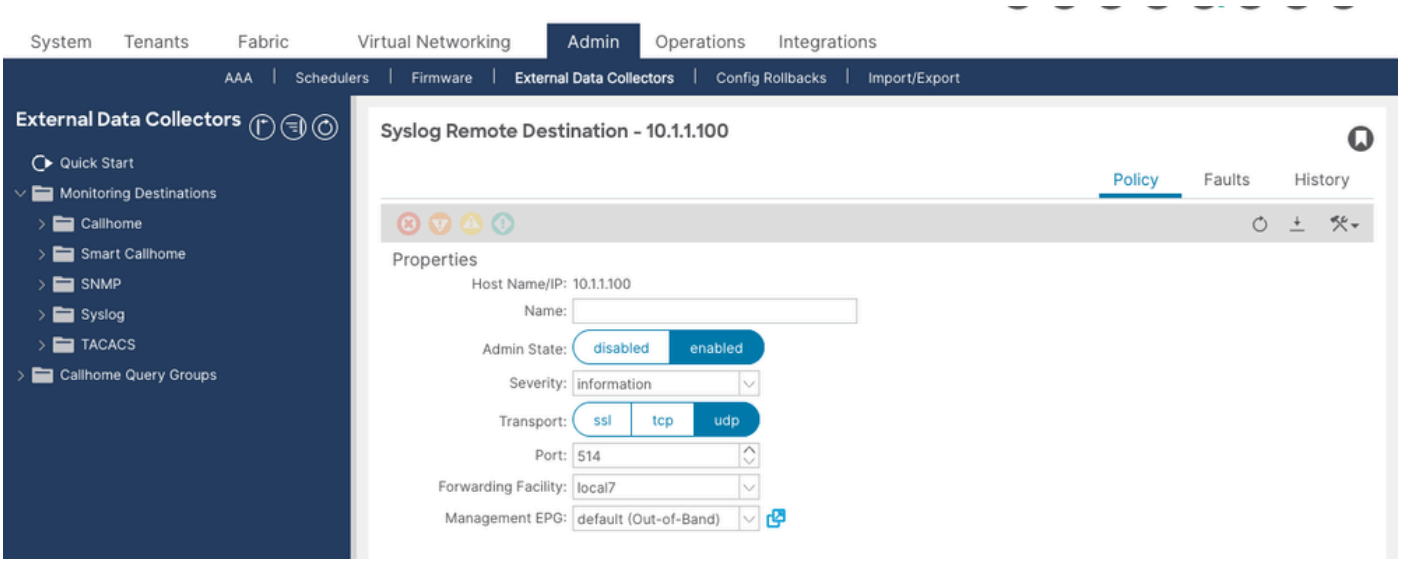
Destination Group (Crea gruppo di destinazione di monitoraggio syslog).

Nella procedura guidata, configurare quanto segue nella prima pagina (profilo gruppo):

- Nome — un nome descrittivo, ad esempio Syslog-Dest-Group.
- Format — aci (predefinito, compatibile con RFC 3164) o nxos.
- Stato amministratore — enabled.
- Stato amministratore destinazione file locale — enabled (consigliato). In questo modo i messaggi vengono scritti /var/log/external/messages su ogni nodo della struttura ed è essenziale per la risoluzione dei problemi locali anche quando un server remoto non è raggiungibile.
- Gravità destinazione file locale — information.
- Stato amministrazione destinazione console — disabled (consigliato per gli ambienti di produzione).

Fare clic su Next (Avanti). Nella seconda pagina, fare clic su + nell' area Crea destinazioni remote per aggiungere un server syslog remoto.

Passaggio 2: Aggiungi destinazione remota



Configurare il server syslog remoto nella finestra di dialogo Create Syslog Remote Destination:

