在ACI中配置系统日志并对其进行故障排除

简介

本文档介绍如何在思科以应用为中心的基础设施(ACI)中配置、验证系统日志记录(syslog)并对其进行故障排除。 它包括完整的配置工作流、使用应用策略基础设施控制器(APIC)托管对象(MO)模型的编程验证，以及针对APIC控制器和枝叶和主干交换机的结构化故障排除工作流。

概述

ACI系统日志完全由策略驱动。与独立的Cisco NX-OS®软件不同，ACI枝叶**logging server**或主干交换机上没有CLI命令。所有系统日志配置均通过APIC自动推送到每个交换矩阵节点的APIC策略完成。

关键组件

ACI中的系统日志子系统由以下托管对象构建：

- Syslog Destination Group(syslogGroup)-所有系统日志目标的顶级容器。它控制消息格式（ACI或NX-OS样式）和时间戳选项。它可以包含一个或多个远程目标、本地文件目标和控制台目标。
- Syslog Profile(syslogProf) — 控制组级别管理状态和传输协议（UDP、TCP或SSL）的目标组的子级。
- Syslog Remote Destination(syslogRemoteDest) — 代表一个远程syslog服务器的目标组的子级。控制用于访问服务器的服务器IP或主机名、端口、严重性过滤器、系统日志设施和管理终端组(EPG)。
- Syslog Local File(syslogFile) — 目标组的子级，控制将系统日志消息写入每个交换矩阵节点上的/var/log/external/messages本地文件。
- Syslog Source(syslogSrc)-附加到监控策略。控制发送哪些消息类型（审计、事件、故障、会话）和最低严重性，以及通过关系链接到目标syslogRsDestGroup组。

系统日志源连接点

ACI使用四个监控策略范围，控制哪些节点和对象生成系统日志消息：

- 通用监控策略monCommonPol(uni/fabric/moncommon,) — 交换矩阵范围。适用于所有故障和事件的基本监控策略，可自动部署到交换矩阵中的所有节点（枝叶和主干交换机）和所有控制器(APIC)。涵盖所有交换矩阵、访问和租户层次结构。位于Fabric > Fabric Policies > Policies >

Monitoring > Common Policy。

- 交换矩阵监控策略monInfraPol(uni/infra/moninfra-default,) — 交换矩阵范围。为交换矩阵级对象生成系统日志：交换矩阵端口、卡、机箱组件和风扇托架。位于Fabric > Fabric Policies > Policies > Monitoring > Default。
- 访问监控策略monFabricPol(uni/fabric/monfab-default,) — 访问（基础设施）范围。为面向访问的组件生成系统日志：接入端口、交换矩阵扩展器(FEX)设备和虚拟机(VM)控制器事件。位于Fabric > Access Policies > Policies > Monitoring Policies > default。
- 租户监控策略monEPGPol(uni/tn-common/monepg-default,) — 租户范围。为租户范围对象生成系统日志：终端组(EPG)、应用配置文件和服务。在[Tenant] > Monitoring Policies > default的每个租户下找到。

注意：通用监控策略是系统日志配置的建议起点，因为它提供跨所有层次结构的交换矩阵范围覆盖，并自动部署到所有节点。除了通用策略外，还可以配置交换矩阵和访问监控策略，以便对特定对象层次结构进行更精细的控制，也可以使用通用策略来将系统日志限制在更窄的范围。

系统日志消息格式

当组格式设置为aci（默认值）时，ACI系统日志消息遵循RFC 3164格式：

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

例如：

```
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
```

消息正文包括受影响对象的ACI故障代码、生命周期状态(例如，soaking, retaining, cleared)、严重性和可分辨名称(DN)，使消息具有自我描述性。

有三种消息格式选项可供选择：

- aci（默认） — 符合RFC 3164的格式。建议用于大多数部署。
- nxos - NX-OS样式格式。如果系统日志平台需要NX-OS格式的消息，请使用此命令。
- 增强型日志(APIC 5.2(8)及更高版本) — 符合RFC 5424的格式，具有包括年份的增强型时间戳。

严重性映射

系统日志严重性字段是一个从0（最严重）到7（最不严重）的单个数字。 下表显示了系统日志严重性级别与ACI/国际电信联盟(ITU)严重性术语之间的映射：

系统日志严重性	ACI/ITU级别	描述
0 — 紧急	—	系统不可用
1 — 警报	关键	需要立即采取措施
2 — 关键	重大	严重情况
3 — 错误	Minor（轻微）	错误条件
4 — 警告	警告	警告条件
5 — 通知	不确定/已清除	正常但重要的情况
6 — 信息性	—	仅信息性消息
7 — 调试	—	仅调试输出

