Configuración y solución de problemas de Syslog en ACI

Introducción

Este documento describe cómo configurar, verificar y solucionar problemas de registro del sistema (syslog) en Cisco Application Centric Infrastructure (ACI). Abarca todo el flujo de trabajo de configuración, la verificación programática mediante el modelo de objetos administrados (MO) del Application Policy Infrastructure Controller (APIC) y un flujo de trabajo estructurado de solución de problemas tanto para los controladores APIC como para los switches de columna y hoja.

Overview

El syslog de ACI está totalmente basado en políticas. A diferencia del software Cisco NX-OS® independiente, no hay comandos de **logging server** CLI en los switches de columna u hoja de ACI. Toda la configuración de syslog se realiza mediante políticas APIC que el APIC envía a cada nodo de fabric automáticamente.

Componentes clave

El subsistema syslog de ACI se crea a partir de los siguientes objetos administrados:

- Syslog Destination Group (syslogGroup): contenedor de nivel superior para todos los destinos de syslog. Controla el formato del mensaje (estilo ACI o NX-OS) y las opciones de marca de hora. Puede contener uno o más destinos remotos, un destino de archivo local y un destino de consola.
- Perfil de Syslog (syslogProf): Elemento secundario del grupo de destino que controla el estado administrativo de nivel de grupo y el protocolo de transporte (UDP, TCP o SSL).
- Syslog Remote Destination (syslogRemoteDest): un hijo del grupo de destino que representa un servidor syslog remoto. Controla la IP o el nombre de host del servidor, el puerto, el filtro de gravedad, la función syslog y el grupo de terminales de administración (EPG) que se utiliza para alcanzar el servidor.
- Archivo local de registro del sistema (syslogFile): un elemento secundario del grupo de destino que controla la escritura de mensajes de registro del sistema en el archivo local /var/log/external/messages en cada nodo de fabric.
- Origen de Syslog (syslogSrc): adjunto a una política de supervisión. Controla los tipos de mensajes (auditoría, eventos, fallos, sesión) y la gravedad mínima que se envían, así como

los enlaces al grupo de destino a través de una syslogRsDestGroup relación.

Puntos de archivo adjunto de origen Syslog

ACI utiliza cuatro ámbitos de políticas de supervisión que controlan qué nodos y objetos generan mensajes de syslog:

- Política de supervisión común (monCommonPol, uni/fabric/moncommon): ámbito de todo el fabric. Una política de supervisión básica que se aplica a todos los fallos y eventos y que se implementa automáticamente en todos los nodos (switches de hoja y columna) y en todos los controladores (APIC) del fabric. Cubre todas las jerarquías de fabric, acceso y arrendatarios. Encontrado en Fabric > Fabric Policies > Policies > Monitoring > Common Policy.
- Política de supervisión de fabric (monInfraPol, uni/infra/moninfra-default): ámbito de fabric. Genera syslog para objetos de nivel de fabric: puertos de fabric, tarjetas, componentes de chasis y bandejas de ventilador. Se encuentra en Fabric > Fabric Policies > Policies > Monitoring > default.
- Directiva de supervisión de acceso (monFabricPol, uni/fabric/monfab-default): ámbito de acceso (infraestructura). Genera syslog para componentes de acceso: puertos de acceso, dispositivos Fabric Extender (FEX) y eventos de controlador de máquinas virtuales (VM). Se encuentra en Fabric > Access Policies > Policies > Monitoring Policies > default.
- Directiva de supervisión de arrendatarios (monEPGPol, uni/tn-common/monepg-default): ámbito del arrendatario. Genera syslog para objetos de ámbito de arrendatario: grupos de terminales (EPG), perfiles de aplicación y servicios. Se encuentra debajo de cada arrendatario en [Arrendatario] > Supervisión de políticas > predeterminado.

Nota: La política de supervisión común es el punto de partida recomendado para la configuración de syslog, ya que proporciona cobertura en todo el fabric en todas las jerarquías y se implementa automáticamente en todos los nodos. Las políticas de supervisión de acceso y fabric se pueden configurar además de la política común para un control más granular sobre jerarquías de objetos específicos, o en lugar de la política común para restringir syslog a un ámbito más estrecho.

Formato de mensaje de Syslog

Los mensajes de syslog de ACI siguen el formato RFC 3164 cuando el formato de grupo se establece en aci (el valor predeterminado):

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

Por ejemplo:

```
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
```

El cuerpo del mensaje incluye el código de error de ACI, el estado del ciclo de vida (por ejemplo, soaking, retaining, cleared), la gravedad y el nombre distinguido (DN) del objeto afectado, lo que hace que los mensajes se describan a sí mismos.

Hay disponibles tres opciones de formato de mensaje:

- aci (predeterminado): formato compatible con RFC 3164. Recomendado para la mayoría de implementaciones.
- nxos: formato de estilo NX-OS. Utilice esta opción si la plataforma syslog espera recibir mensajes con formato NX-OS.
- Registro mejorado (APIC 5.2(8) y versiones posteriores): formato compatible con RFC 5424 con marcas de tiempo mejoradas que incluyen el año.

Asignación de gravedad

El campo de gravedad de syslog es un solo dígito entre 0 (el más grave) y 7 (el menos grave). La siguiente tabla muestra la correspondencia entre los niveles de gravedad de syslog y la terminología de gravedad de ACI/Unión Internacional de Telecomunicaciones (ITU):

Gravedad de Syslog	Nivel ACI/ITU	Descripción
0 — emergencia	—	El sistema no se puede utilizar
1 — alerta	Crítico	Acción inmediata requerida
2 — crítico	Principal	Condición crítica
3 — error	Menor	Condición de error
4 — advertencia	Advertencia	Condición de advertencia
5 — notificación	Indeterminado/Borrado	Condición normal pero significativa
6 — informativo	—	Sólo mensaje informativo
7: debugging	—	Sólo salida de depuración

Opciones de transporte

ACI admite tres protocolos de transporte para syslog remoto:

- UDP (predeterminado): disponible en todas las versiones de APIC. Entrega estándar de

fuego y olvídate.