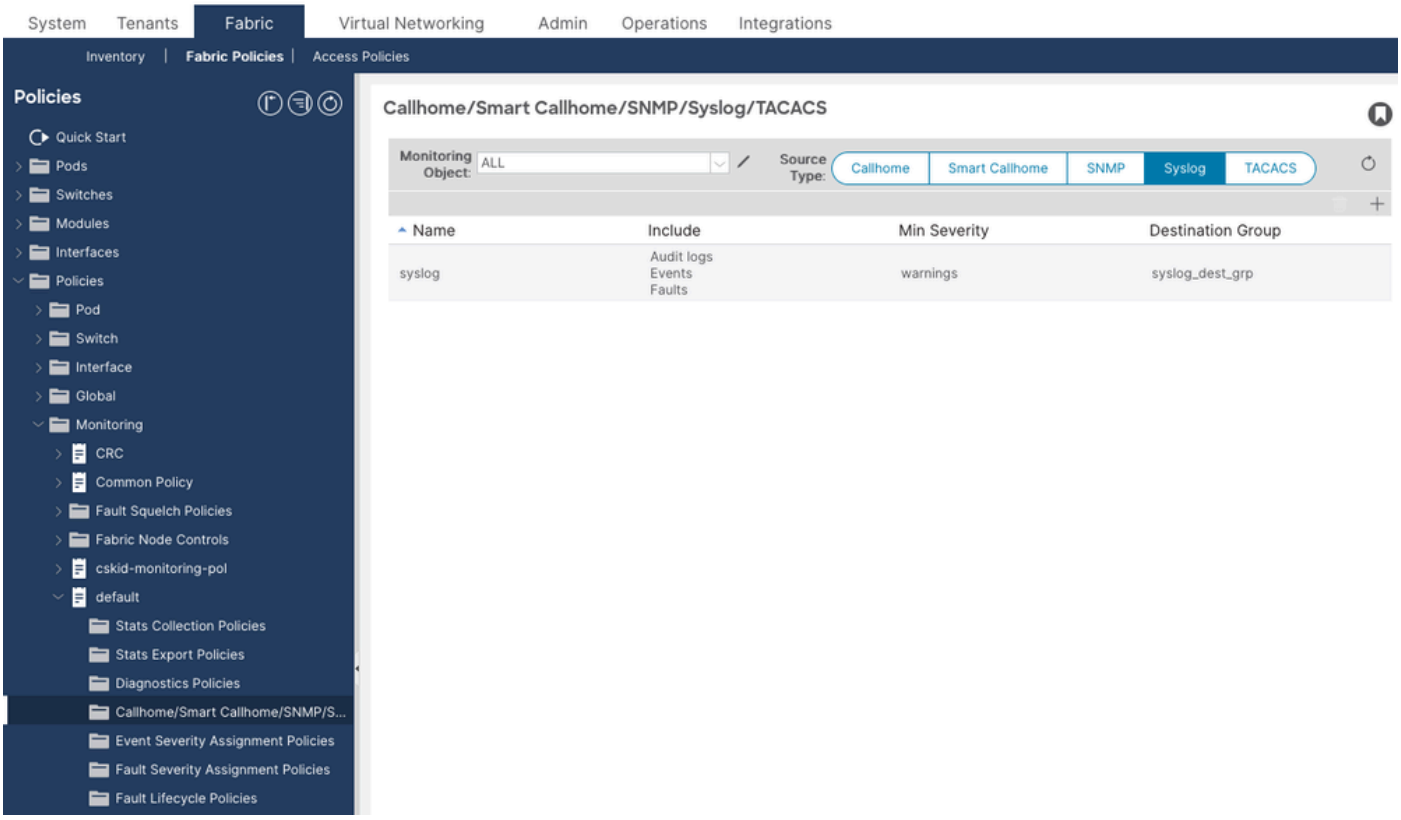
- Host: indirizzo IP del server syslog. Utilizzare un indirizzo IP anziché un nome host. Se si utilizza un nome host, è necessario verificare che il server DNS (Domain Name System) sia raggiungibile tramite l'interfaccia di gestione fuori banda (OOB). I server DNS raggiungibili solo tramite connettività in banda non possono essere risolti quando vengono generati messaggi syslog durante un'interruzione della rete.

- Stato amministratore — enabled.
- Gravità — information (consigliato). Gravità minima inviata a questo server remoto specifico.
- Porta — 514 (impostazione predefinita).
- Struttura — local7 (impostazione predefinita). Impostare questa opzione in modo che corrisponda al valore della struttura configurato per accettare e instradare il server syslog.
- Trasporto — udp (impostazione predefinita). Usare tcp per una consegna affidabile (richiede APIC 5.2(3) o versioni successive) o per ssl il trasporto crittografato (richiede APIC 5.2(4) o versioni successive e un certificato caricato nell'APIC).
- EPG di gestione: selezionare l'EPG di gestione che ha raggiungibilità sul server syslog. Per la gestione OOB: uni/tn-mgmt/mgmtp-default/oob-default. Per la gestione in banda, selezionare l'EPG in banda appropriato. Questo campo non può essere vuoto.

Fare clic su OK, quindi su Fine.

Nota: È possibile aggiungere più destinazioni remote allo stesso gruppo di destinazione. Ogni destinazione può avere una soglia di gravità, una struttura e un protocollo di trasporto diversi.

Passaggio 3: Creare un'origine syslog nei criteri di monitoraggio dell'infrastruttura



Questo passaggio consente di configurare syslog per la gerarchia degli oggetti fabric: porte fabric, schede, componenti dello chassis e alloggiamenti per ventole. In questo modo si completa la

politica di monitoraggio comune (Fase 4) con un controllo specifico della gerarchia.

