Configurar e solucionar problemas de Syslog na ACI

Introdução

Este documento descreve como configurar, verificar e solucionar problemas de registro do sistema (syslog) na Cisco Application Centric Infrastructure (ACI). Ele abrange o fluxo de trabalho completo de configuração, verificação programática usando o modelo de objeto gerenciado (MO) do Application Policy Infrastructure Controller (APIC) e um fluxo de trabalho estruturado de solução de problemas para controladores APIC e switches leaf e spine.

Overview

O syslog da ACI é totalmente orientado por políticas. Ao contrário do software Cisco NX-OS® autônomo, não há comandos CLI nos switches leaf ou spine da ACI **logging server**. Toda a configuração de syslog é feita por meio de políticas do APIC que o APIC envia para cada nó de estrutura automaticamente.

Principais componentes

O subsistema syslog na ACI é criado a partir dos seguintes objetos gerenciados:

- Syslog Destination Group (syslogGroup) — O contêiner de nível superior para todos os destinos de syslog. Controla o formato da mensagem (estilo ACI ou NX-OS) e as opções de carimbo de data/hora. Ele pode conter um ou mais destinos remotos, um destino de arquivo local e um destino de console.
- Syslog Profile (syslogProf) — Um filho do grupo de destino que controla o estado administrativo em nível de grupo e o protocolo de transporte (UDP, TCP ou SSL).
- Destino remoto de syslog (syslogRemoteDest) — Um filho do grupo de destino que representa um servidor syslog remoto. Controla o IP do servidor ou o nome do host, a porta, o filtro de gravidade, o recurso de syslog e o grupo de endpoint de gerenciamento (EPG) usado para acessar o servidor.
- Arquivo local de syslog (syslogFile) — Um filho do grupo de destino que controla a gravação de mensagens de syslog no arquivo local /var/log/external/messages em cada nó de malha.
- Origem de Syslog (syslogSrc) — Anexada a uma política de monitoramento. Controla quais tipos de mensagem (auditoria, eventos, falhas, sessão) e a severidade mínima são enviados, além de links para o grupo de destino por meio de um syslogRsDestGroup relacionamento.

Pontos de conexão da origem do Syslog

A ACI usa quatro escopos de política de monitoramento que controlam quais nós e objetos geram mensagens de syslog:

- Política de monitoramento comum (monCommonPol, uni/fabric/moncommon) — escopo de toda a malha. Uma política de monitoramento básica que se aplica a todas as falhas e eventos e é implantada automaticamente em todos os nós (switches leaf e spine) e em todos os controladores (APICs) na malha. Abrange todas as hierarquias de malha, acesso e locatário. Encontrado em Fabric > Fabric Policies > Policies > Monitoring > Common Policy.
- Política de monitoramento de malha (monInfraPol, uni/infra/moninfra-default) — escopo de malha. Gera syslog para objetos em nível de estrutura: portas de estrutura, placas, componentes do chassi e bandejas de ventilador. Encontrado em Fabric > Fabric Policies > Policies > Monitoring > default.
- Access Monitoring Policy (monFabricPol, uni/fabric/monfab-default) — Escopo de acesso (infraestrutura). Gera syslog para componentes de acesso: portas de acesso, dispositivos FEX (Fabric Extender) e eventos de controlador de máquina virtual (VM). Encontrado em Fabric > Access Policies > Policies > Monitoring Policies > default.
- Política de Monitoramento de Locatário (monEPGPol, uni/tn-common/monepg-default) — Escopo do locatário. Gera syslog para objetos com escopo de espaço: grupos de endpoint (EPGs), perfis de aplicativos e serviços. Encontrado em cada locatário em [Locatário] > Políticas de monitoramento > padrão.

Note: A política de monitoramento comum é o ponto de partida recomendado para a configuração de syslog porque fornece cobertura em toda a malha em todas as hierarquias e é implantada automaticamente em todos os nós. As Políticas de monitoramento de acesso e estrutura podem ser configuradas além da Política comum para um controle mais granular sobre hierarquias de objetos específicos ou, em vez da Política comum, para restringir o syslog a um escopo mais restrito.

Formato de mensagem do Syslog

As mensagens de syslog da ACI seguem o formato RFC 3164 quando o formato do grupo é definido como aci (o padrão):

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

Por exemplo:

```
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
```

O corpo da mensagem inclui o código de falha da ACI, o estado do ciclo de vida (por exemplo, soaking, retaining, cleared), a gravidade e o nome distinto (DN) do objeto afetado, tornando as mensagens autodescritivas.

Três opções de formato de mensagem estão disponíveis:

- aci (padrão) — formato compatível com RFC 3164. Recomendado para a maioria das implantações.
- nxos — formato de estilo NX-OS. Use esta opção se a plataforma syslog esperar mensagens formatadas no NX-OS.
- Registro aprimorado (APIC 5.2(8) e posterior) — formato compatível com RFC 5424 com carimbos de data/hora aprimorados que incluem o ano.

Mapeamento de severidade

O campo de gravidade do syslog é um único dígito de 0 (mais grave) a 7 (menos grave). A tabela a seguir mostra o mapeamento entre os níveis de gravidade do syslog e a terminologia de gravidade da ACI/International Telecommunication Union (ITU):

Severidade do Syslog	Nível de ACI / ITU	Descrição
0 — emergência	—	O sistema está inutilizável
1 — alerta	Crítico	Ação imediata necessária
2 — crítico	Principal	Condição crítica
3 — erro	Menor	Condição de erro
4 — aviso	Aviso	Condição de aviso
5 — notificação	Indeterminado/Apagado	Condição normal, mas significativa
6 — informativo	—	Apenas mensagem informativa
7 — debugging	—	Somente saída de depuração

Opções de transporte

A ACI suporta três protocolos de transporte para syslog remoto:

- UDP (padrão) — Disponível em todas as versões do APIC. Entrega padrão do tipo "fogo e esquece".
- TCP — Disponível no APIC versão 5.2(3) e posterior. Fornece entrega confiável com transporte orientado a conexão.
- SSL — Disponível no APIC versão 5.2(4) e posterior. Fornece transporte criptografado