传输选项

ACI支持三种远程系统日志传输协议：

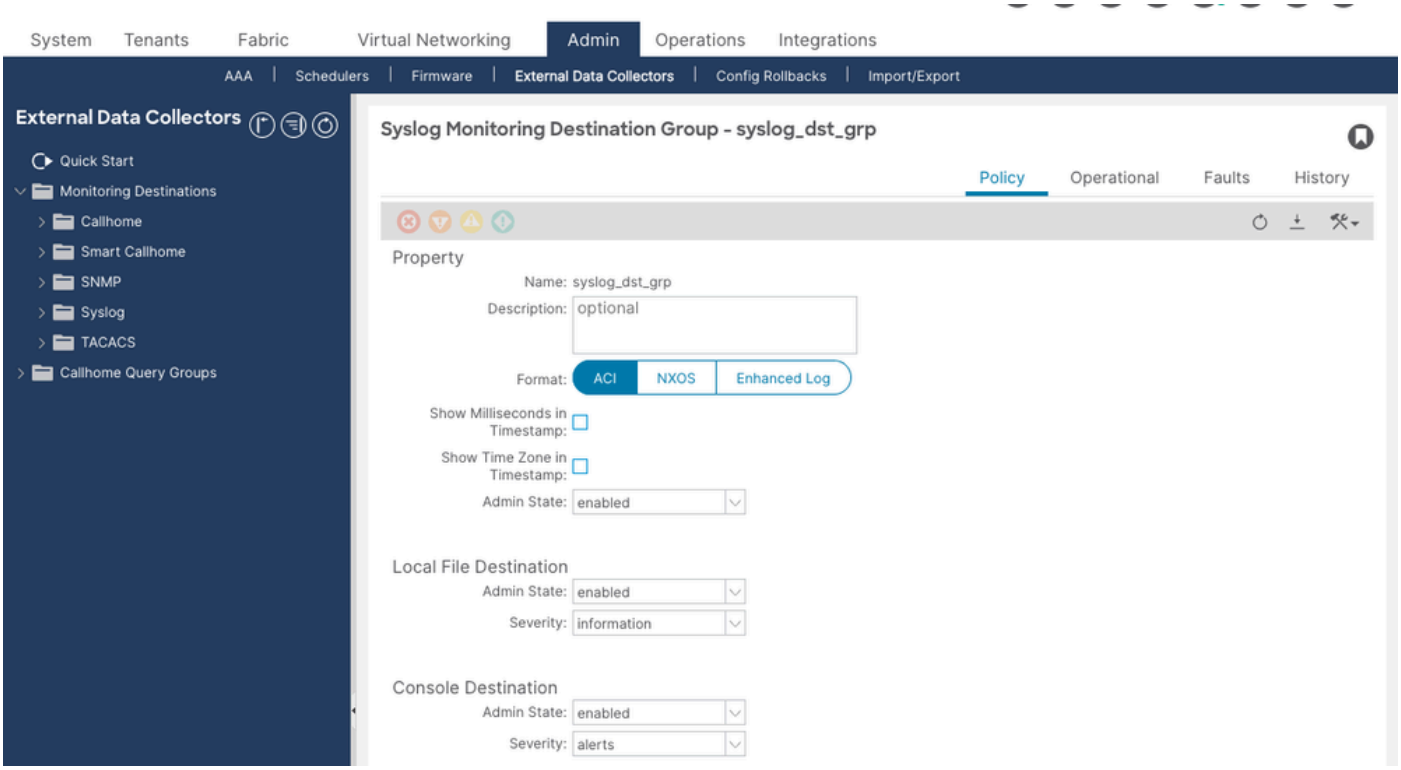
- UDP(默认) — 适用于所有APIC版本。标准的即刻即逝的传送。
- TCP — 从APIC版本5.2(3)及更高版本提供。通过面向连接的传输提供可靠传输。
- SSL — 从APIC版本5.2(4)及更高版本可用。使用TLS提供加密传输。每个ACI节点（APIC或交换机）充当TLS客户端，并发起到系统日志服务器的出站连接。服务器证书必须上传到APIC，其地址为Admin > AAA > Security > Public Key Management > Certificate Authorities。

注意：如果远程目标配置了SSL传输，并且APIC降级为不支持SSL的版本，则传输协议会自动恢复为UDP。确保系统日志服务器也可以接受UDP连接作为回退。

配置

以下步骤从端到端配置ACI系统日志。完成所有步骤，以便从APIC控制器和枝叶和主干交换机启用系统日志转发。

步骤 1：创建系统日志目标组



目标组定义系统日志消息的发送位置以及发送格式。首先创建此组，因为在后续步骤中配置的系统日志源按名称引用此组。

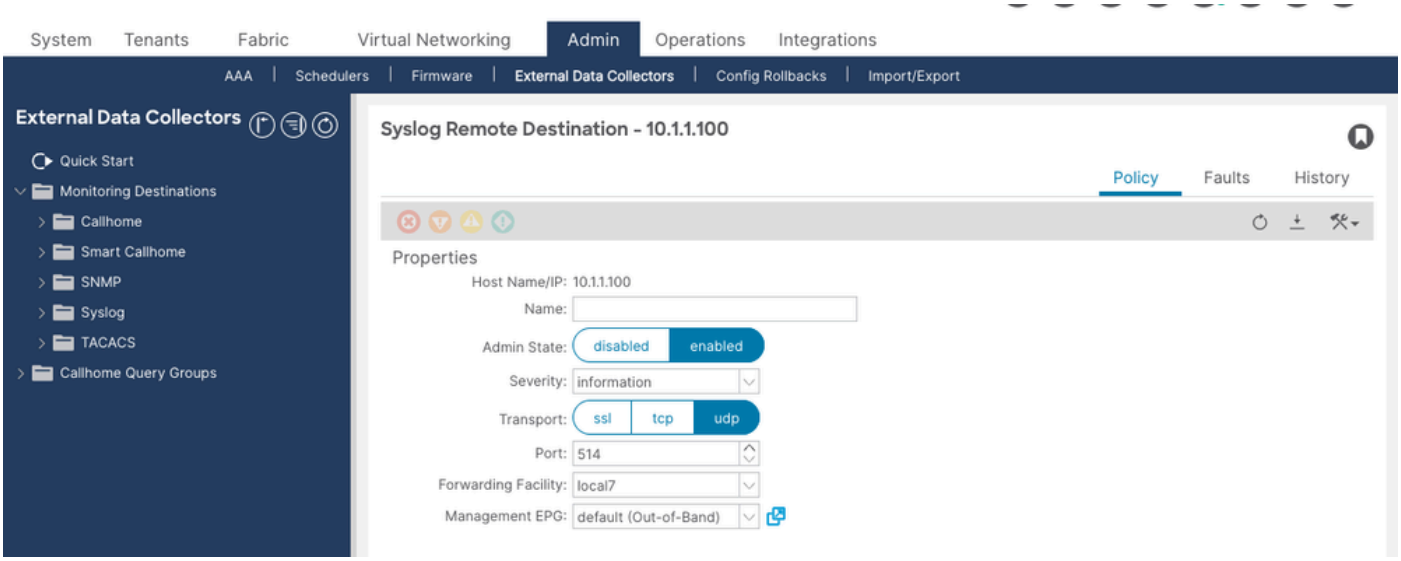
导航到Admin > External Data Collectors > Monitoring Destinations > Syslog。右键单击Syslog并选择Create Syslog Monitoring Destination Group。