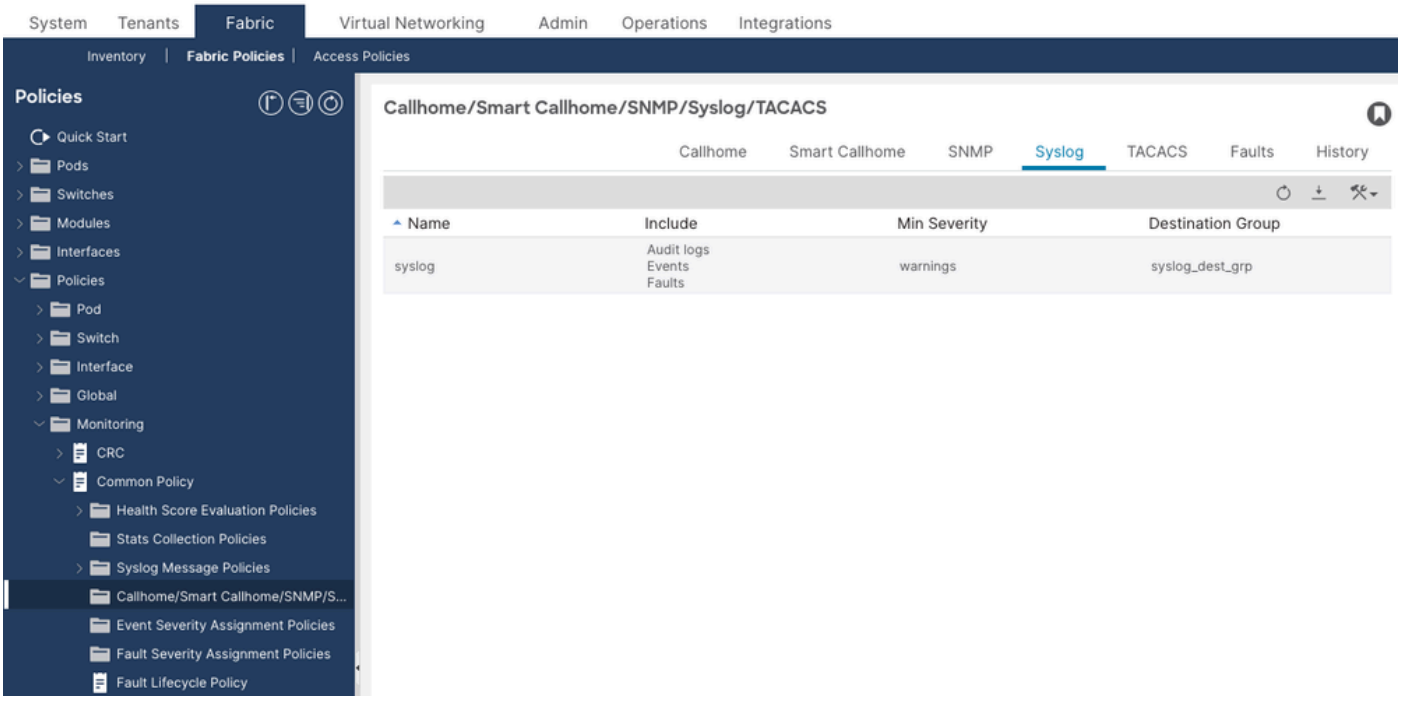
Passare a Fabric > Fabric Policies > Policies > Monitoring > default > Callhome/Smart Callhome/SNMP/Syslog/TACACS.

Nel riquadro di destra, impostare Source Type (Tipo di origine) su Syslog. Fare clic su + per creare un'origine syslog:

- Nome — un nome descrittivo, ad esempio Syslog-Source-Fabric.
- Gravità minima — information (consigliata per la copertura completa).
- Includi - Controlla audit, eventi e errori. Facoltativamente, aggiungere sessione per gli eventi di accesso e disconnessione.
- Gruppo di destinazione - Selezionare il gruppo di destinazione creato nel passo 1.

Fare clic su Invia.

Passaggio 4: Configurazione dei criteri di monitoraggio comuni (syslog a livello di sistema)