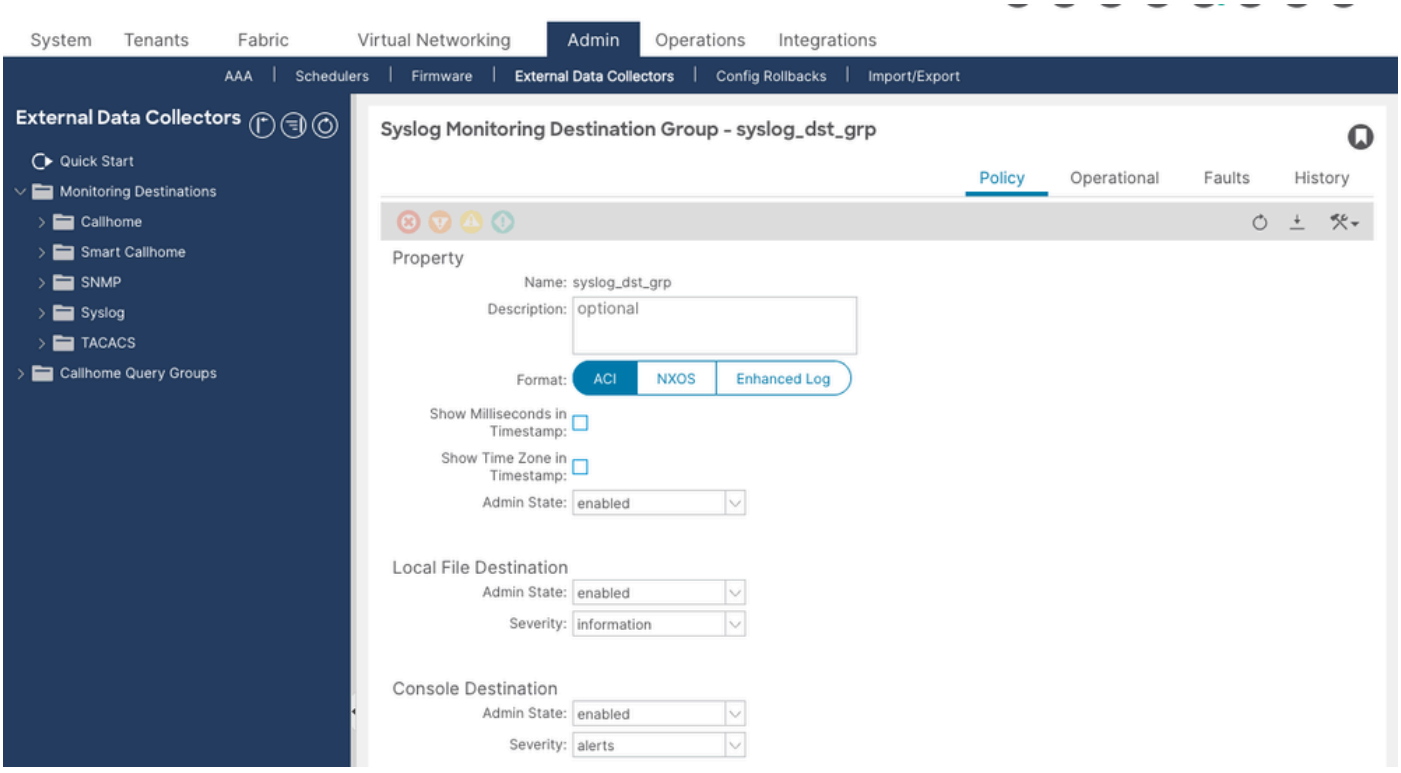
usando TLS. Cada nó ACI (APIC ou switch) atua como o cliente TLS e inicia uma conexão de saída com o Servidor syslog. O certificado do servidor deve ser carregado no APIC em Admin > AAA > Security > Public Key Management > Certificate Authorities.

Note: Se um destino remoto for configurado com transporte SSL e o APIC for submetido a downgrade para uma versão que não suporte SSL, o protocolo de transporte reverterá automaticamente para UDP. Verifique se o Servidor syslog também pode aceitar conexões UDP como um fallback.

Configuração

As etapas a seguir configuram o syslog da ACI de ponta a ponta. Conclua todas as etapas para ativar o encaminhamento de syslog dos controladores APIC e dos switches leaf e spine.

Passo 1: Crie o grupo de destino do Syslog



O grupo de destino define para onde as mensagens de syslog são enviadas e em que formato. Crie isso primeiro, pois as origens de syslog configuradas em etapas posteriores fazem referência a esse grupo por nome.

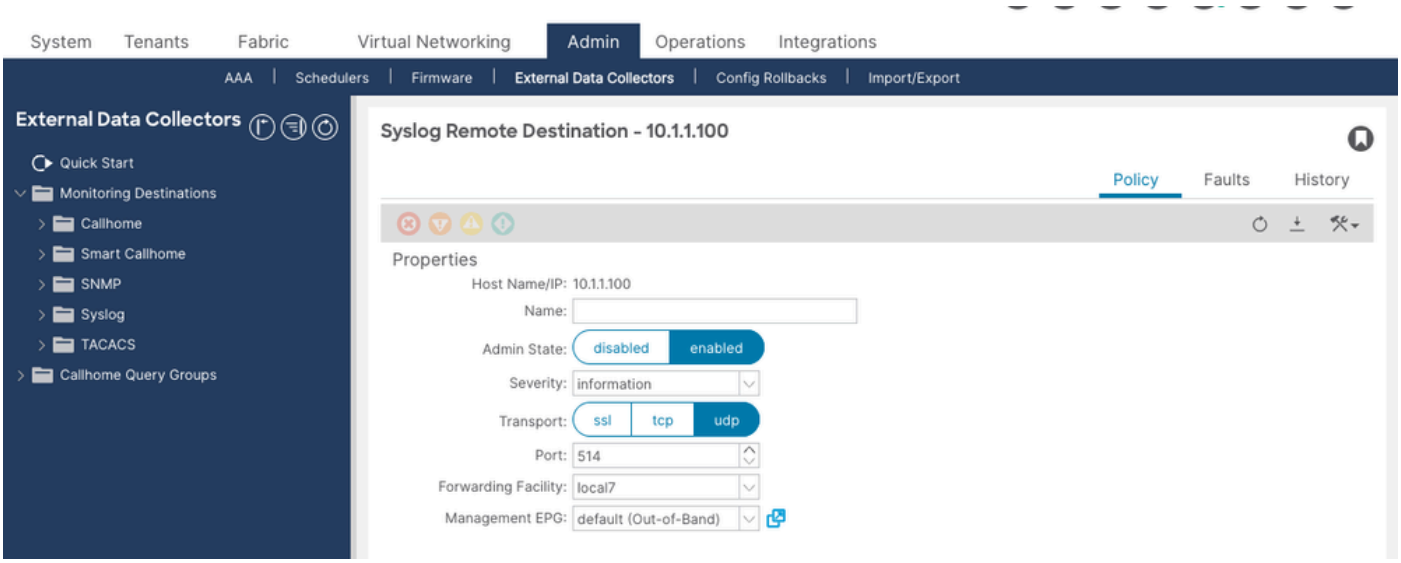
Navegue até Admin > External Data Collectors > Monitoring Destinations > Syslog. Clique com o botão direito do mouse em Syslog e selecione Create Syslog Monitoring Destination Group.