在向导的第一页（组配置文件）上配置以下内容：

- Name — 描述性名称，Syslog-Dest-Group如。
- 格式(aci默认，兼容RFC 3164)或nxos。
- 管理状态 — enabled。
- 本地文件目标管理状态enabled —（推荐）。 这会将消息写入到每/var/log/external/messages个交换矩阵节点上，并且对于本地故障排除至关重要，即使远程服务器无法访问。
- 本地文件目标严重性information—。
- 控制台目标管理状态disabled —（建议用于生产环境）。

单击 Next。在第二页上，单击创建远程目标区域中的+以添加远程系统日志服务器。

步骤 2：添加远程目标



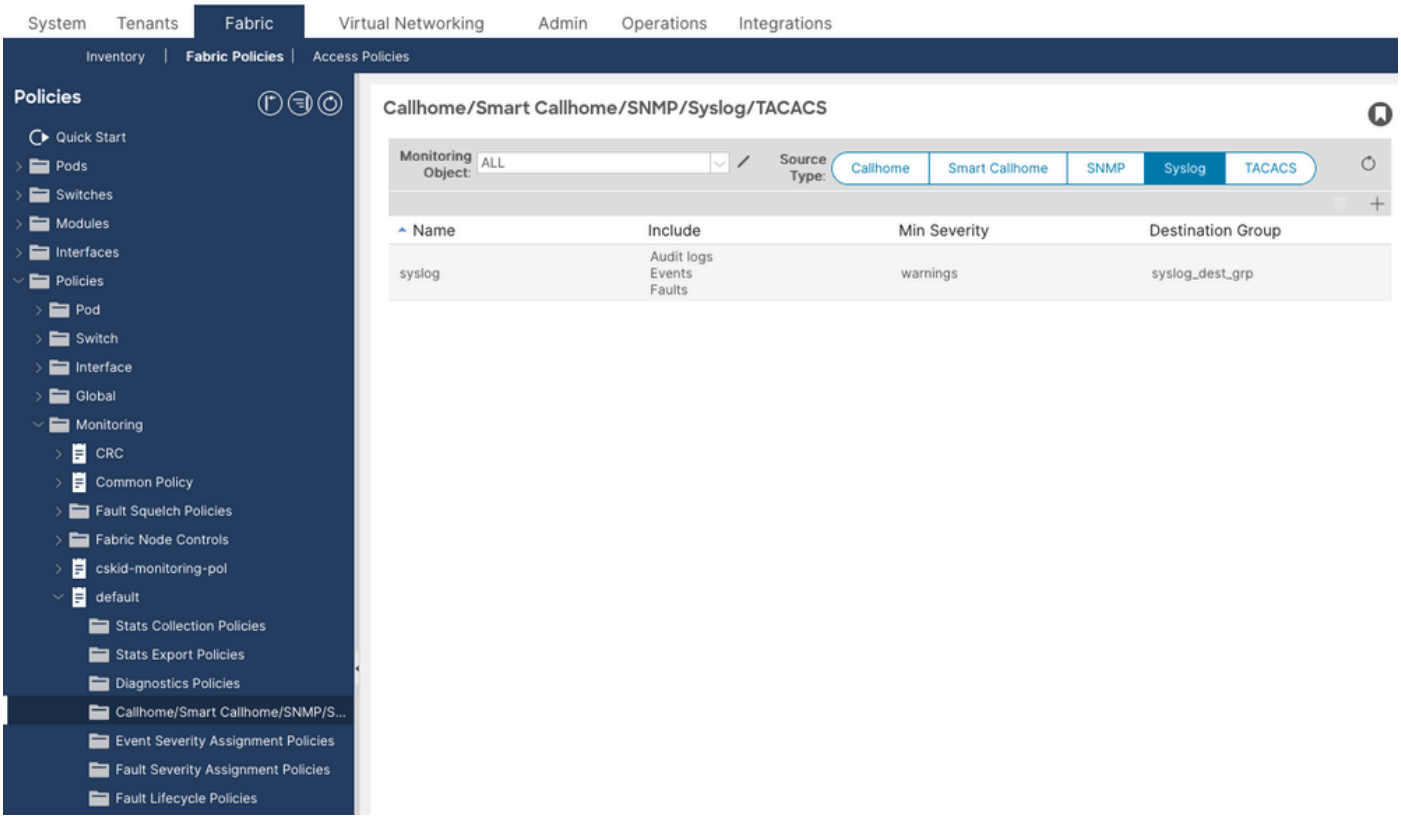
在Create Syslog Remote Destination对话框中配置远程系统日志服务器：