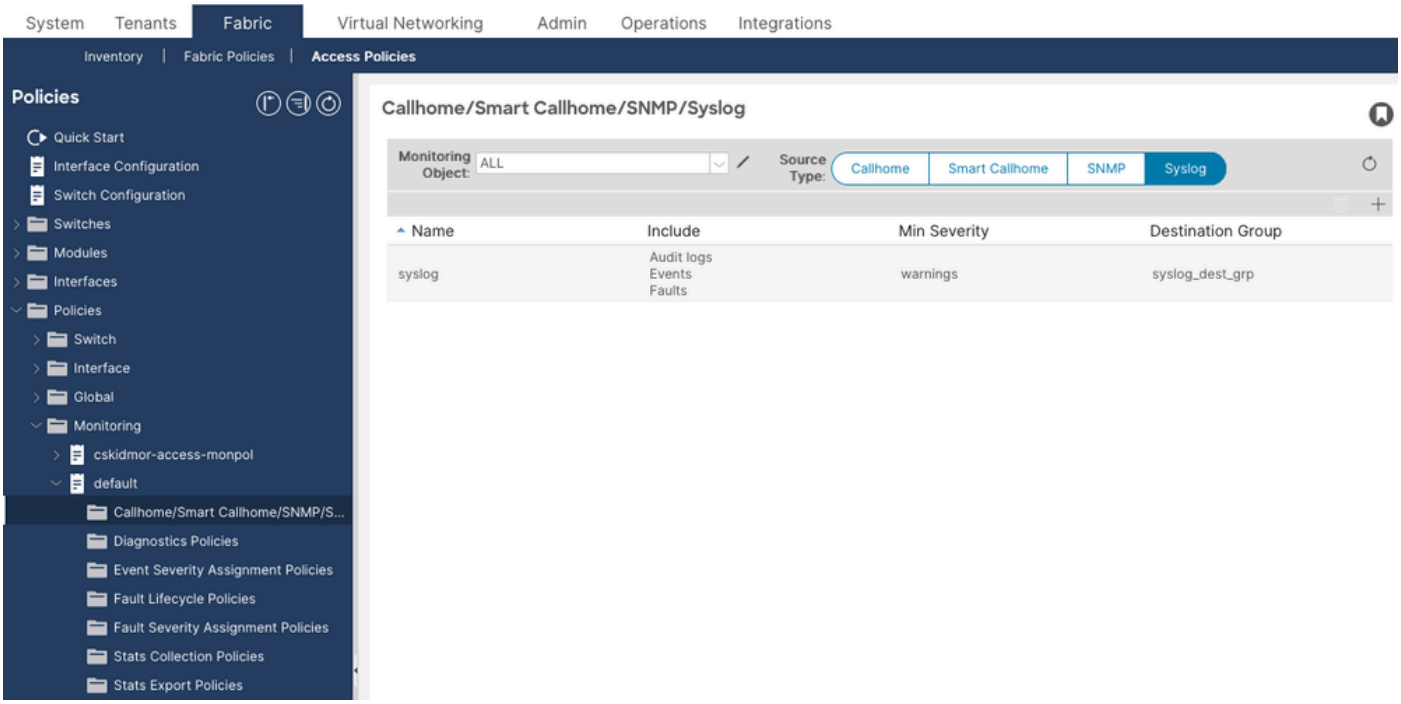


I criteri di monitoraggio comuni forniscono la copertura syslog a livello di sistema che viene distribuita automaticamente in tutti i nodi e i controller dell'infrastruttura. Questo passaggio collega l'origine syslog di sistema al gruppo di destinazione.

Selezionare Fabric > Fabric Policies > Policies > Monitoring > Common Policy (Policy di fabric > Monitoraggio > Criteri comuni). Nella sezione Syslog, collegare l'origine syslog di sistema al gruppo di destinazione creato nel passo 1.

L'origine syslog del sistema di criteri comuni utilizza l'oggetto MO syslogRsSystemDestGroup nel uni/fabric/moncommon/systemslsrc/rssystemDestGroupDN.

Passaggio 5: Creare un'origine syslog nei criteri di monitoraggio dell'accesso



Questo passaggio consente di configurare syslog per la gerarchia degli oggetti di accesso, ovvero porte di accesso, dispositivi Fabric Extender (FEX) ed eventi del controller della macchina virtuale (VM). In questo modo si completa la politica di monitoraggio comune (Fase 4) con un controllo specifico della gerarchia.

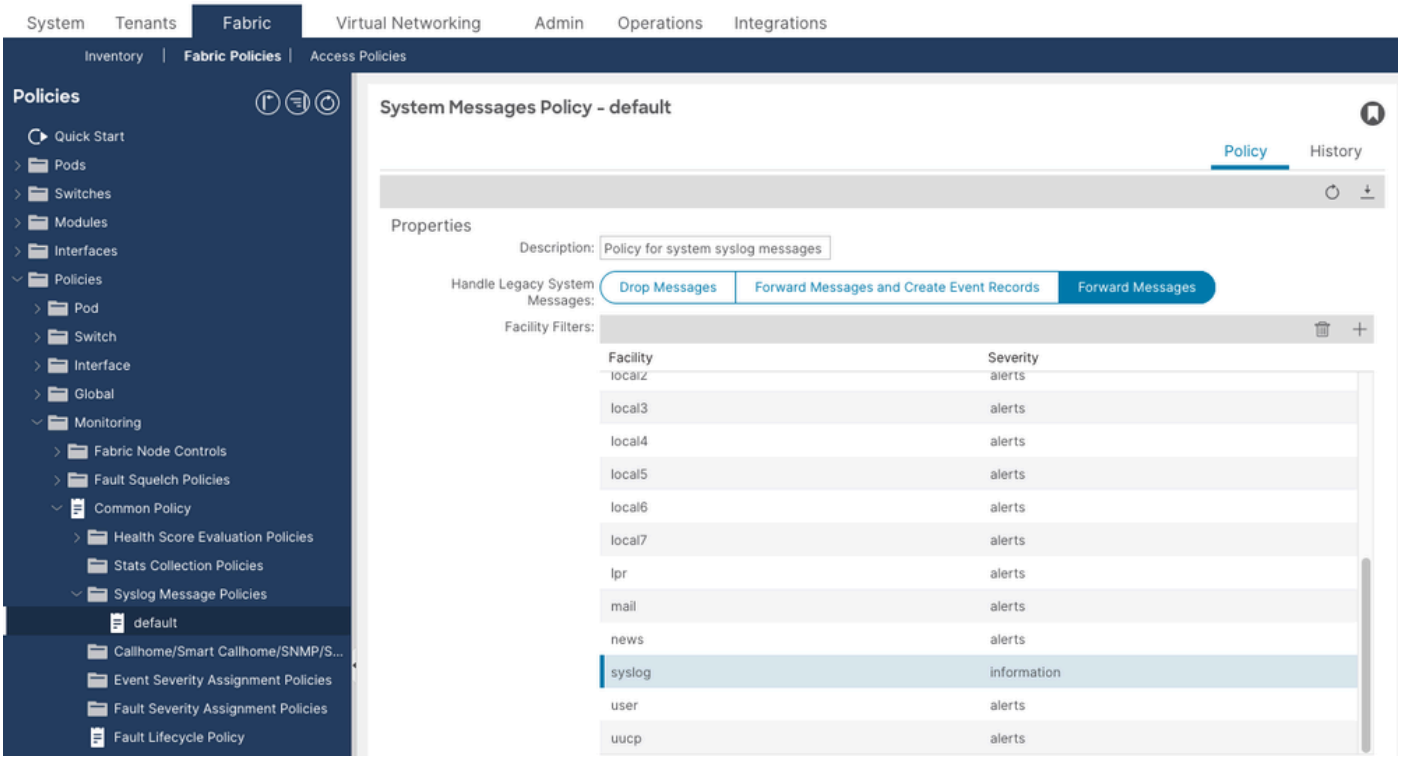
Selezionare Fabric > Access Policies > Policies > Monitoring Policies > default > Callhome/SNMP/Syslog.