No assistente, configure o seguinte na primeira página (perfil de grupo):

- Nome — Um nome descritivo como Syslog-Dest-Group.
- Formato — aci (padrão, compatível com RFC 3164) ou nxos.
- Estado do administrador — enabled.
- Estado de Administração de Destino de Arquivo Local — enabled (recomendado). Isso grava mensagens em todos /var/log/external/messages os nós de estrutura e é essencial para a solução de problemas locais, mesmo quando um servidor remoto está inacessível.
- Severidade do destino do arquivo local — information.
- Console Destination Admin State — disabled (recomendado para ambientes de produção).

Clique em Next. Na segunda página, clique em + na área Criar destinos remotos para adicionar um servidor syslog remoto.

Passo 2: Adicionar um destino remoto



Configure o servidor syslog remoto na caixa de diálogo Create Syslog Remote Destination:

- Host — Endereço IP do Servidor syslog. Use um endereço IP em vez de um nome de host. Se você usar um nome de host, deverá garantir que o servidor DNS (Domain Name System) esteja acessível pela interface de gerenciamento fora de banda (OOB). Servidores DNS acessíveis apenas por meio da conectividade em banda podem falhar ao resolver quando mensagens de syslog são geradas durante uma interrupção de rede.
- Estado do administrador — enabled.
- Severidade — information (recomendado). Esta é a severidade mínima enviada para este servidor remoto específico.
- Porta — 514 (padrão).
- Recurso — local7 (padrão). Defina-o para corresponder ao valor do recurso que seu Servidor

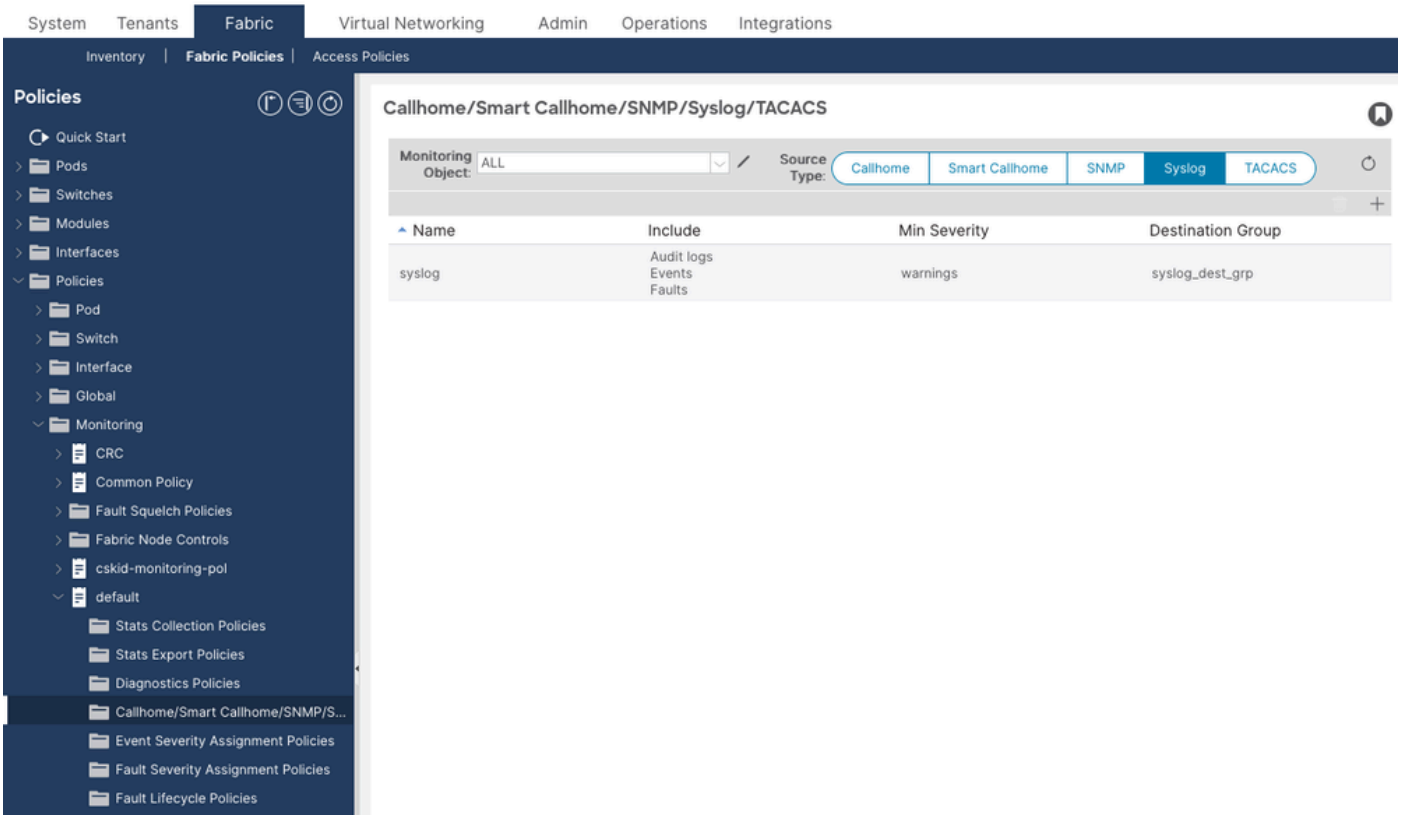
syslog está configurado para aceitar e rotear.