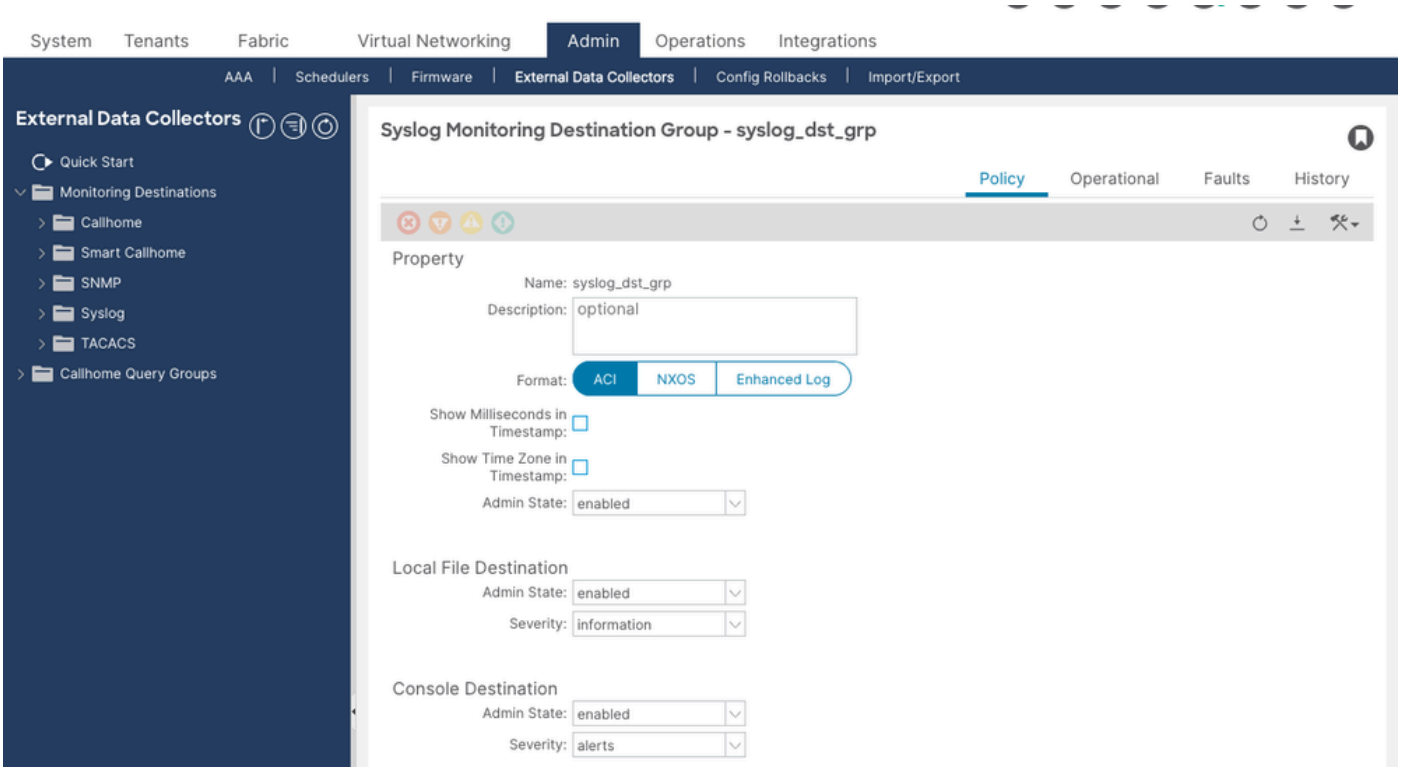
- TCP: disponible a partir de APIC versión 5.2(3) y posteriores. Proporciona una entrega fiable con transporte orientado a la conexión.
- SSL: disponible a partir de APIC versión 5.2(4) y posteriores. Proporciona transporte cifrado mediante TLS. Cada nodo ACI (APIC o switch) actúa como cliente TLS e inicia una conexión saliente con el servidor syslog. El certificado del servidor se debe cargar en el APIC en Admin > AAA > Security > Public Key Management > Certificate Authorities.

Nota: Si un destino remoto se configura con transporte SSL y el APIC se rebaja a una versión que no admite SSL, el protocolo de transporte revierte automáticamente a UDP. Asegúrese de que el servidor syslog también pueda aceptar conexiones UDP como reserva.

Configuración

Los siguientes pasos configuran el syslog de ACI de principio a fin. Complete todos los pasos para habilitar el reenvío de syslog desde los controladores APIC y los switches de hoja y columna.

Paso 1: Crear el grupo de destino de Syslog



El grupo de destino define dónde se envían los mensajes de syslog y en qué formato. Cree esto primero, porque los orígenes de syslog configurados en pasos posteriores hacen referencia a este grupo por su nombre.