- 主机 — 系统日志服务器的IP地址。使用IP地址而非主机名。如果使用主机名，必须确保通过带外(OOB)管理接口可以访问域名系统(DNS)服务器。当网络中断期间生成系统日志消息时，只能通过带内连接访问的DNS服务器可能无法解析。
- 管理状态 — enabled。
- 严重性—information（推荐）。 这是发送到此特定远程服务器的最低严重性。
- 端口(514默认)。
- 设施—local7（默认）。 将此设置为与配置为accept和route的syslog服务器的设施值匹配。
- 传输(udp默认)。 用于tcp可靠传输(需要APIC 5.2(3)或更高版本)或加密传输(需要APIC 5.2(4)或更高版本以及上传到APIC的证书ssl)。
- 管理EPG — 选择可访问系统日志服务器的管理EPG。对于OOB管理：uni/tn-mgmt/mgmtp-default/oob-default.对于带内管理，请选择适当的带内EPG。此字段不能为空。

单击OK，然后单击Finish。

注意：您可以将多个远程目标添加到同一个目标组。每个目标可以有不同的严重性阈值、设施和传输协议。

步骤 3：在交换矩阵监控策略下创建系统日志源



此步骤为交换矩阵对象层次结构（交换矩阵端口、卡、机箱组件和风扇托架）配置系统日志。这通过特定于层次的控制对通用监控策略（第4步）进行补充。

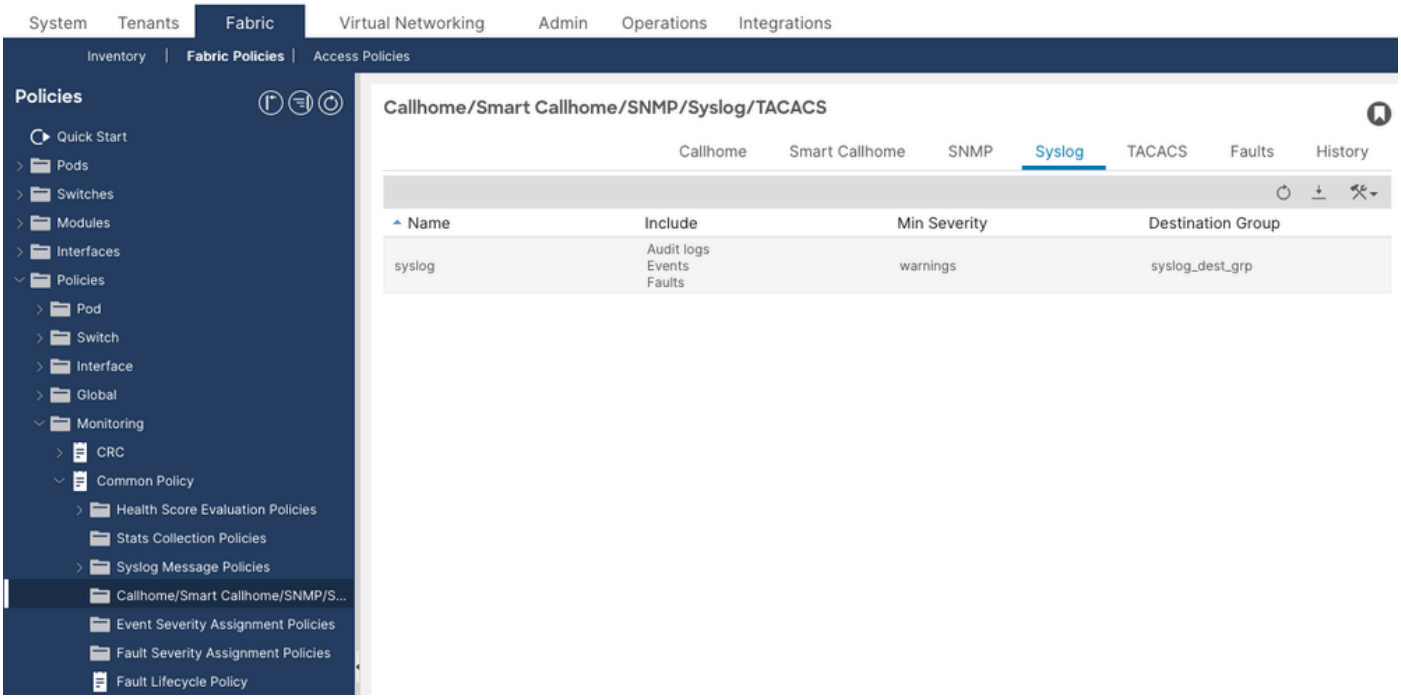
导航到Fabric > Fabric Policies > Policies > Monitoring > default > Callhome/Smart Callhome/SNMP/Syslog/TACACS。

在右侧窗格中，将Source Type设置为Syslog。单击+以创建系统日志源：

- Name — 描述性名称，Syslog-Source-Fabric如。
- 最小严重性—information（建议用于完全覆盖）。
- Include — 检查、事件和故障。或者，为登录和注销事件添加session。
- 目标组 — 选择在步骤1中创建的目标组。