- Transporte — udp (padrão). Use tcp ssl para entrega confiável (requer APIC 5.2(3) ou posterior), ou para transporte criptografado (requer APIC 5.2(4) ou posterior e um certificado carregado para o APIC).
- EPG de gerenciamento — Selecione o EPG de gerenciamento que tem acessibilidade ao Servidor syslog. Para gerenciamento OOB: uni/tn-mgmt/mgmtp-default/oob-default. Para o gerenciamento em banda, selecione o EPG em banda apropriado. Este campo não pode estar vazio.

Clique em OK e em Concluir.

Note: Você pode adicionar vários destinos remotos ao mesmo grupo de destinos. Cada destino pode ter um limite de severidade, instalação e protocolo de transporte diferente.

Passo 3: Crie uma fonte de Syslog na política de monitoramento de estrutura



Esta etapa configura o syslog para a hierarquia de objetos de estrutura — portas de estrutura, placas, componentes do chassi e bandejas de ventilador. Isso complementa a Política de Monitoramento Comum (Etapa 4) com o controle específico da hierarquia.

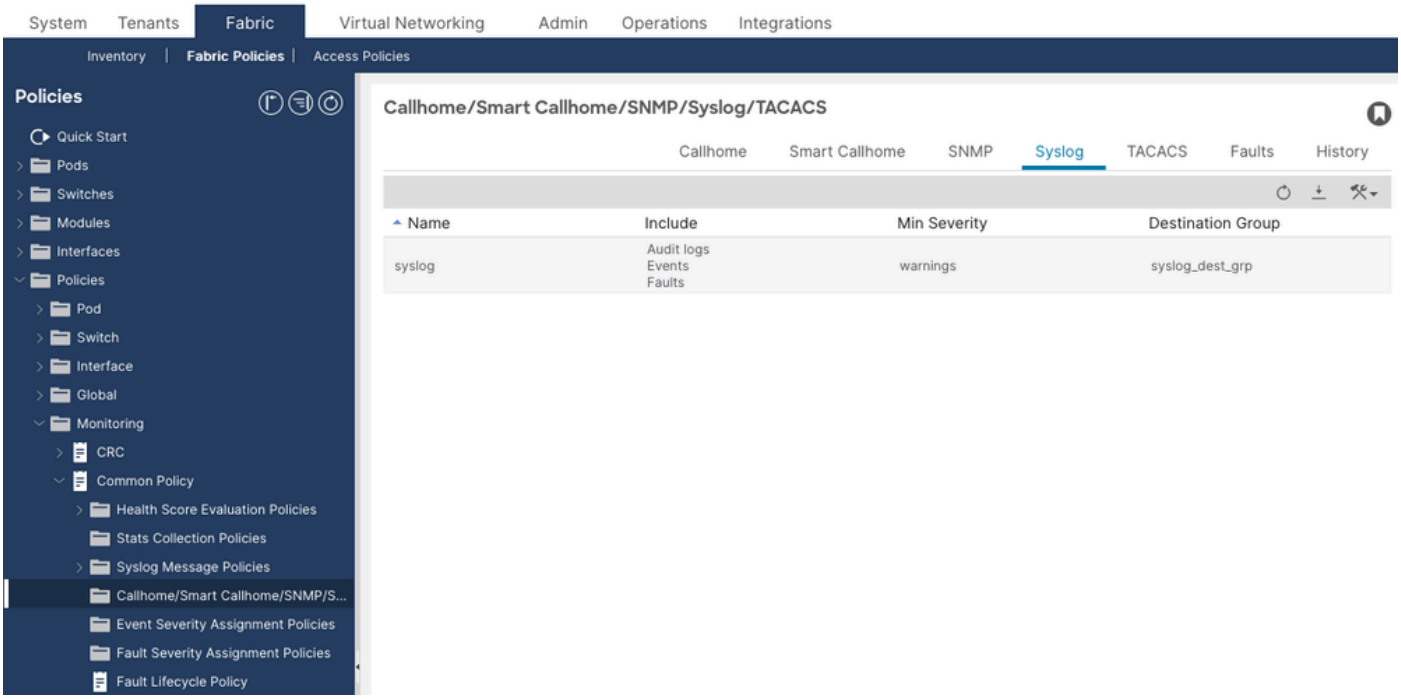
Navegue até Fabric > Fabric Policies > Policies > Monitoring > default > Callhome/Smart Callhome/SNMP/Syslog/TACACS.

No painel direito, defina Tipo de origem como Syslog. Clique em + para criar uma origem de syslog:

- Nome — Um nome descritivo como Syslog-Source-Fabric.
- Gravidade mínima — information (recomendado para cobertura completa).
- Incluir — Verificar auditoria, eventos e falhas. Opcionalmente, adicione session para eventos de login e logout.
- Grupo Destino — Selecione o grupo destino criado na Etapa 1.

Clique em Submit.

Passo 4: Configurar a política de monitoramento comum (Syslog de todo o sistema)