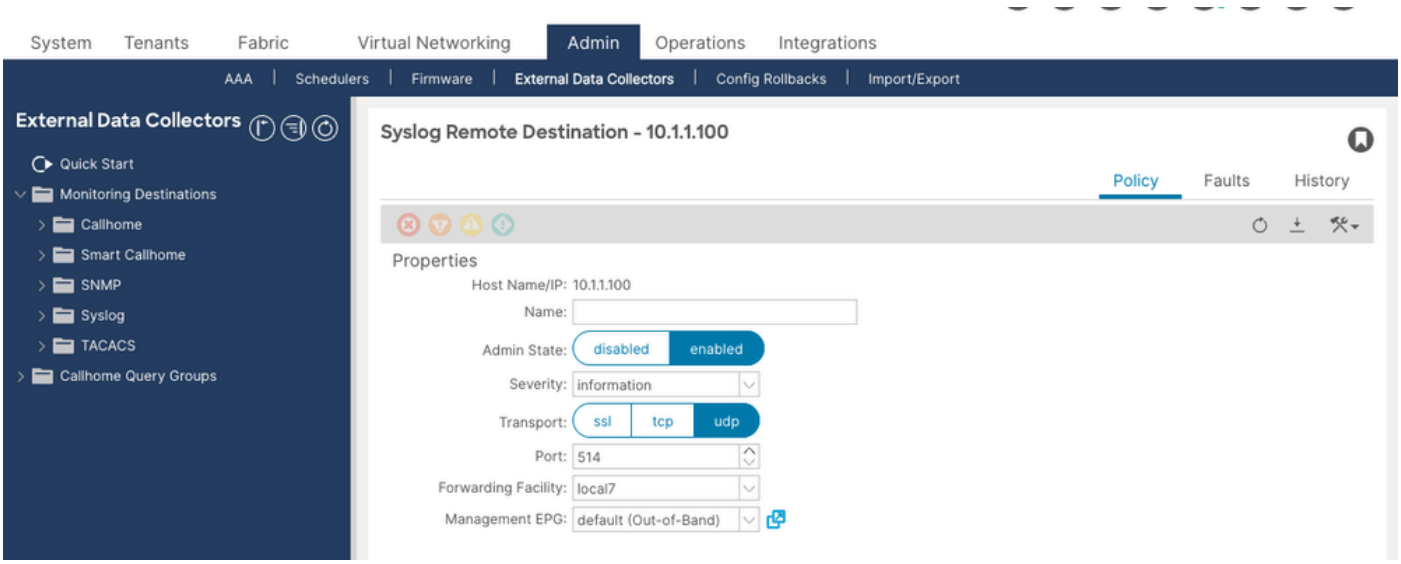
Vaya a Admin > External Data Collectors > Monitoring Destinations > Syslog. Haga clic con el botón derecho en Syslog y seleccione Crear grupo de destino de monitoreo de Syslog.

En el asistente, configure lo siguiente en la primera página (perfil de grupo):

- Nombre: un nombre descriptivo como Syslog-Dest-Group.
- Formato: aci (predeterminado, compatible con RFC 3164) o nxos.
- Estado de administración: enabled.
- Archivo local Estado de administración de destino: enabled (recomendado). Esto escribe mensajes en /var/log/external/messages en cada nodo de fabric y es esencial para la resolución de problemas local incluso cuando un servidor remoto es inalcanzable.
- Gravedad de destino del archivo local: information.
- Estado de administración de destino de la consola: disabled (recomendado para entornos de producción).

Haga clic en Next (Siguiente). En la segunda página, haga clic en + en el área Crear destinos remotos para agregar un servidor syslog remoto.

Paso 2: Agregar un destino remoto



Configure el servidor syslog remoto en el cuadro de diálogo Create Syslog Remote Destination:

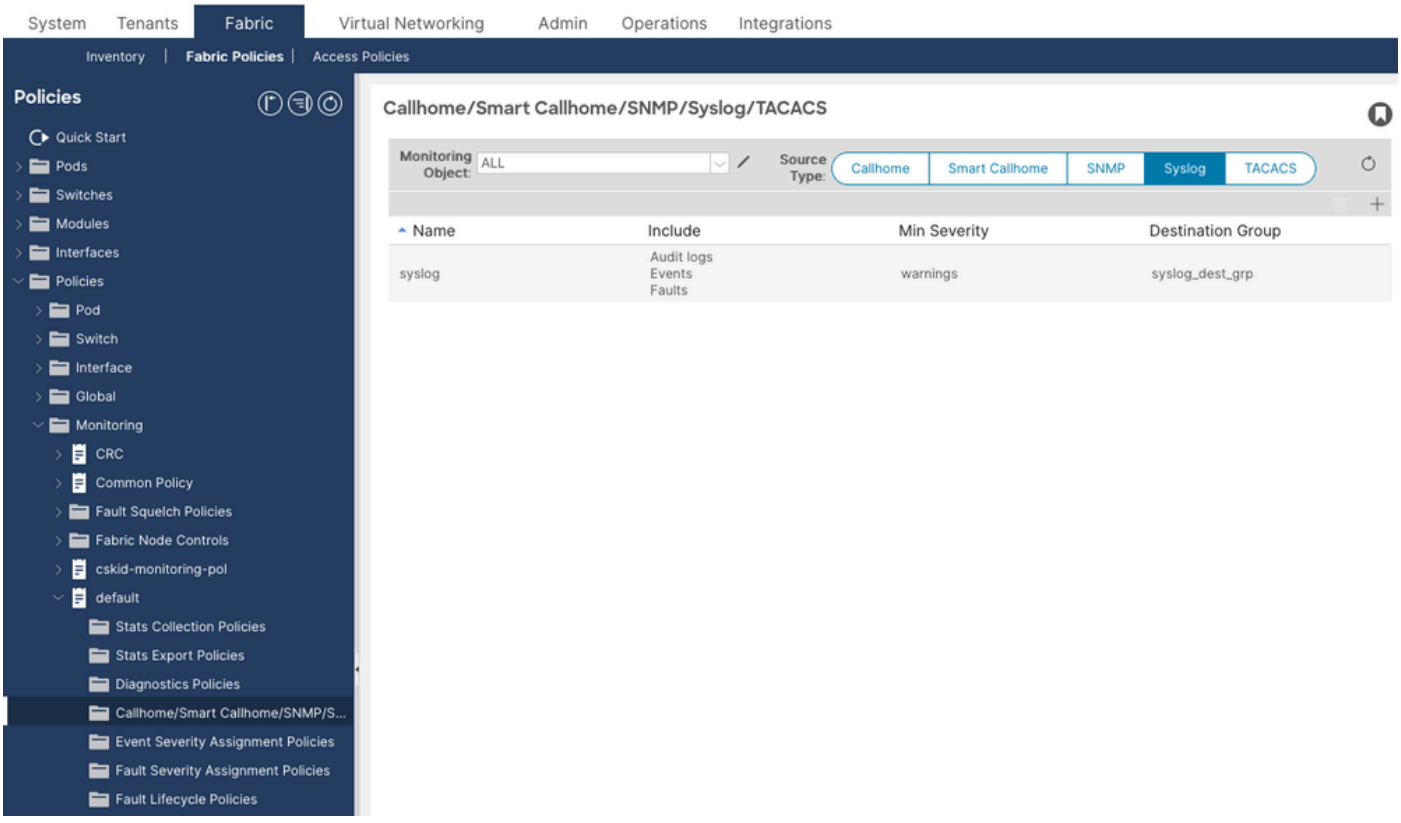
- Host: dirección IP del servidor syslog. Utilice una dirección IP en lugar de un nombre de host. Si utiliza un nombre de host, debe asegurarse de que el servidor del Sistema de nombres de dominio (DNS) es accesible a través de la interfaz de administración fuera de banda (OOB). Los servidores DNS accesibles sólo a través de conectividad en banda