单击 submit。

步骤 4：配置通用监控策略（系统级系统日志）

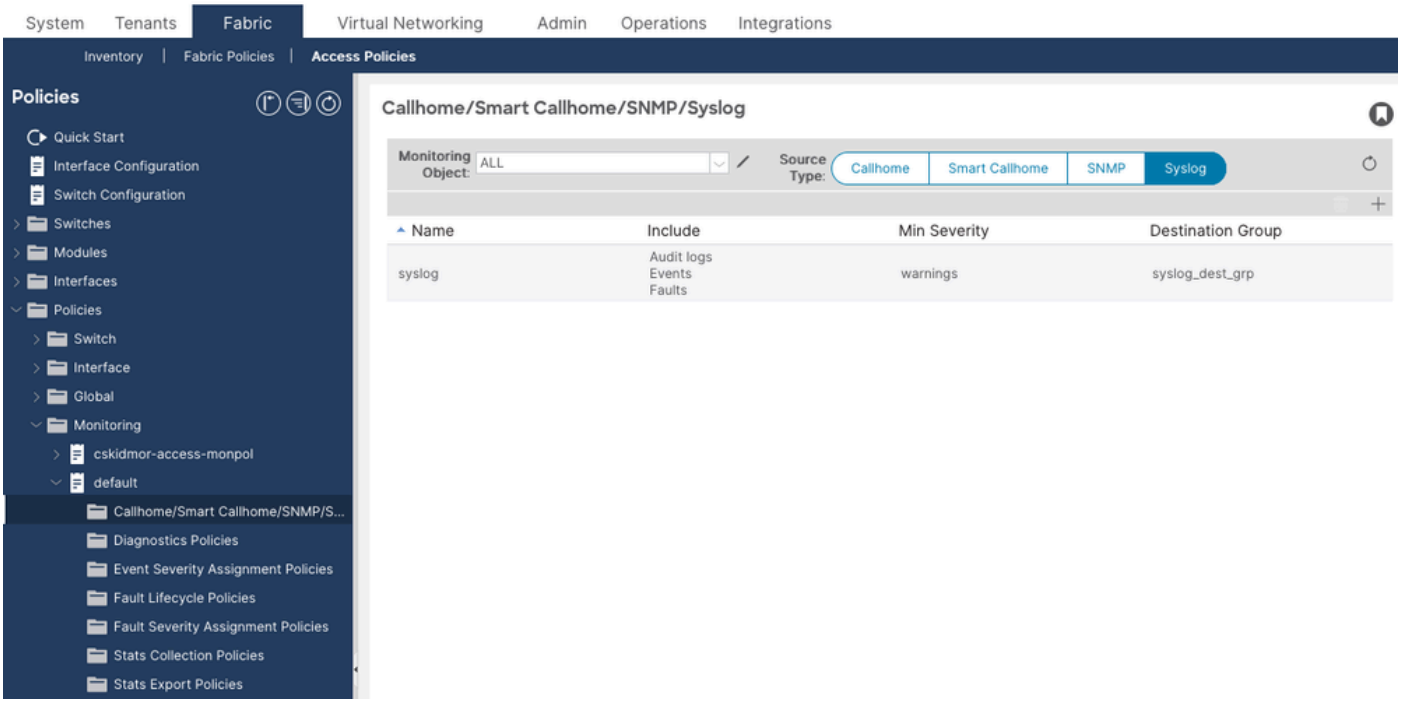


通用监控策略提供系统范围的系统日志覆盖，系统范围自动部署到交换矩阵中的所有节点和控制器。此步骤将系统系统日志源链接到目标组。

导航到交换矩阵>交换矩阵策略>策略>监控>通用策略。在Syslog部分下，将系统syslog源链接到第1步中创建的目标组。

公共策略系统syslog源使用DN处syslogRsSystemDestGroup的MOuni/fabric/moncommon/systemslsrc/rssystemDestGroup。

步骤 5：在访问监控策略下创建系统日志源



此步骤为访问对象层次结构(访问端口、交换矩阵扩展器(FEX)设备和虚拟机(VM)控制器事件)配置系统日志。这通过特定于层次的控制对通用监控策略（第4步）进行补充。