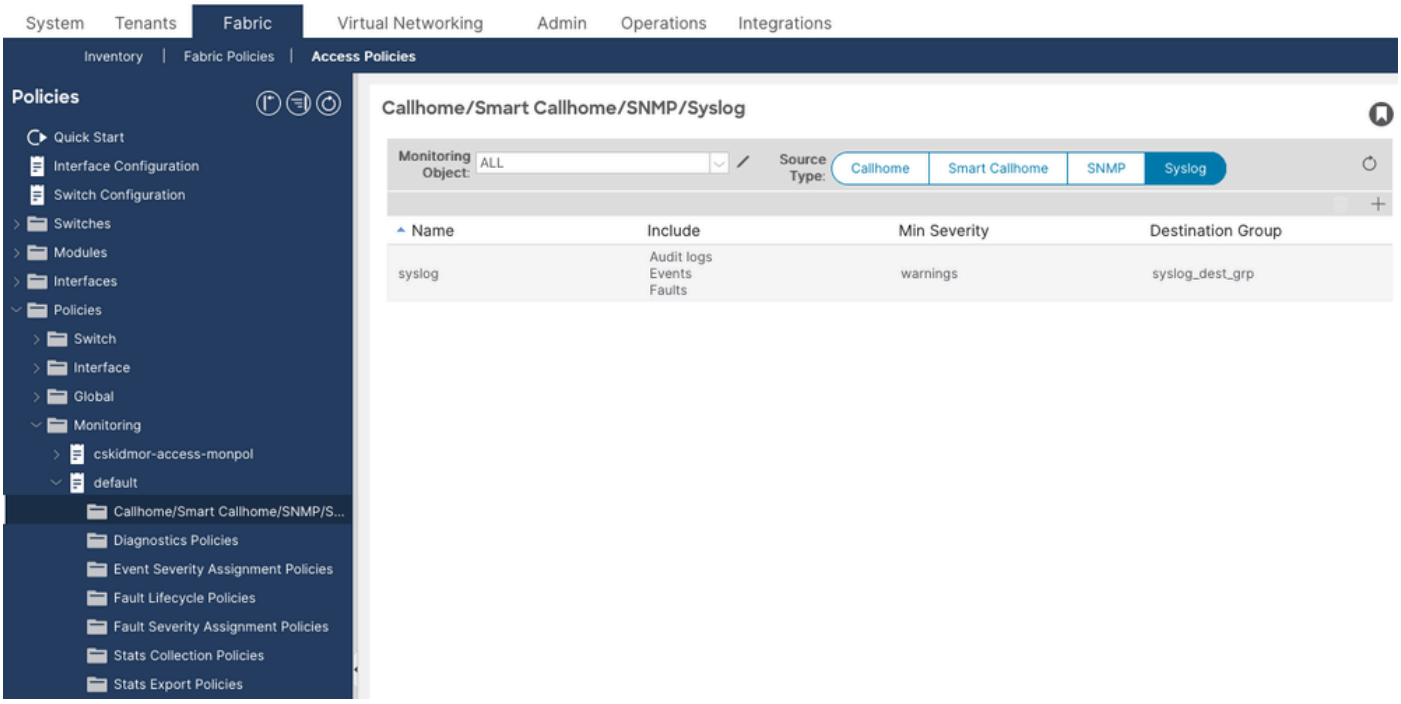


A política de monitoramento comum fornece cobertura de syslog em todo o sistema que é implantada automaticamente em todos os nós e controladores na malha. Esta etapa vincula a origem do syslog do sistema ao grupo de destino.

Navegue até Fabric > Fabric Policies > Policies > Monitoring > Common Policy. Na seção Syslog, vincule a origem do syslog do sistema ao grupo de destino criado na Etapa 1.

A origem do syslog do sistema de política comum usa o MO syslogRsSystemDestGroup no DN uni/fabric/moncommon/systemslsrc/rssystemDestGroup.

Passo 5: Crie uma origem de Syslog na política de monitoramento de acesso



Esta etapa configura o syslog para a hierarquia de objetos de acesso — portas de acesso, dispositivos FEX (Fabric Extender) e eventos do controlador da máquina virtual (VM). Isso complementa a Política de Monitoramento Comum (Etapa 4) com o controle específico da hierarquia.

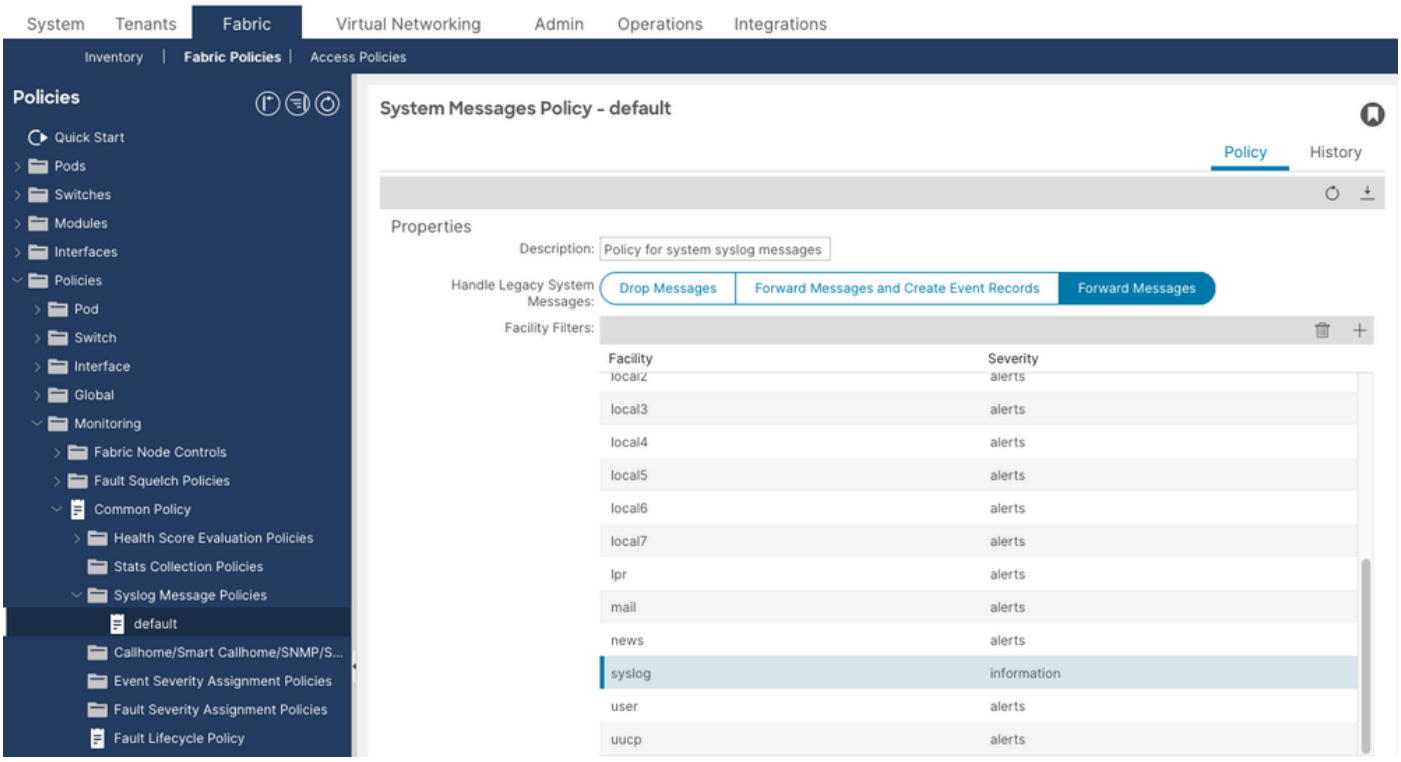
Navegue até Fabric > Access Policies > Policies > Monitoring Policies > default > Callhome/SNMP/Syslog.