pueden fallar al resolver cuando se generan mensajes de syslog durante una interrupción de la red.
- Estado de administración: enabled.
- Gravedad: information (recomendado). Esta es la gravedad mínima enviada a este servidor remoto específico.
- Puerto: 514 (predeterminado).
- Recurso: local7 (valor predeterminado). Configure esto para que coincida con el valor de la facilidad que su servidor syslog está configurado para aceptar y rutear.
- Transporte: udp (valor predeterminado). Se utiliza tcp para entrega fiable (requiere APIC 5.2(3) o posterior) o ssl para transporte cifrado (requiere APIC 5.2(4) o posterior y un certificado cargado en el APIC).
- EPG de administración: seleccione el EPG de administración que tiene disponibilidad para el servidor syslog. Para la gestión OOB: uni/tn-mgmt/mgmtp-default/oob-default. Para la administración en banda, seleccione el EPG en banda adecuado. Este campo no debe estar vacío.

Haga clic en Aceptar y, a continuación, en Finalizar.

Nota: Puede agregar varios destinos remotos al mismo grupo de destino. Cada destino puede tener un umbral de gravedad, una instalación y un protocolo de transporte diferentes.

Paso 3: Cree un origen de Syslog en la política de supervisión de fabric



Este paso configura syslog para la jerarquía de objetos de fabric: puertos de fabric, tarjetas, componentes de chasis y bandejas de ventilador. Esto complementa la política de supervisión común (paso 4) con un control específico de la jerarquía.

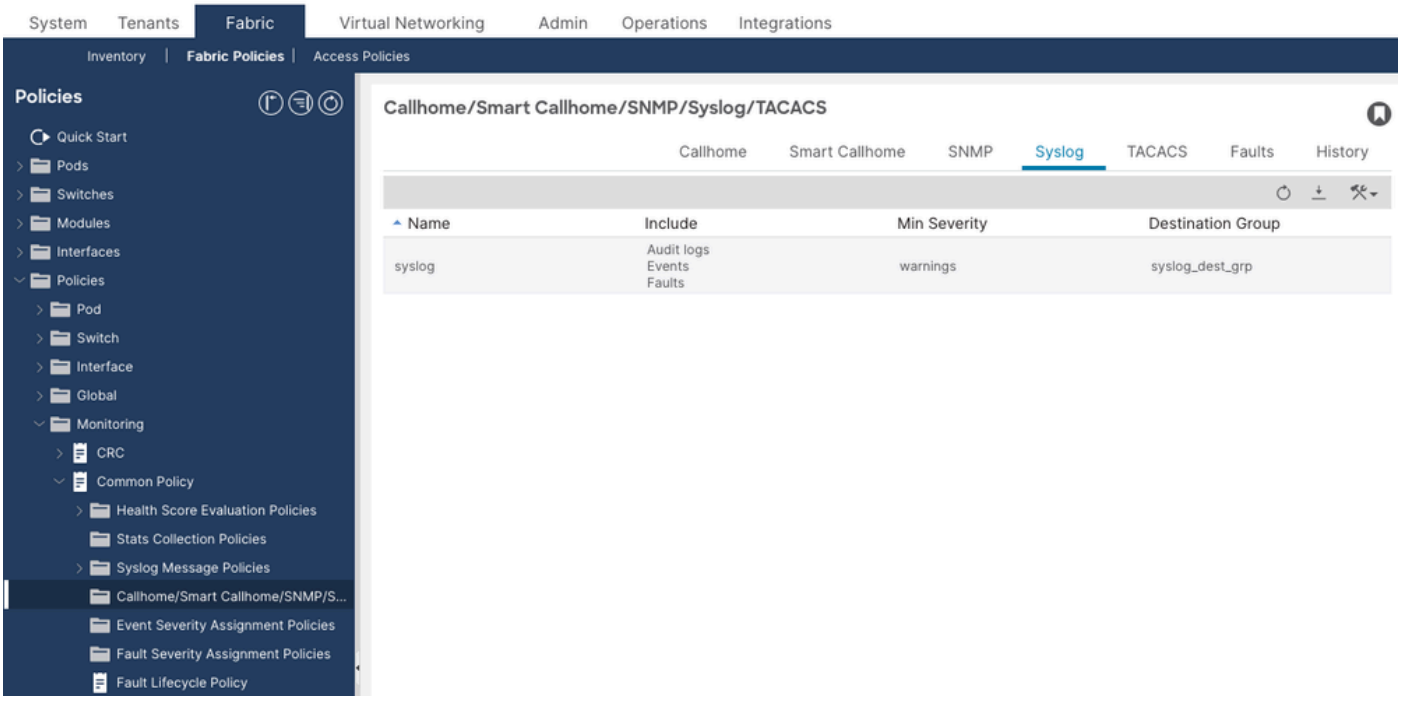
Vaya a Fabric > Fabric Policies > Policies > Monitoring > default > Callhome/Smart Callhome/SNMP/Syslog/TACACS.