Impostare Source Type su Syslog. Fare clic su + e configurare le stesse impostazioni del passo 3:

- Nome - ad esempio, Syslog-Source-Access.
- Gravità minima — information.
- Includi - Controlla audit, eventi e errori.
- Gruppo di destinazione - Selezionare lo stesso gruppo di destinazione.

Fare clic su Invia.

Passaggio 6 (facoltativo): Modifica dei criteri messaggi syslog per la registrazione degli ACL dei contratti



Se si desidera che i log dei pacchetti (ACLLOG_PKTLOG_PERMIT / ACLLOG_PKTLOG_DENY) vengano visualizzati nel server syslog remoto per consentire o negare l'accesso al contratto, è necessario impostare il filtro dei messaggi syslog sulla gravità informativa.

Selezionare Fabric > Fabric Policies > Policies > Monitoring > Common Policy > Syslog Message Policies > default (Fabric > Criteri fabric > Criteri di monitoraggio > Criteri comuni > Criteri messaggi syslog > predefiniti). Nell'elenco dei filtri, selezionare la funzione syslog e impostarne il livello di gravità minimo su information. Questo è l'syslogFacilityFilterMO al DN uni/fabric/moncommon/sysmsgp/ff-syslog.

Nota: Affinché i log degli ACL del contratto possano raggiungere il server syslog remoto, è necessario che siano soddisfatte quattro condizioni: (1) l'origine del syslog minSev deve essere informazione, (2) la gravità della destinazione remota deve essere informazione, (3) il filtro della funzione syslog dei criteri messaggi del syslog minSev deve essere informazione, e (4) la direttiva Log deve essere abilitata sulla voce del filtro del contratto. Quando tutte e tre le condizioni sono soddisfatte, i messaggi di log ACL hanno origine dallo switch foglia (non dall'APIC), quindi vengono visualizzati prima in `/var/log/external/messages` sulla foglia. Le velocità di registrazione dei pacchetti ACL del contratto sono limitate dal protocollo CoPP:

---

per impostazione predefinita, deny logs equivale a 500 pacchetti al secondo (pps), mentre per impostazione predefinita, deny logs equivale a 300 pps per foglia.

Nota: L'utilizzo della direttiva Log sui filtri nei contratti di gestione non è supportato e causa errori di distribuzione della regola di suddivisione in zone. Applicare la registrazione dei contratti solo ai contratti del piano dati del tenant.

Verifica della configurazione

Verificare la configurazione prima di risolvere eventuali problemi operativi. La causa principale più comune dei messaggi syslog mancanti è la configurazione errata, non un errore di rete o software.

Verifica del gruppo di destinazione e del profilo

Eseguire **moquery -c syslogGroup** su APIC per verificare l'esistenza dei gruppi di destinazione e controllare i relativi attributi:

<#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
```

Verificare quindi il profilo (stato di amministrazione a livello di gruppo) con **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
```

Per trovare un gruppo di destinazione il cui profilo sia disabilitato, eseguire:

<#root>

```
apic1#

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

Di conseguenza, il gruppo di destinazione non inoltra alcun traffico syslog, indipendentemente dallo stato di amministrazione della destinazione remota.

Verifica destinazione remota

Eseguire **moquery -c syslogRemoteDest** per verificare la configurazione di ogni server remoto:

<#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
```

Tre attributi richiedono particolare attenzione:

- statoAmmin: deve essere enabled. Se disattivato, il server remoto specifico non riceverà nulla.
- PGDN: non deve essere vuoto. Se il valore epgDn è vuoto, l'infrastruttura non è in grado di

individuare l'interfaccia da cui inviare il traffico syslog, quindi l'infrastruttura non viene chiusa da alcun messaggio.
- Stato operazione: sconosciuto: questo valore è previsto e non indica un problema. ACI non verifica attivamente la raggiungibilità dei server syslog.

Verifica delle origini del syslog

Eseguire **moquery -c syslogSrc** per verificare che le origini siano presenti nei criteri di monitoraggio corretti:

<#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
```

Confermare l'esistenza delle origini nei criteri di monitoraggio appropriati:

- Un'origine in uni/fabric/moncommon — Common Monitoring Policy (Policy di monitoraggio comune), per la copertura a livello di struttura di tutti i nodi e di tutte le gerarchie di oggetti.
- Un'origine in uni/infra/moninfra-default — la politica di monitoraggio del fabric, per gli oggetti a livello di fabric (porte, schede, chassis).
- Un'origine in uni/fabric/monfab-default — Criteri di monitoraggio dell'accesso, per gli oggetti a livello di accesso (porte di accesso, FEX, controller VM).

Verificare inoltre che l'origine syslog del sistema di criteri di monitoraggio comuni sia collegata:

<#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
```

Se è richiesta la registrazione degli ACL del contratto, verificare la gravità del filtro della funzionalità dei criteri dei messaggi di syslog con **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
```

Verifica del file di log locale

Il file locale in /var/log/external/messages è il modo più diretto per confermare che i messaggi syslog vengono generati su qualsiasi nodo fabric, anche quando un server remoto non è raggiungibile. Controllare sia sull'APIC che sull'interruttore a foglia:

<#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
```

Se il file è vuoto o non viene aggiornato in un nodo, non verranno generati messaggi nell'origine. Se il file ha del contenuto ma il server syslog remoto non riceve messaggi, il problema è l'inoltro (gruppo di destinazione, rete o firewall) e non la generazione del messaggio.