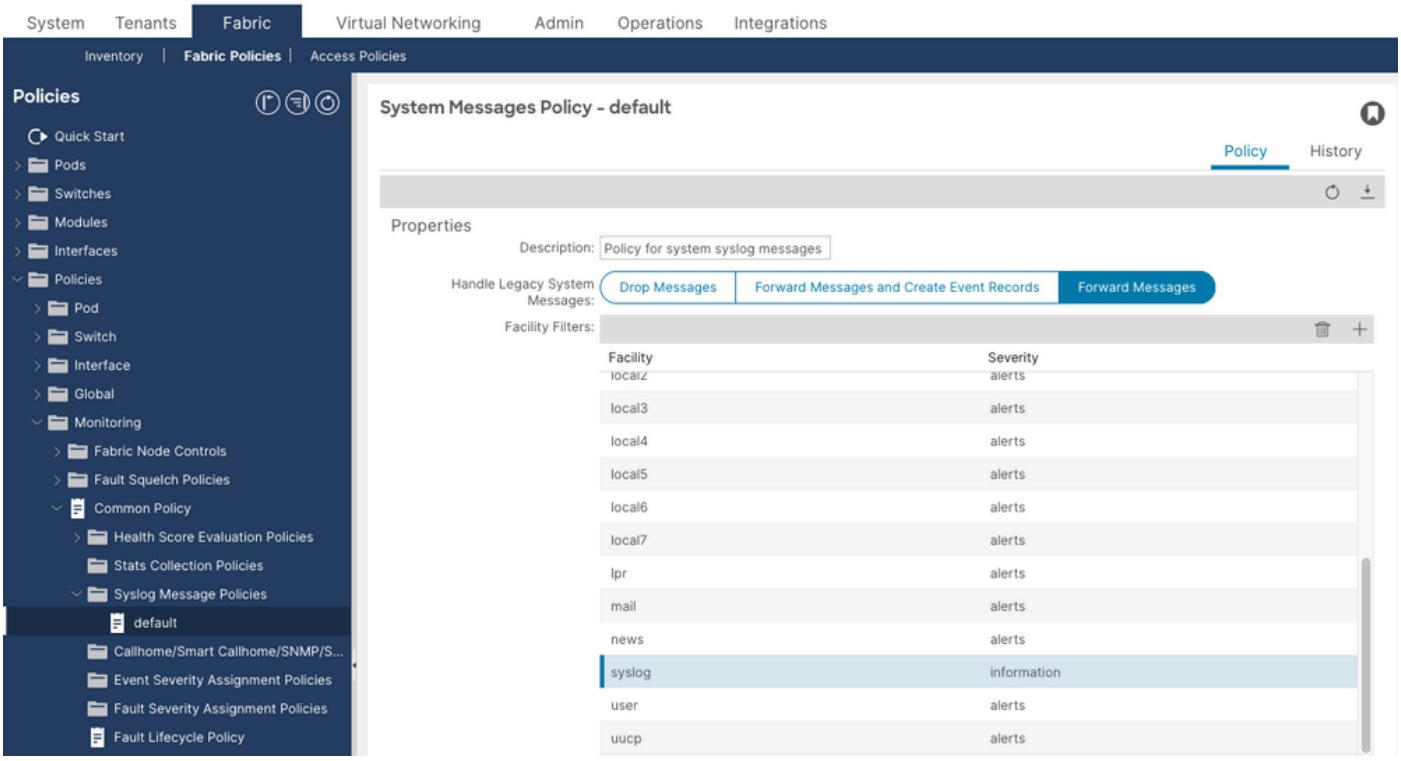
导航到Fabric > Access Policies > Policies > Monitoring Policies > default > Callhome/SNMP/Syslog。

将Source Type设置为Syslog。单击+，配置与步骤3相同的设置：

- 名称 — 例如Syslog-Source-Access。
- 最小严重性(Min Severity)—information。
- Include — 检查、事件和故障。
- 目标组 — 选择相同的目标组。

单击 submit。

第6步（可选）：调整合同ACL日志记录的系统日志消息策略



如果需要在远程系统日志服务器中显示合同ACL permit或deny数据包日志(ACLLOG_PKTLOG_PERMIT / ACLLOG_PKTLOG_DENY)，则必须将系统日志消息设备过滤器设置为信息性严重性。

导航到Fabric > Fabric Policies > Policies > Monitoring > Common Policy > Syslog Message Policies > default。在Facility filter列表中，选择syslog facility并将Min Severity设置为information。这是DNsyslogFacilityFilter的MOuni/fabric/moncommon/sysmsgp/ff-syslog。

注意：要使合同ACL允许和拒绝日志到达远程系统日志服务器，必须满足以下四个条件：(1)syslog source minSev必须是information,(2)remote destination severity必须是information,(3)Syslog Message Policy syslog facility filter minSev必须为information,(4)必须在合同过滤器条目上启用Log指令。当满足所有三个条件时，ACL日志消息来自枝叶交换机（而不是来自APIC），因此它们首先出现在枝叶交换机的/var/log/external/messages中。合同ACL数据包日志速率受CoPP限制：deny logs默认为500 packets per second(pps),permit logs默认为300 pps per leaf。

注意：不支持在管理合同中对过滤器使用Log指令，这会导致分区规则部署失败。仅将合同日志记录应用于租户数据平面合同。

检查配置

在排除任何运行问题之前检验配置。缺少系统日志消息的最常见根本原因是配置错误，而不是网络或软件故障。

验证目标组和配置文件

在APIC**moquery -c syslogGroup**上运行以确认目标组存在并检查其属性：

<#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
```

然后使用以下信息验证配置文件(组级别管理状态**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
```

要查找配置文件已禁用的任何目标组，请运行：

<#root>

```
apic1#

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

此处的结果意味着无论远程目标管理状态如何，目标组都不会转发任何系统日志流量。

检验远程目标

运行**moquery -c syslogRemoteDest**以验证每个远程服务器配置：

<#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
```

需要特别注意以下三个属性：

- 管理状态：一定是enabled的。如果禁用，此特定远程服务器不会收到任何内容。
- epgDn:不能为空。空表示交epgDn换矩阵不知道发送系统日志流量的接口，因此没有消息离开交换矩阵。
- operState:未知:此值是预期值，并不表示有问题。ACI不会主动探测系统日志服务器的可达性。

验证系统日志源

运行**moquery -c syslogSrc**以确认源存在于正确的监控策略下：

<#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
```

确认源位于相应的监控策略下：

- 下面的“uni/fabric/moncommonCommon Monitoring Policy”源，用于覆盖整个交换矩阵的所有节点和所有对象层次结构。
- 下的源 — uni/infra/moninfra-default交换矩阵监控策略，用于交换矩阵级对象（交换矩阵端口、卡、机箱）。
- 以下的uni/fabric/monfab-default源 — 访问监控策略，用于访问级别对象（访问端口、FEX、VM控制器）。

另请验证Common Monitoring Policy system syslog源已链接：

<#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
```

如果需要合同ACL日志记录，请使用以下内容验证系统日志消息策略设备过滤器严**moquery -d uni/fabric/moncommon/sysmsgp/ff-syslog**重性：