En el panel derecho, establezca Tipo de Origen en Syslog. Haga clic en + para crear un origen de syslog:

- Nombre: un nombre descriptivo como Syslog-Source-Fabric.
- Gravedad mínima: information (se recomienda para una cobertura completa).
- Incluir: verifique auditoría, eventos y fallos. Opcionalmente, agregue session para los eventos de login y logout.
- Grupo de destino: seleccione el grupo de destino creado en el paso 1.

Haga clic en Submit (Enviar).

Paso 4: Configuración de la política de supervisión común (registro del sistema en todo el sistema)

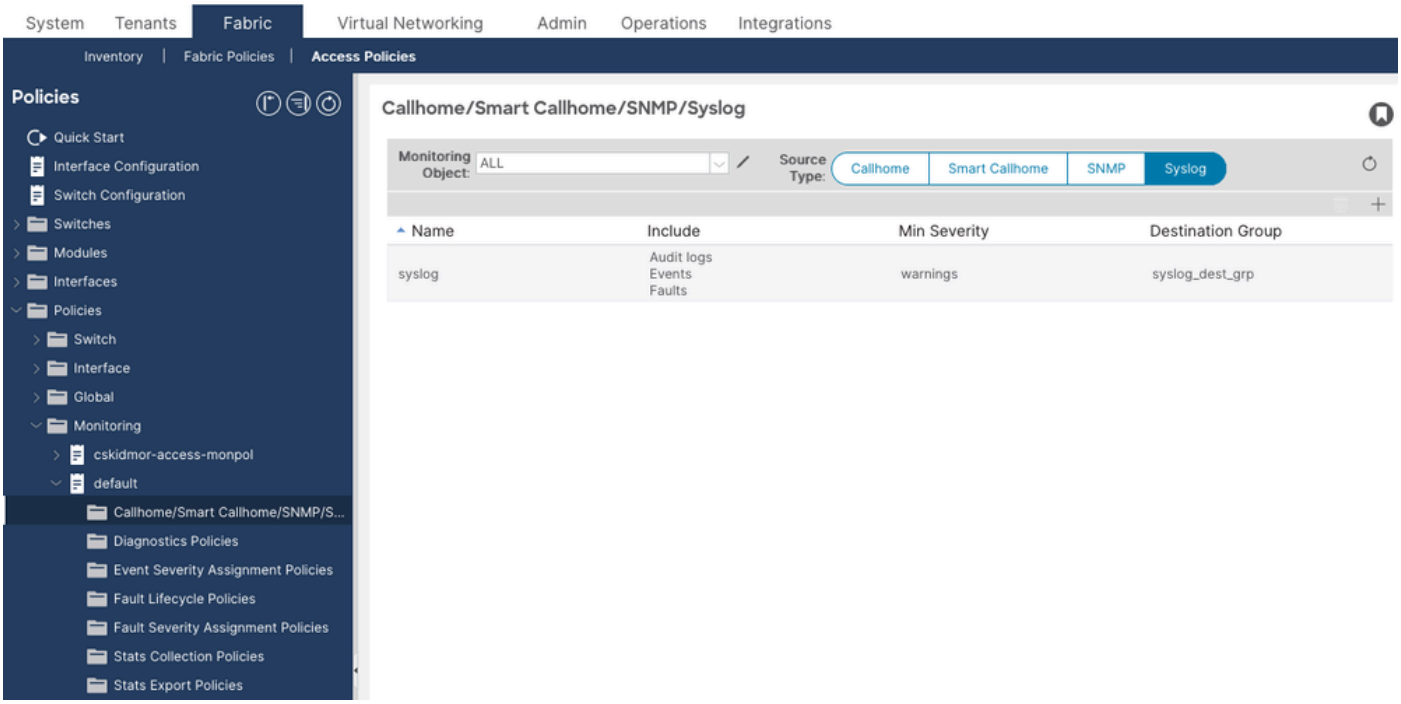


La política de supervisión común proporciona una cobertura de registro del sistema en todo el sistema que se implementa automáticamente en todos los nodos y controladores del fabric. Este paso vincula el origen de syslog del sistema al grupo de destino.

Vaya a Fabric > Fabric Policies > Policies > Monitoring > Common Policy. En la sección Syslog, vincule el origen de syslog del sistema al grupo de destino creado en el Paso 1.

El sistema de políticas comunes de origen de syslog utiliza el MO syslogRsSystemDestGroup en el DN uni/fabric/moncommon/systemslsrc/rssystemDestGroup.

Paso 5: Cree un origen Syslog bajo la política de monitoreo de acceso



Este paso configura el registro del sistema para la jerarquía de objetos de acceso: puertos de acceso, dispositivos Fabric Extender (FEX) y eventos de controlador de máquina virtual (VM). Esto complementa la política de supervisión común (paso 4) con un control específico de la jerarquía.