Verifica della raggiungibilità del server Syslog

Eseguire il ping tra l'APIC e il server syslog per verificare la raggiungibilità dell'IP sulla rete di gestione:

```
<#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
```

Da un interruttore a foglia o a dorso, usare `ping` con l'indicatore `-V` per specificare il VRF. Utilizzare `management` per out-of-band o `mgmt:inb` per in-band, a seconda di quale Management EPG è assegnato alla destinazione syslog:

```
<#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
```

Se il ping ha esito positivo, viene confermata la raggiungibilità dell'IP, ma non la porta UDP o TCP 514. Il protocollo ICMP (Internet Control Message Protocol) e il syslog utilizzano protocolli diversi.

Risoluzione dei problemi

Flusso di lavoro triage

Utilizzare la struttura decisionale seguente quando i messaggi syslog non arrivano al server remoto:

```
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
```

Scenari comuni

Scenario 1: Nessun messaggio syslog ricevuto sul server remoto

Problema: Il gruppo di destinazione syslog e la destinazione remota sono configurati, ma al server remoto non arriva alcun messaggio. Il file locale /var/log/external/messages sull'APIC e sugli switch contiene le voci recenti.

Controllo configurazione:

<#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
```

Causa principale: Lo stato di amministrazione della destinazione remota è disabled. Ciò può verificarsi se la destinazione è stata creata ma inavvertitamente disabilitata oppure se è stata disabilitata durante la manutenzione e non è mai stata riabilitata.

Soluzione: Passare a Amministrazione > Agenti di raccolta dati esterni > Destinazioni di monitoraggio > Syslog > [nome gruppo] > Destinazioni remote > [server]. Modificare la destinazione remota e impostare Admin State su enabled.

Scenario 2: Profilo Del Gruppo Di Destinazione Syslog Disabilitato

Problema: Nessun messaggio viene inoltrato da qualsiasi nodo anche se lo stato di amministrazione della destinazione remota è abilitato.

Controllo configurazione:

<#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
```

Causa principale: Lo stato syslogProf admin controlla l'intero gruppo di destinazione. Quando è disattivata, non viene inoltrato alcun messaggio da alcun nodo, a prescindere dallo stato delle singole destinazioni remote.

Soluzione: Passare ad Amministrazione > Raccoglitori di dati esterni > Destinazioni di controllo > Syslog > [nome gruppo]. Modificare il profilo e impostare Admin State su enabled.

Scenario 3: Eventi mancanti — Criterio di monitoraggio comune non collegato

Problema: I messaggi syslog provenienti da alcuni nodi o gerarchie di oggetti non raggiungono il server remoto, anche se un'origine syslog è configurata in Fabric o nei criteri di monitoraggio degli accessi.

Controllo configurazione:

<#root>

```
apic1#

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

Total Objects shown: 0
```

L'origine syslog del sistema di criteri di monitoraggio comuni non è collegata al gruppo di destinazione.

Causa principale: La Common Monitoring Policy (uni/fabric/moncommon) fornisce la copertura syslog a livello di struttura in tutte le gerarchie e viene distribuita automaticamente in tutti i nodi e controller. Senza di esso, vengono inoltrati solo gli eventi corrispondenti alle gerarchie specifiche dei criteri di monitoraggio dell'infrastruttura o dell'accesso. Il criterio di monitoraggio dell'infrastruttura (uni/infra/moninfra-defaultFabric Monitoring Policy) copre gli oggetti a livello di struttura, mentre il criterio di monitoraggio dell'accesso (uni/fabric/monfab-defaultAccess Monitoring Policy) copre gli oggetti a livello di accesso, ma non fornisce la copertura a livello di struttura offerta dal criterio comune.

Soluzione: Selezionare Fabric > Fabric Policies > Policies > Monitoring > Common Policy (Policy di fabric > Monitoraggio > Criteri comuni). Nella sezione Syslog, collegare l'origine syslog di sistema al gruppo di destinazione. Verificare con **moquery -d uni/fabric/moncommon/systemslsrc/rssystemDestGroup** che il tDn punto punti al gruppo di destinazione.

Scenario 4: Gravità troppo restrittiva — Messaggi previsti mancanti

Problema: Alcuni messaggi arrivano al server syslog, ma gli eventi informativi, le voci del log di controllo o gli eventi di accesso alla sessione risultano mancanti. Vengono visualizzati solo i difetti principali e critici.