<#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
```

验证本地日志文件

上的本地文件/var/log/external/messages是确认系统日志消息正在任何交换矩阵节点上生成的最直接方式，即使无法访问远程服务器也是如此。在APIC和枝叶交换机上检查它：

```
<#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
```

如果此文件为空或未在节点上更新，则不会在源位置生成消息。如果文件包含内容，但远程系统日志服务器没有接收消息，则问题在于转发（目标组、网络或防火墙），而不是消息生成。

验证与Syslog服务器的可达性

从APIC ping syslog服务器，以验证通过管理网络的IP可达性：

```
<#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
```

在枝叶或主干交换机上，使用带-V标志的iping指定VRF。根据为系统日志目标分配的管理EPG，将

management用于带外或将mgmt:inb用于带内：

```
<#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操作可确认IP可达性，但不确认是否允许UDP或TCP端口514。Internet控制消息协议(ICMP)和系统日志使用不同的协议。

故障排除

分类工作流

当系统日志消息未到达远程服务器时，请使用以下诊断树：

```
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
```

常见情况

情形 1：远程服务器未收到系统日志消息

问题：系统日志目标组和远程目标已配置，但没有消息到达远程服务器。APIC和交换机 /var/log/external/messages上的本地文件包含最近的条目。

配置检查：

<#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：远程目标管理状态为disabledID。如果目标已创建但无意中保持禁用状态，或者在维护期间禁用了目标并且从未重新启用，则可能会出现这种情况。

解决方案：导航到Admin > External Data Collectors > Monitoring Destinations > Syslog > [group name] > Remote Destinations > [server]。编辑远程目标并将Admin State设置为enabled。

方案 2：系统日志目标组配置文件已禁用

问题：即使启用了远程目标管理状态，也不会从任何节点转发消息。

配置检查：

<#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状态控制整个目标组。当它被禁用时，无论单个远程目标状态如何，都不会从任何节点转发消息。

解决方案：导航到Admin > External Data Collectors > Monitoring Destinations > Syslog > [group name]。编辑配置文件并将Admin State设置为enabled。

情形 3：缺少事件 — 公用监视策略未链接

问题：来自某些节点或对象层次的系统日志消息无法到达远程服务器，即使在交换矩阵或访问监控策略下配置了系统日志源。

配置检查：

<#root>

```
apic1#
```

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

```
Total Objects shown: 0
```

通用监控策略系统系统日志源未链接到目标组。

根本原因：通用监控策略(uni/fabric/moncommon)提供跨所有层次结构的交换矩阵范围系统日志覆盖，并自动部署到所有节点和控制器。如果没有它，则仅转发与特定交换矩阵或访问监控策略层次结构匹配的事件。交换矩阵监控策略(uni/infra/moninfra-default)涵盖交换矩阵级对象，访问监控策略(uni/fabric/monfab-default)涵盖访问级对象，但两者都不提供通用策略提供的交换矩阵范围覆盖。

解决方案：导航到交换矩阵>交换矩阵策略>策略>监控>通用策略。在Syslog部分下，将系统syslog源链接到目标组。使用验**moquery -d uni/fabric/moncommon/systemslsrc/rssystemDestGroup**证是否tDn指向您的目标组。

场景 4：严重性限制过多 — 缺少预期消息

问题：有些消息到达系统日志服务器，但缺少信息性事件、审核日志条目或会话登录事件。仅发现严重故障和重大故障。

配置检查：

<#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：系统日志过滤发生在两点：源(minSev)和远程目标(severity)。 仅转发通过两个过滤器的邮件。如果以上任一选项设置information为，信息性消息将被丢弃。

解决方案：编辑syslog源并将Min Severity设置为信息，并在Include字段中选中audit、events和faults。编辑远程目标并将Severity设置为information。

场景 5：未向远程目标分配管理EPG

问题：远程服务器未收到任何系统日志消息。目标组已启用，远程目标已启用，并且本地日志文件包含内容。

配置检查：

<#root>

```
apic1#

moquery -c syslogRemoteDest

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

根本原因：如果没有管理EPG，APIC和交换机不知道使用哪个物理接口来发送系统日志消息。消息已生成，但无法转发。

解决方案：编辑远程目标，选择适当的管理EPG。对于OOB管理，请选择uni/tn-mgmt/mgmtp-default/oob-default。对于带内管理，请选择适当的带内EPG。

场景 6：错误的管理EPG（带内与带外）

问题：系统日志消息间歇性到达或仅从某些节点到达。系统日志服务器只能通过OOB管理访问，但远程目标引用带内EPG。

配置检查：

<#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
```

如果只能通过OOB网络访问系统日志服务器，则带内EPG会导致消息从带内接口发出，而无法访问服务器。

解决方案：编辑远程目标并将Management EPG更改为uni/tn-mgmt/mgmtp-default/oob-default。从APIC bash**ping -c 3 10.1.1.100**验证以确认OOB可达性。

场景 7：防火墙阻止系统日志流量

问题：本地日志文件在APIC和枝叶节点上都有内容，配置正确，对syslog服务器的ICMP ping成功，但没有消息到达服务器。

运行检查：从APIC ping syslog服务器以验证IP可达性：

<#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，但系统日志消息未到达。ICMP(ping)通过，而UDP端口514被阻止。

根本原因：管理网络和syslog服务器之间的防火墙或ACL阻止UDP端口514（如果配置了TCP传输，则阻止TCP 514）。ICMP和UDP是独立的 — ICMP传递不确认是否允许UDP 514。此外，每个枝叶和主干直接从自己的OOB IP地址发送系统日志。仅允许APIC OOB IP的防火墙会丢弃来自交换机节点的系统日志数据包。