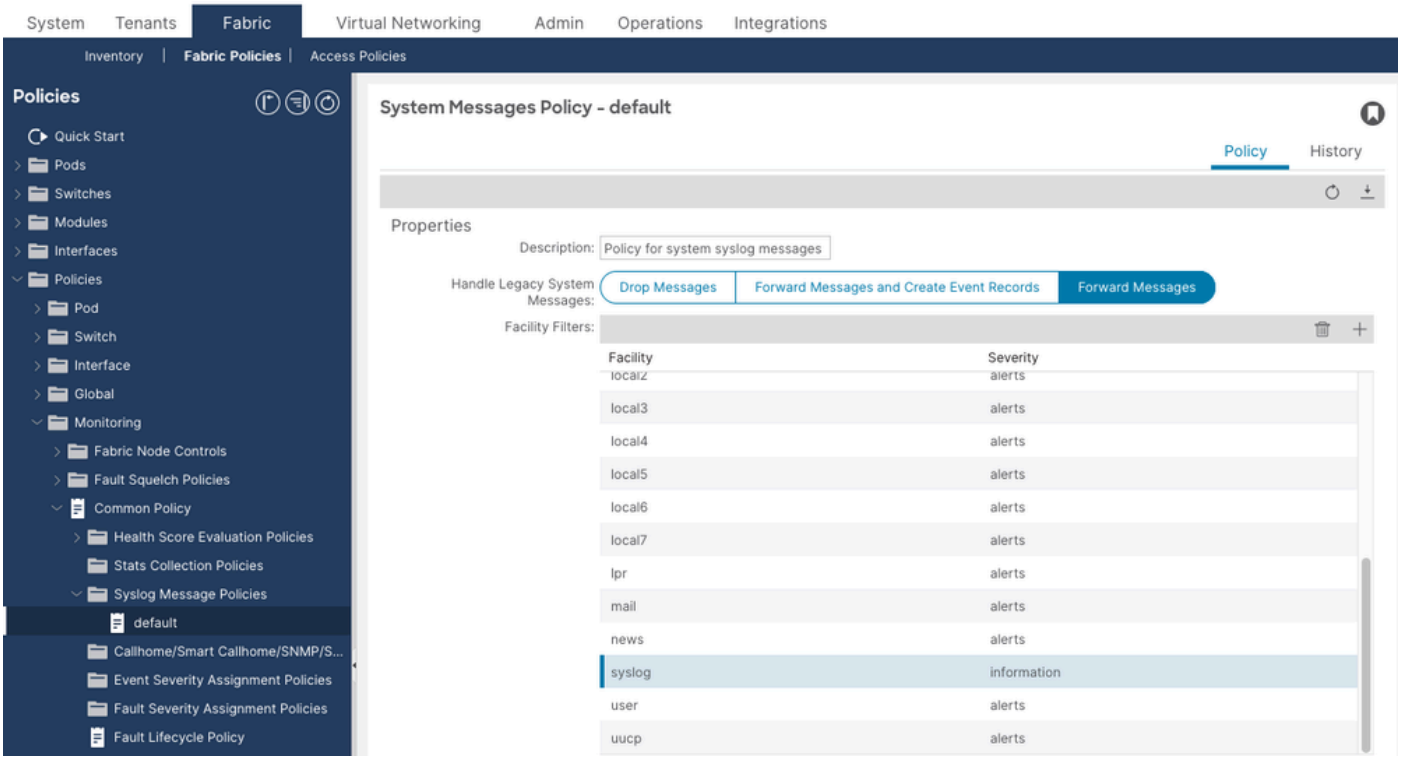
Vaya a Fabric > Access Policies > Policies > Monitoring Policies > default > Callhome/SNMP/Syslog.

Establezca Source Type en Syslog. Haga clic en + y configure los mismos parámetros que en el paso 3:

- Nombre: por ejemplo, Syslog-Source-Access.
- Gravedad mínima: information.
- Incluir: verifique auditoría, eventos y fallos.
- Grupo de destino: seleccione el mismo grupo de destino.

Haga clic en Submit (Enviar).

Paso 6 (opcional): Ajuste de la Política de Mensajes de Syslog para el Registro de ACL de Contrato



Si necesita que los registros de paquetes (ACLLOG_PKTLOG_PERMIT / ACLLOG_PKTLOG_DENY) de permiso o denegación de ACL de contrato aparezcan en el servidor syslog remoto, el filtro de la función de mensajes syslog debe configurarse en la gravedad informativa.

Vaya a Fabric > Fabric Policies > Policies > Monitoring > Common Policy > Syslog Message Policies > default. En la lista de filtros de recursos, seleccione el recurso syslog y establezca su Gravedad mínima en information. Este es el syslogFacilityFilter MO en DN uni/fabric/moncommon/sysmsgp/ff-syslog.

Nota: Para que los registros de permiso y denegación de ACL de contrato lleguen al servidor syslog remoto, deben cumplirse cuatro condiciones: (1) el syslog source minSev debe ser información, (2) la gravedad del destino remoto debe ser información, (3) el syslog Message Policy syslog facility filter minSev debe ser información, y (4) la directiva Log debe estar habilitada en la entrada de filtro de contrato. Cuando se cumplen las tres condiciones, los mensajes de registro de ACL se originan desde el switch de hoja (no desde el APIC), por lo que aparecen en `/var/log/external/messages` en la hoja primero. CoPP limita las velocidades de registro de paquetes de ACL de contrato: deny logs default a 500 packets per second (pps) y permit logs default a 300 pps per leaf.

Nota: No se admite el uso de la directiva Log en los filtros de los contratos de administración y provoca un error en la implementación de la regla de zonificación. Aplique el registro de contratos solo a los contratos de plano de datos de arrendatarios.

Verifique la Configuración

Verifique la configuración antes de resolver cualquier problema operativo. La causa raíz más común de la falta de mensajes de syslog es la configuración incorrecta, no una falla de red o de software.

Verificar el Grupo de Destino y el Perfil

Ejecute **moquery -c syslogGroup** en el APIC para confirmar que existen grupos de destino y verifique sus 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
```

A continuación, verifique el perfil (estado de administrador de nivel de grupo) 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
```

Para encontrar cualquier grupo de destino cuyo perfil esté inhabilitado, ejecute:

<#root>

```
apic1#

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

Un resultado aquí significa que el grupo de destino no está reenviando ningún tráfico de syslog independientemente del estado de administración de destino remoto.

Verificar el destino remoto

Ejecute **moquery -c syslogRemoteDest** para verificar cada configuración 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
```

Hay tres atributos que requieren una atención especial:

- adminState: debe serlo enabled. Si se inhabilita, este servidor remoto específico no recibe nada.
- epgDn: no debe estar vacío. Un valor vacío epgDn significa que el entramado no sabe desde qué interfaz enviar el tráfico de syslog, por lo que no hay mensajes que salgan del

entramado.
- operState: desconocido: se espera este valor y no indica un problema. ACI no sondea activamente la disponibilidad de los servidores de syslog.