Controllo configurazione:

<#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
```

Causa principale: Il filtro Syslog si verifica in due punti: l'origine (minSev) e la destinazione remota (severity). Solo i messaggi che superano entrambi i filtri vengono inoltrati. Se uno dei due è impostato sopra, informationi messaggi informativi vengono eliminati.

Soluzione: Modificare l'origine del syslog e impostare Gravità minima su informazioni, quindi selezionare audit, events, faults nel campo Include (Includi). Modificare la destinazione remota e impostare Gravità su Informazioni.

Scenario 5: Nessun EPG di gestione assegnato alla destinazione remota

Problema: Nessun messaggio syslog ricevuto sul server remoto. Il gruppo di destinazione è abilitato, la destinazione remota è abilitata e il file di registro locale ha del contenuto.

Controllo configurazione:

<#root>

```
apic1#

moquery -c syslogRemoteDest

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

Causa principale: Senza un Management EPG, l'APIC e gli switch non sanno quale interfaccia fisica usare per inviare i messaggi syslog. I messaggi vengono generati ma non possono essere inoltrati.

Soluzione: Modificare la destinazione remota e selezionare il Management EPG appropriato. Per la gestione fuori banda, selezionare uni/tn-mgmt/mgmtp-default/oob-default. Per la gestione in banda, selezionare l'EPG in banda appropriato.

Scenario 6: Gestione errata EPG (In-Band vs Out-of-Band)

Problema: I messaggi Syslog arrivano in modo intermittente o solo da alcuni nodi. Il server syslog è raggiungibile solo tramite la gestione OOB, ma la destinazione remota fa riferimento all'EPG in-band.

Controllo configurazione:

<#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
```

Se il server syslog è raggiungibile solo attraverso la rete OOB, l'EPG in-band genera messaggi provenienti dall'interfaccia in-band, che non possono raggiungere il server.

Soluzione: Modificare la destinazione remota e impostare Management EPG su uni/tn-mgmt/mgmtp-default/oob-default. Verificare con **ping -c 3 10.1.1.100** dall'host APIC per verificare la raggiungibilità dell'OOB.

Scenario 7: Traffico syslog bloccato dal firewall

Problema: Il file di log locale include contenuto sia sui nodi APIC che sui nodi foglia, la configurazione è corretta, il ping ICMP sul server syslog ha esito positivo, ma il server non riceve messaggi.

Controllo operativo: Eseguire il ping tra l'APIC e il server syslog per verificare la raggiungibilità dell'IP:

<#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
```

Il ping è riuscito, ma i messaggi syslog non arrivano. Il protocollo ICMP (ping) viene eseguito mentre la porta UDP 514 è bloccata.

Causa principale: Un firewall o un ACL tra la rete di gestione e il server syslog blocca la porta UDP 514 (o TCP 514 se il trasporto TCP è configurato). ICMP e UDP sono indipendenti. Il passaggio di ICMP non conferma che UDP 514 sia consentito. Inoltre, ogni foglia e dorso invia syslog direttamente dal proprio indirizzo IP OOB. Un firewall che consente solo agli IP OOB APIC di eliminare i pacchetti syslog provenienti dai nodi dello switch.

Soluzione: Verificare che il firewall consenta l'uso della porta UDP/TCP 514 dall'intervallo di indirizzi IP OOB di tutti i nodi della struttura, inclusi tutti gli APIC, tutti gli switch foglia e tutti gli switch spine. L'acquisizione di un pacchetto sul server syslog conferma l'arrivo dei pacchetti UDP 514.

Scenario 8: Log degli ACL del contratto consentiti/negati non in arrivo

Problema: I registri dei pacchetti (ACLLOG_PKTLOG_PERMIT / ACLLOG_PKTLOG_DENY) consentiti o negati dal contratto non arrivano al server syslog.

Controllo configurazione:

1. Verificare che il livello di gravità dell'origine syslog sia information:
   <#root>

   ```
   apic1#

   moquery -c syslogSrc

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

2. Verificare che il livello di gravità della destinazione remota sia information:
   <#root>

   ```
   apic1#

   moquery -c syslogRemoteDest

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

3. Verificare che il livello di gravità del filtro della funzionalità dei criteri dei messaggi di syslog sia 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. Verificare che la direttiva di registrazione sia abilitata nel filtro del contratto. Passare a Tenant > [tenant] > Contratti > [contratto] > Soggetti > [oggetto] > Filtri e verificare che la colonna Direttive mostri il log per la voce di filtro pertinente.
5. Verificare che i log ACL siano stati generati sullo switch foglia (i log ACL provengono dalla foglia, non dall'APIC):
   <#root>