解决方案：验证防火墙是否允许来自所有交换矩阵节点的OOB IP地址范围的UDP/TCP端口514(包括所有APIC、所有枝叶交换机和所有主干交换机)。系统日志服务器上的数据包捕获确认UDP 514数据包是否到达。

场景 8：合同ACL允许/拒绝日志未到达

问题：合同permit或deny数据包日志ACLLOG_PKTLOG_PERMIT(/ACLLOG_PKTLOG_DENY)未到达syslog服务器。

配置检查：

1. 验证系统日志源严重性是information否：
   <#root>

   apic1#

   moquery -c syslogSrc

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

2. 验证远程目标严重性是information否：
   <#root>

   apic1#

   moquery -c syslogRemoteDest

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

3. 验证Syslog消息策略设备过滤器严重性是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. 验证已在合同过滤器上启用log指令。导航到租户> [租户] >合同> [合同] >主题> [主题] >过滤器，确认指令列显示相关过滤器条目的日志。
5. 验证是否在枝叶交换机上生成ACL日志（ACL日志源自枝叶，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
```

如果未显ACLLOG示任何条目，则log指令不会触发枝叶上的日志生成。这可能表示合同指令配置错误、没有匹配流量进入合同，或者CoPP速率限制在记录数据包之前丢弃数据包。

根本原因：合同ACL日志严重级别为(informational系统日志级别6)。 如果上面设置了系统日志链中的任何过滤器(源minSev severity、远程目标或系统日志消息策略工具过滤器(syslogFacilityFilter at uni/fabric/moncommon/sysmsgp/ff-syslog))，则ACL日志消息会在离开交换矩阵节点之前静默丢弃information。

解决方案：在minSevsyslog源上设置为information，在远程目标上设置为severityinformationsyslog minSev，在Common Policy > Syslog Message Policies > default下将设备过滤器设置为information，确认已在合同过滤器上启用Log指令，并验证防火墙是否允许来自枝叶交换机OOB IP地址(而不仅仅是APIC IP)的系统日志流量，因为ACL日志是从交换机发送的。

场景 9：重命名目标组后，系统日志停止

问题：更改系统日志目标组的名称后，系统日志消息停止到达远程服务器。更改端口或设施不会导致此问题。禁用和重新启用策略不会恢复消息传送。

根本原因：这是已知的软件缺陷。请参阅Cisco Bug ID CSCwj23752。重命名目标组会中断内部系统日志转发关联。在APIC版本6.0(6)及更高版本中修复了该问题。

解决方案：升级到APIC版本6.0(6c)或更高版本。作为受影响版本的一种解决方法，请删除重命名的目标组并使用所需的名称重新创建它，然后重新关联系统日志源。

场景 10：过多系统日志导致APIC GUI缓慢

问题：APIC GUI变慢，并且APIC CPU利用率高。如果在正常操作期间启用合同ACL日志记录，生成大量信息性系统日志消息，并将其转换为APIC数据库中的对象，则会发生这种情况eventRecord。

根本原因：当Common Policy Syslog Message Policy severity设置为information时，每个信息性系统日志消息（包括大量ACL日志）都会在APICeventRecord中生成。这会淹没APIC数据库并导致GUI缓慢。

解决方案：

- 在正常操作期间禁用合同ACL日志记录。仅在故障排除或维护时段启用它。
- 如果ACL日志记录必须保持启用状态，请在Fabric > Fabric Policies > Policies > Monitoring > Common Policy > Syslog Message Policies > default将系统日志消息策略严重性设置为alerts。

这可以防止信息性系统日志消息转换为事件，同时仍允许它们转发到远程系统日志服务器。
- 压制操作上无用的噪声事件代码。可以取消事件代码，以防止它生成事件记录而不影响系统日志转发。

已知的 Bug

以下已知软件缺陷影响ACI系统日志功能：

- Cisco bug ID CSCwj23752 — 重命名系统日志目标组会停止系统日志传送。已在APIC版本6.0(6c)及更高版本中修复。

升级条件

在以下情况下，收集技术支持并联系思科TAC:

- /var/log/external/messages系统日志消息在本地交换矩阵节点上显示，目标组和远程目标管理状态都为enabled，管理EPG正确，网络可达性得到确认（ping和防火墙检查通过），但消息仍然没有到达远程服务器。
- 系统日志消息来自一些交换矩阵节点，但来自其他交换矩阵节点，两者之间的配置没有差异，这表明策略部署不一致。
- 目标组配置文件或远程目标已重新启用，但消息不会在配置更改后的几分钟内恢复。
- APIC升级后，系统日志消息停止到达，表明可能存在软件缺陷。

打开TAC案例之前要收集的数据：

- 来自受影响的APIC和一个受影响枝叶节点的按需技术支持。
- APICmoquery -c syslogGroup、 moquery -c syslogProf和moquery -c syslogRemoteDest的moquery -c syslogSrc输出。
- 的输出moquery -d uni/fabric/moncommon/systemslsrc/rssystemDestGroup，用于验证通用策略链路。
- 来自/var/log/external/messagesAPIC和受影响枝叶的尾部。
- 从系统日志服务器捕获数据包，确认UDP/TCP 514数据包是否来自交换矩阵OOB地址。

参考

- 思科APIC基本配置指南，版本6.1(x) — 管理
- 思科ACI系统消息参考指南
- 思科ACI故障、事件和系统消息管理指南
- 思科ACI合同指南白皮书
- 排除速度缓慢的APIC GUI故障

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。