Verificar las fuentes de Syslog

Ejecute **moquery -c syslogSrc** para confirmar que existen orígenes bajo las políticas de monitoreo correctas:

<#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 la existencia de orígenes en las políticas de supervisión apropiadas:

- Un origen bajo uni/fabric/moncommon : la Política de supervisión común, para la cobertura de todo el fabric de todos los nodos y todas las jerarquías de objetos.
- Una fuente en uni/infra/moninfra-default : la política de supervisión de fabric, para los objetos de nivel de fabric (puertos de fabric, tarjetas, chasis).
- Un origen en uni/fabric/monfab-default : la directiva de supervisión de acceso, para objetos de nivel de acceso (puertos de acceso, FEX, controladores de VM).

También verifique que el origen de syslog del sistema de Política de Monitoreo Común esté vinculado:

<#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
```

Si se requiere el registro de ACL de contrato, verifique la gravedad del filtro de la utilidad de política de mensajes de 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
```

Verificar el archivo de registro local

El archivo local en /var/log/external/messages es la manera más directa de confirmar que los mensajes de syslog se están generando en cualquier nodo de fabric, incluso cuando no se puede alcanzar un servidor remoto. Compruébelo tanto en el APIC como en un switch de hoja:

<#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
```

Si este archivo está vacío o no se actualiza en un nodo, no se generarán mensajes en el origen. Si el archivo tiene contenido pero el servidor syslog remoto no recibe mensajes, el problema está en el reenvío (grupo de destino, red o firewall), no en la generación de mensajes.

Verificar la disponibilidad del servidor Syslog

Ejecute un ping desde el APIC al servidor syslog para verificar el alcance IP a través de la red de administración:

```
<#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
```

Desde un switch de columna u hoja, utilice `iping` con el indicador `-V` para especificar el VRF. Utilice `management` para fuera de banda o `mgmt:inb` para dentro de banda, dependiendo del EPG de administración asignado al destino de 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
```

Un ping exitoso confirma la disponibilidad de IP pero no confirma que el puerto 514 UDP o TCP esté permitido. El protocolo de mensajes de control de Internet (ICMP) y syslog utilizan protocolos diferentes.

Resolución de problemas

Flujo de trabajo de selección

Utilice el siguiente árbol de decisiones cuando los mensajes de syslog no lleguen al 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
```

Escenarios de ejemplo

Escenario 1: No se reciben mensajes de Syslog en el servidor remoto

Problema: El grupo de destino de syslog y el destino remoto están configurados, pero no llega ningún mensaje al servidor remoto. El archivo local /var/log/external/messages en el APIC y los switches contiene entradas recientes.

Comprobación de configuración:

<#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 raíz: El estado del administrador de destino remoto es disabled. Esto puede suceder si el destino fue creado pero inadvertidamente dejado inhabilitado, o si fue inhabilitado durante el mantenimiento y nunca se volvió a habilitar.

Solución: Vaya a Admin > External Data Collectors > Monitoring Destinations > Syslog > [group name] > Remote Destinations > [server]. Edite el destino remoto y establezca Admin State en enabled.

Escenario 2: El Perfil Del Grupo De Destino De Syslog Está Inhabilitado

Problema: No se reenvían mensajes desde ningún nodo aunque el estado de administración de destino remoto esté habilitado.

Comprobación de configuración:

<#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 raíz: El syslogProf estado de administrador controla todo el grupo de destino. Cuando está inhabilitada, no se reenvía ningún mensaje desde ningún nodo independientemente de los estados de destino remoto individuales.

Solución: Vaya a Admin > External Data Collectors > Monitoring Destinations > Syslog > [group name]. Edite el perfil y establezca Admin State en enabled.

Escenario 3: Eventos que faltan: Política de supervisión común no vinculada

Problema: Los mensajes de registro del sistema de algunos nodos o jerarquías de objetos no están llegando al servidor remoto, aunque se haya configurado un origen de registro del sistema en la directiva de supervisión de acceso o fabric.

Comprobación de configuración:

<#root>

```
apic1#

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

Total Objects shown: 0
```

El origen de syslog del sistema de Directiva de supervisión común no está vinculado al grupo de destino.

Causa raíz: La política de supervisión común (uni/fabric/moncommon) proporciona cobertura de registro del sistema en todo el fabric en todas las jerarquías y se implementa automáticamente en todos los nodos y controladores. Sin ella, solo se reenvían los eventos que coinciden con las jerarquías específicas de la política de supervisión de acceso o fabric. La política de supervisión de fabric (uni/infra/moninfra-default) cubre los objetos de nivel de fabric y la política de supervisión de acceso (uni/fabric/monfab-default) cubre los objetos de nivel de acceso, pero ninguna de las dos proporciona la

cobertura de todo el fabric que ofrece la política común.

Solución: Vaya a Fabric > Fabric Policies > Policies > Monitoring > Common Policy. En la sección Syslog, vincule el origen de syslog del sistema al grupo de destino. Compruebe con **moquery -d uni/fabric/moncommon/systemslsrc/rssystemDestGroup** que el tDn apunta al grupo de destino.

Escenario 4: Gravedad Demasiado Restrictiva: Faltan Mensajes Esperados

Problema: Algunos mensajes llegan al servidor syslog, pero faltan eventos informativos, entradas del registro de auditoría o eventos de inicio de sesión. Solo se ven fallos importantes y críticos.

Comprobación de configuración:

<#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 raíz: El filtrado de Syslog se produce en dos puntos: el origen (minSev) y el destino remoto (severity). Sólo se reenvían los mensajes que superan ambos filtros. Si se establece alguno de los dos arriba information, los mensajes informativos se descartan.

Solución: Edite el origen de syslog y establezca Gravedad mínima en información, y verifique auditoría, eventos, fallas en el campo Incluir. Edite el destino remoto y establezca Severity en information.

Escenario 5: No hay ningún EPG de gestión asignado al destino remoto

Problema: No se reciben mensajes de syslog en el servidor remoto. El grupo de destino está habilitado, el destino remoto está habilitado y el archivo de registro local tiene contenido.

Comprobación de configuración:

<#root>

```
apic1#

moquery -c syslogRemoteDest

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

Causa raíz: Sin un EPG de administración, el APIC y los switches no saben qué interfaz física utilizar para enviar mensajes de syslog. Los mensajes se generan pero no se pueden reenviar.