   ```
   leaf1#

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

<#root>

leaf1#

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

Se non viene visualizzata alcuna ACLLOG voce, la direttiva log non attiva la generazione del log nella foglia. Ciò può indicare una direttiva di contratto configurata in modo errato, che nessun traffico corrispondente sta violando il contratto o che la limitazione della velocità CoPP sta ignorando i pacchetti prima che vengano registrati.

Causa principale: Il livello di gravità del registro ACL del contratto è informational (livello syslog 6). Se un filtro della catena syslog (origine minSev, destinazione remota severityo filtro delle funzionalità dei criteri dei messaggi Syslog (syslogFacilityFilter at uni/fabric/moncommon/sysmsgp/ff-syslog)) è impostato sopra information, i messaggi del log ACL vengono eliminati automaticamente prima di uscire dal nodo dell'infrastruttura.

Soluzione: Impostare minSev su information sull'origine syslog, impostare severity su information sulla destinazione remota, impostare il filtro della syslog struttura minSev su information in Criteri comuni > Criteri messaggi syslog > predefinito, verificare che la direttiva Log sia abilitata sul filtro del contratto e verificare che il firewall consenta il traffico syslog dagli indirizzi IP OB dello switch foglia, non solo dagli IP APIC, in quanto i log ACL vengono inviati dallo switch.

Scenario 9: Syslog si arresta dopo la ridenominazione del gruppo di destinazione

Problema: I messaggi syslog non arrivano più al server remoto dopo la modifica del nome del gruppo di destinazione syslog. La modifica della porta o dell'infrastruttura non causa il problema. La disattivazione e la riattivazione del criterio non comporta la ripresa del recapito dei messaggi.

Causa principale: Si tratta di un difetto software noto. Vedere l'ID bug Cisco CSCwj23752. La ridenominazione del gruppo di destinazione interrompe l'associazione di inoltro syslog interna. È fissato in APIC versione 6.0(6) e successive.

Soluzione: Eseguire l'aggiornamento a APIC versione 6.0(6c) o successive. Per risolvere il problema relativo alle versioni interessate, eliminare il gruppo di destinazione rinominato e ricrearlo con il nome desiderato, quindi riassociare le origini syslog.

Scenario 10: Syslog eccessivo che causa rallentamento dell'interfaccia grafica di APIC

Problema: L'interfaccia grafica APIC diventa lenta e l'utilizzo della CPU APIC è elevato. Questa situazione può verificarsi quando la registrazione degli ACL dei contratti rimane abilitata durante le

normali operazioni, generando un volume elevato di messaggi di syslog informativi che vengono convertiti in eventRecord oggetti nel database APIC.

Causa principale: Quando il livello di gravità del criterio dei messaggi di syslog dei criteri comuni è impostato su information, ogni messaggio di syslog informativo, inclusi i log ACL di grandi volumi, genera un errore eventRecord nell'APIC. Questo può sopraffare il database APIC e causare rallentamento della GUI.

Soluzione:

- Disabilita la registrazione degli ACL del contratto durante le normali operazioni. Abilitarlo solo durante le finestre di risoluzione dei problemi o di manutenzione.
- Se la registrazione ACL deve rimanere abilitata, impostare la gravità dei criteri dei messaggi di syslog su Fabric > Criteri fabric > Criteri > Monitoraggio > Criteri comuni > Criteri dei messaggi di syslog > alerts predefinito. In questo modo si evita che i messaggi di syslog informativi vengano convertiti in eventi, pur consentendo l'inoltro al server syslog remoto.
- Codici di eventi squelch rumorosi non utili dal punto di vista operativo. Il codice di un evento può essere compresso per evitare che generi record di eventi senza influire sull'inoltro del syslog.

Bug noti

I seguenti difetti noti del software influiscono sulla funzionalità del syslog ACI:

- ID bug Cisco CSCwj23752 — La ridenominazione del gruppo di destinazione syslog interrompe il recapito del syslog. Corretto in APIC versione 6.0(6c) e successive.

Criteri di escalation

Raccogliere un supporto tecnico e contattare Cisco TAC quando:

- I messaggi syslog vengono visualizzati /var/log/external/messages localmente nei nodi fabric, gli stati di amministrazione del gruppo di destinazione e della destinazione remota sono entrambi enabled, il Management EPG è corretto, la raggiungibilità della rete è confermata (ping e controllo del firewall), ma i messaggi non arrivano ancora al server remoto.
- I messaggi di syslog arrivano da alcuni nodi fabric ma non da altri, senza alcuna differenza nella configurazione tra di essi, suggerendo un'incoerenza nella distribuzione dei criteri.
- Il profilo del gruppo di destinazione o la destinazione remota è stata riattivata, ma i messaggi non riprendono entro pochi minuti dalla modifica della configurazione.
- I messaggi Syslog non sono più arrivati dopo un aggiornamento APIC, suggerendo un

potenziale difetto del software.

Dati da raccogliere prima di aprire una richiesta TAC:

- Supporto tecnico su richiesta dall'APIC interessato e da un nodo foglia interessato.
- Output di `moquery -c syslogGroup`, `moquery -c syslogProf`, `moquery -c syslogRemoteDest`, e `moquery -c syslogSrc` dall'APIC.
- Output di per `moquery -d uni/fabric/moncommon/systemslsrc/rssystemDestGroup` verificare il collegamento Criteri comuni.
- Coda di `/var/log/external/messages` sia da un APIC che da una foglia interessata.
- Acquisizione dei pacchetti dal server syslog per confermare se i pacchetti UDP/TCP 514 provengono dagli indirizzi OOB dell'infrastruttura.

Riferimenti

- Guida alla configurazione base di Cisco APIC, versione 6.1(x) — Gestione
- Guida di riferimento ai messaggi di sistema Cisco ACI
- Guida alla gestione di errori, eventi e messaggi di sistema Cisco ACI
- White paper sulla guida al contratto Cisco ACI
- Risoluzione dei problemi relativi a un'interfaccia grafica APIC lenta

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).