Defina Source Type como Syslog. Clique em + e defina as mesmas configurações como Etapa 3:

- Nome — Por exemplo, Syslog-Source-Access.
- Gravidade mínima — information.
- Incluir — Verificar auditoria, eventos e falhas.
- Grupo de Destino — Selecione o mesmo grupo de destino.

Clique em Submit.

Etapa 6 (opcional): Ajuste a política de mensagens do Syslog para registro de ACL de contrato



Se você precisar que os logs de permissão ou negação de pacotes de ACL de contrato (ACLLOG_PKTLOG_PERMIT / ACLLOG_PKTLOG_DENY) apareçam no Servidor syslog remoto, o filtro de recurso de mensagem syslog deve ser definido como severidade informativa.

Navegue até Fabric > Fabric Policies > Policies > Monitoring > Common Policy > Syslog Message Policies > default. Na lista de filtros da instalação, selecione a instalação syslog e defina sua Severidade mínima como information. Este é o syslogFacilityFilter MO no DN uni/fabric/moncommon/sysmsgp/ff-syslog.

Note: Para permitir e negar registros da ACL de contrato para acessar o Servidor syslog remoto, quatro condições devem ser atendidas: (1) o syslog source minSev deve ser uma informação, (2) a severidade do destino remoto deve ser uma informação, (3) o syslog Syslog Message Policy do filtro de recurso minSev deve ser uma informação, e (4) a diretiva Log deve ser habilitada na entrada do filtro do contrato. Quando todas as três condições são atendidas, as mensagens de log da ACL se originam do switch de folha (não do APIC), de modo que aparecem primeiro em `/var/log/external/messages` na folha. As taxas de registro de pacote ACL de contrato são limitadas por CoPP: o padrão dos logs deny é de 500 pacotes por segundo (pps) e permit logs é de 300 pps por leaf.

Note: O uso da diretiva Log em filtros em contratos de gerenciamento não é suportado e causa falha na implantação da regra de zoneamento. Aplique o registro de contratos somente a contratos de plano de dados de locatário.

Verificar a configuração

Verifique a configuração antes de solucionar qualquer problema operacional. A causa raiz mais comum de mensagens de syslog ausentes é a configuração incorreta, não uma falha de rede ou de software.

Verifique o grupo de destino e o perfil

Execute **moquery -c syslogGroup** no APIC para confirmar a existência de grupos de destino e verifique seus atributos:

<#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
```

Em seguida, verifique o perfil (estado admin de nível de grupo) com **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
```

Para localizar qualquer grupo de destinos cujo perfil esteja desativado, execute:

<#root>

```
apic1#

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

Um resultado aqui significa que o grupo de destino não está encaminhando nenhum tráfego de syslog, independentemente do estado do administrador de destino remoto.

Verifique o destino remoto

Execute **moquery -c syslogRemoteDest** para verificar cada configuração de servidor 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
```

Três atributos requerem atenção especial:

- EstadoAdmin: deve ser enabled. Se desabilitado, este servidor remoto específico não recebe nada.
- epgDn: não deve estar vazio. Um espaço vazio epgDn significa que a estrutura não sabe de qual interface enviar o tráfego de syslog, portanto nenhuma mensagem sai da estrutura.
- Estado da operadora: desconhecido: esse valor é esperado e não indica um problema. A ACI não investiga ativamente a acessibilidade dos servidores syslog.

Verificar as fontes de Syslog

Executar **moquery -c syslogSrc** para confirmar se as fontes estão sob as políticas de monitoramento corretas:

<#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
```

Confirme se as fontes estão de acordo com as políticas de monitoramento apropriadas:

- Uma origem sob uni/fabric/moncommon — a Common Monitoring Policy, para cobertura em toda a malha de todos os nós e todas as hierarquias de objetos.
- Uma origem sob uni/infra/moninfra-default — a Política de monitoramento de estrutura, para objetos de estrutura (portas de estrutura, placas, chassi).
- Uma origem sob uni/fabric/monfab-default — a Access Monitoring Policy, para objetos de nível de acesso (portas de acesso, FEX, controladores de VM).

Verifique também se a origem do syslog do sistema Common Monitoring Policy está vinculada:

<#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 o registro de ACL de contrato for necessário, verifique a severidade do filtro de recurso de política de mensagens do Syslog com **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
```

Verificar o arquivo de log local

O arquivo local em /var/log/external/messages é a maneira mais direta de confirmar que as mensagens de syslog estão sendo geradas em qualquer nó de estrutura, mesmo quando um servidor remoto não está acessível. Verifique-o no APIC e em um switch leaf:

<#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 esse arquivo estiver vazio ou não estiver sendo atualizado em um nó, as mensagens não serão geradas na origem. Se o arquivo tiver conteúdo, mas o servidor syslog remoto não estiver recebendo mensagens, o problema está no encaminhamento (grupo de destino, rede ou firewall), e não na geração de mensagens.

Verifique a acessibilidade ao Servidor Syslog

Execute um ping do APIC para o Servidor syslog a fim de verificar a alcançabilidade IP na rede de gerenciamento:

```
<#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
```

A partir de um switch leaf ou spine, use `iping` com o flag `-V` para especificar o VRF. Use `management` para fora da banda ou `mgmt:inb` para dentro da banda, dependendo de qual EPG de gerenciamento está atribuído ao destino do 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
```

Um ping bem-sucedido confirma a acessibilidade do IP, mas não confirma se a porta UDP ou

TCP 514 é permitida. O Internet Control Message Protocol (ICMP) e o syslog usam protocolos diferentes.

Troubleshooting

Fluxo de Trabalho de Triagem

Use a seguinte árvore decisória quando as mensagens de syslog não estiverem chegando ao servidor 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
```

Cenários comuns

Cenário 1: Nenhuma mensagem de Syslog recebida no servidor remoto

Problema: O grupo de destino de syslog e o destino remoto estão configurados, mas nenhuma mensagem chega ao servidor remoto. O arquivo local /var/log/external/messages no APIC e nos switches contém entradas recentes.

Verificação de configuração:

<#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 raiz: O estado do administrador de destino remoto é disabled. Isso pode acontecer se o destino tiver sido criado, mas tiver sido desabilitado inadvertidamente ou se tiver sido desabilitado durante a manutenção e nunca tiver sido reabilitado.

Solução: Navegue até Admin > External Data Collectors > Monitoring Destinations > Syslog > [nome do grupo] > Remote Destinations > [servidor]. Edite o destino remoto e defina Admin State como enabled.

Cenário 2: O Perfil Do Grupo De Destino Do Syslog Está Desabilitado

Problema: Nenhuma mensagem é encaminhada de nenhum nó, mesmo que o estado do administrador de destino remoto esteja habilitado.

Verificação de configuração:

<#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 raiz: O estado de administração syslogProf controla todo o grupo de destino. Quando desativado, nenhuma mensagem é encaminhada de qualquer nó, independentemente dos estados de destino remoto individuais.

Solução: Navegue até Admin > External Data Collectors > Monitoring Destinations > Syslog > [group name]. Edite o perfil e defina Admin State como enabled.

Cenário 3: Eventos em falta — Política comum de acompanhamento não ligada

Problema: As mensagens de syslog de alguns nós ou hierarquias de objetos não estão acessando o servidor remoto, mesmo que uma origem de syslog esteja configurada na Política de Monitoramento de Malha ou Acesso.

Verificação de configuração:

<#root>

```
apic1#

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

Total Objects shown: 0
```

A origem do syslog do sistema de Política de Monitoramento Comum não está vinculada ao grupo de destino.

Causa raiz: A Common Monitoring Policy (uni/fabric/moncommon) fornece cobertura de syslog em toda a malha em todas as hierarquias e é implantada automaticamente em todos os nós e controladores. Sem ele, somente os eventos correspondentes às hierarquias específicas da Fabric ou da Access Monitoring Policy são encaminhados. A Política de monitoramento de estrutura (uni/infra/moninfra-default) abrange objetos no nível da estrutura, e a Política de monitoramento de acesso (uni/fabric/monfab-default) abrange objetos no nível do acesso, mas não fornece a cobertura em toda a estrutura que a Política comum oferece.

Solução: Navegue até Fabric > Fabric Policies > Policies > Monitoring > Common Policy. Na seção Syslog, vincule a origem do syslog do sistema ao grupo de destino. Verifique com **moquery -d uni/fabric/moncommon/systemslsrc/rssystemDestGroup** o se o aponta para o seu grupo de tDn destino.

Cenário 4 : Severidade Muito Restritiva — Mensagens Esperadas Ausentes

Problema: Algumas mensagens chegam ao Servidor syslog, mas eventos informativos, entradas de log de auditoria ou eventos de logon de sessão estão ausentes. Somente falhas críticas e principais são vistas.

Verificação de configuração:

<#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 raiz: A filtragem de syslog ocorre em dois pontos: origem (minSev) e destino remoto (severity). Somente as mensagens que passam ambos os filtros são encaminhadas. Se qualquer um for definido acima information, as mensagens informativas serão descartadas.

Solução: Edite a origem do syslog e defina a Severidade mínima como informações, e marque audit, events, faults no campo Incluir. Edite o destino remoto e defina Severity como information.

Cenário 5 : Nenhum EPG de gerenciamento atribuído ao destino remoto

Problema: Nenhuma mensagem de syslog é recebida no servidor remoto. O grupo de destino está habilitado, o destino remoto está habilitado e o arquivo de log local tem conteúdo.

Verificação de configuração:

<#root>

```
apic1#

moquery -c syslogRemoteDest

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

Causa raiz: Sem um EPG de gerenciamento, o APIC e os switches não sabem qual interface física usar para enviar mensagens de syslog. As mensagens são geradas, mas não podem ser encaminhadas.

Solução: Edite o destino remoto, selecione o EPG de gerenciamento apropriado. Para gerenciamento OOB, selecione uni/tn-mgmt/mgmtp-default/oob-default. Para o gerenciamento em banda, selecione o EPG em banda apropriado.

Cenário 6 : EPG de gerenciamento incorreto (dentro da banda versus fora da banda)

Problema: As mensagens de syslog chegam intermitentemente ou apenas de alguns nós. O Servidor syslog só é alcançável através do gerenciamento OOB, mas o destino remoto faz referência ao EPG em banda.

Verificação de configuração:

<#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 o Servidor syslog for alcançável somente através da rede OOB, o EPG in-band resultará em mensagens sendo originadas da interface in-band, que não pode alcançar o servidor.

Solução: Edite o destino remoto e altere o EPG de gerenciamento para uni/tn-mgmt/mgmtp-default/oob-default. Verifique com **ping -c 3 10.1.1.100** a partir da base APIC para confirmar a acessibilidade OB.

Cenário 7 : Firewall Bloqueando Tráfego Syslog

Problema: O arquivo de log local tem conteúdo nos nós de folha e APIC, a configuração está correta, o ping ICMP para o Servidor syslog é bem-sucedido, mas nenhuma mensagem chega ao servidor.

Verificação operacional: Execute um ping do APIC para o Servidor syslog para verificar a acessibilidade do 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
```

O ping é bem-sucedido, mas as mensagens de syslog não chegam. O ICMP (ping) é aprovado enquanto a porta UDP 514 está bloqueada.

Causa raiz: Um firewall ou ACL entre a rede de gerenciamento e o Servidor syslog está bloqueando a porta UDP 514 (ou TCP 514 se o transporte TCP estiver configurado). O ICMP e o UDP são independentes — A passagem pelo ICMP não confirma se o UDP 514 é permitido. Além disso, cada leaf e spine enviam syslog diretamente de seu próprio endereço IP OOB. Um firewall que permite apenas IPs OOB do APIC descarta pacotes de syslog originados de nós de switch.

Solução: Verifique se o firewall permite a porta UDP/TCP 514 do intervalo de endereços IP OOB de todos os nós de estrutura, incluindo todos os APICs, todos os switches leaf e todos os switches spine. Uma captura de pacote no Servidor syslog confirma se os pacotes UDP 514 estão chegando.

Cenário 8 : Logs de permissão/negação de ACL de contrato não chegando

Problema: Os registros de pacotes de permissão ou negação de contrato (ACLLOG_PKTLOG_PERMIT / ACLLOG_PKTLOG_DENY) não estão chegando ao Servidor syslog.

Verificação de configuração:

1. Verifique se a gravidade da origem do syslog é information:
   <#root>

   ```
   apic1#
   ```

   moquery -c syslogSrc

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

2. Verifique se a gravidade do destino remoto é information:
   <#root>

   ```
   apic1#
   ```

   moquery -c syslogRemoteDest

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

3. Verifique se a severidade do filtro de recurso da Política de Mensagens do Syslog é 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. Verifique se a diretiva log está habilitada no filtro de contrato. Navegue para Locatários > [locatário] > Contratos > [contrato] > Assuntos > [assunto] > Filtros e confirme se a coluna Diretivas mostra log para a entrada de filtro relevante.
5. Verifique se os logs ACL estão sendo gerados no switch leaf (os logs ACL se originam da leaf, não do APIC):
   <#root>

   ```
   leaf1#
   ```

   show logging ip access-list internal packet-log deny

   <#root>

   ```
   leaf1#
   ```

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

   Se nenhuma ACLLOG entrada aparecer, a diretiva log não está disparando a geração de log na folha. Isso pode indicar uma diretiva de contrato configurada incorretamente, que nenhum tráfego correspondente está atingindo o contrato ou que o limite de taxa de CoPP

está descartando pacotes antes de serem registrados.

Causa raiz: O nível de gravidade do log da ACL do contrato é informational (nível 6 do syslog). Se qualquer filtro na cadeia de syslog — origem minSev, destino remoto severity, ou o filtro de recurso de política de mensagens do Syslog (syslogFacilityFilter em uni/fabric/moncommon/sysmsgp/ff-syslog) — estiver definido acima information, as mensagens de log da ACL serão descartadas silenciosamente antes de sair do nó de malha.

Solução: Defina minSev como information na origem de syslog, defina severity como information no destino remoto, defina o filtro de syslog recurso minSev como information em Common Policy > Syslog Message Policies > default, confirme se a diretiva Log está habilitada no filtro de contrato e verifique se o firewall permite o tráfego de syslog dos endereços IP OOB do switch folha, não apenas os IPs APIC, porque os logs ACL são enviados do switch.

Cenário 9 : O Syslog é interrompido após renomear o grupo de destino

Problema: As mensagens de syslog param de chegar ao servidor remoto depois que o nome do grupo de destino de syslog é alterado. Alterar o porto ou a instalação não causa esse problema. Desativar e reativar a política não retoma a entrega de mensagens.

Causa raiz: Este é um defeito de software conhecido. Consulte o bug da Cisco ID CSCwj23752. A renomeação do grupo de destino interrompe a associação de encaminhamento de syslog interno. Ele é corrigido no APIC versão 6.0(6) e posterior.

Solução: Atualize para o APIC versão 6.0(6c) ou posterior. Como solução alternativa para as versões afetadas, exclua o grupo de destinos renomeado e recrie-o com o nome desejado e, em seguida, reassocie as origens de syslog.

Cenário 10 : Excesso de Syslog, causando lentidão na GUI do APIC

Problema: A GUI do APIC fica lenta e a utilização da CPU do APIC é alta. Isso pode ocorrer quando o registro de ACL de contrato é deixado ativado durante as operações normais, gerando um alto volume de mensagens de syslog informativas que são convertidas em eventRecord objetos no banco de dados do APIC.

Causa raiz: Quando a gravidade Common Policy Syslog Message Policy é definida como information, cada mensagem de syslog informativa, incluindo logs ACL de alto volume, gera um eventRecord no APIC. Isso pode sobrecarregar o banco de dados do APIC e causar lentidão da GUI.

Solução:

- Desative o registro de ACL de contrato durante as operações normais. Habilite-o somente durante as janelas de solução de problemas ou manutenção.
- Se o registro da ACL precisar permanecer habilitado, defina a severidade da política de mensagens do Syslog como alerts em Fabric > Fabric Policies > Policies > Monitoring > Common Policy > Syslog Message Policies > default. Isso evita que as mensagens de syslog informativas sejam convertidas em eventos, permitindo ainda que sejam encaminhadas ao servidor syslog remoto.
- Códigos de evento com ruído Squelch que não são operacionalmente úteis. Um código de evento pode ser compactado para impedir que gere registros de eventos sem afetar o encaminhamento de syslog.

Erros conhecidos

Os seguintes defeitos de software conhecidos afetam a funcionalidade do syslog da ACI:

- ID de bug da Cisco CSCwj23752 — A renomeação do grupo de destino de syslog interrompe a entrega de syslog. Corrigido no APIC versão 6.0(6c) e posterior.

Critérios de escalonamento

Colete um suporte técnico e envolva o Cisco TAC quando:

- As mensagens de syslog aparecem localmente nos nós da malha, os estados de administração do grupo de destino e do destino remoto são ambos, o EPG de gerenciamento está correto, a acessibilidade da rede é confirmada (/var/log/external/messages enabledping e passagem de verificação do firewall), mas as mensagens ainda não chegam ao servidor remoto.
- As mensagens de syslog chegam de alguns nós de estrutura, mas não de outros, sem nenhuma diferença na configuração entre eles, sugerindo uma inconsistência na implantação da política.
- O perfil do grupo de destino ou o destino remoto foi reativado, mas as mensagens não são retomadas dentro de alguns minutos após a alteração da configuração.
- As mensagens de syslog pararam de chegar após uma atualização do APIC, sugerindo um possível defeito de software.

Dados a serem coletados antes da abertura de um caso de TAC:

- Suporte técnico sob demanda do APIC afetado e um nó de folha afetado.
- Resultado de moquery -c syslogGroup, moquery -c syslogProf, moquery -c syslogRemoteDeste moquery -c syslogSrc do APIC.

- Saída de para `moquery -d uni/fabric/moncommon/systemslsrc/rssystemDestGroup` verificar o link de Política comum.
- Parte posterior `/var/log/external/messages` de uma folha afetada e de um APIC.
- Captura de pacote do Servidor syslog confirmando se os pacotes UDP/TCP 514 estão chegando dos endereços OOB da malha.

Referências

- Guia de configuração básica do Cisco APIC, versão 6.1(x) — Gerenciamento
- Guia de referência de mensagens do sistema da Cisco ACI
- Guia de gerenciamento de falhas, eventos e mensagens do sistema da Cisco ACI
- White paper do guia de contratos da Cisco ACI
- Solucionar problemas de uma GUI do APIC lenta

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.