Solución: Edite el destino remoto y seleccione el EPG de administración adecuado. Para la administración OOB, seleccione uni/tn-mgmt/mgmtp-default/oob-default. Para la administración en banda, seleccione el EPG en banda adecuado.

Escenario 6: EPG de administración incorrecto (en banda frente a fuera de banda)

Problema: Los mensajes de Syslog llegan intermitentemente o sólo desde algunos nodos. El servidor syslog sólo es accesible a través de la administración OOB, pero el destino remoto hace referencia al EPG en banda.

Comprobación de configuración:

<#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
```

Si el servidor syslog sólo es accesible a través de la red OOB, el EPG en banda hace que los mensajes se originen desde la interfaz en banda, que no puede alcanzar el servidor.

Solución: Edite el destino remoto y cambie el EPG de administración a uni/tn-mgmt/mgmtp-default/oob-default. Verifique con **ping -c 3 10.1.1.100** desde el bash APIC para confirmar la disponibilidad OOB.

Escenario 7: Firewall que bloquea el tráfico de Syslog

Problema: El archivo de registro local tiene contenido en los nodos de hoja y APIC, la configuración es correcta, el ping ICMP al servidor syslog se realiza correctamente, pero no llega ningún mensaje al servidor.

Comprobación operativa: Ejecute un ping desde el APIC al servidor syslog para verificar el alcance 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
```

El ping se realiza correctamente, pero los mensajes de syslog no llegan. El ICMP (ping) pasa mientras el puerto UDP 514 está bloqueado.

Causa raíz: Un firewall o ACL entre la red de administración y el servidor syslog está bloqueando el puerto UDP 514 (o TCP 514 si se configura el transporte TCP). El ICMP y el UDP son independientes — El paso del ICMP no confirma que el UDP 514 esté permitido. Además, cada hoja y columna envía syslog directamente desde su propia dirección IP OOB. Un firewall que permite solo las IP OOB de APIC descarta paquetes syslog que se originan en los nodos del switch.

Solución: Verifique que el firewall permita el puerto 514 UDP/TCP desde el rango de direcciones IP OOB de todos los nodos de fabric, incluidos todos los APIC, todos los switches de hoja y todos los switches de columna. Una captura de paquetes en el servidor syslog confirma si los paquetes UDP 514 están llegando.

Escenario 8: Registros de permiso/denegación de ACL del contrato que no llegan

Problema: Los registros de paquetes de permiso o denegación de contrato (ACLLOG_PKTLOG_PERMIT / ACLLOG_PKTLOG_DENY) no llegan al servidor syslog.

Comprobación de configuración:

1. Verifique que la gravedad del origen de syslog sea information:
   <#root>

   ```
   apic1#

   moquery -c syslogSrc

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

2. Verifique que la gravedad del destino remoto sea information:
   <#root>

   ```
   apic1#

   moquery -c syslogRemoteDest

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

3. Verifique que la gravedad del filtro del recurso de directiva de mensajes de Syslog sea 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 que la directiva de registro esté habilitada en el filtro de contrato. Navegue hasta Arrendatarios > [arrendatario] > Contratos > [contrato] > Sujetos > [asunto] > Filtros y confirme que la columna Directivas muestra el registro para la entrada de filtro pertinente.
5. Verifique que los registros de ACL se estén generando en el switch de hoja (los registros de ACL se originan en la hoja, no en el APIC):
   <#root>

   ```
   leaf1#

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

<#root>

leaf1#

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

Si no aparece ninguna ACLLOG entrada, la directiva de registro no está activando la generación de registro en la hoja. Esto puede indicar una directiva de contrato mal configurada, que ningún tráfico coincidente está llegando al contrato o que la limitación de velocidad CoPP está descartando paquetes antes de que se registren.

Causa raíz: El nivel de gravedad del registro ACL del contrato es informational (syslog nivel 6). Si algún filtro en la cadena de syslog — origen minSev, destino remoto severity, o el filtro de recurso de política de mensajes de Syslog (syslogFacilityFilter en uni/fabric/moncommon/sysmsgp/ff-syslog) — se configura arriba information, los mensajes de registro de ACL se descartan silenciosamente antes de salir del nodo de fabric.

Solución: Configure minSev en information en el origen de syslog, configure severity en information en el destino remoto, configure el filtro de syslog facilidad minSev en information en Política Común > Políticas de Mensajes de Syslog > predeterminado, confirme que la directiva Log esté habilitada en el filtro de contrato y verifique que el firewall permita el tráfico de syslog desde las direcciones IP OOB del switch de hoja, no sólo las IP APIC, porque los registros ACL se envían desde el switch.

Escenario 9: Syslog se detiene después de cambiar el nombre del grupo de destino

Problema: Los mensajes de registro del sistema dejan de llegar al servidor remoto después de cambiar el nombre del grupo de destino de registro del sistema. El cambio del puerto o la instalación no causa este problema. Al deshabilitar y volver a habilitar la directiva no se reanuda la entrega de mensajes.

Causa raíz: Se trata de un defecto de software conocido. Consulte Cisco bug ID CSCwj23752. Al cambiar el nombre del grupo de destino se interrumpe la asociación interna de reenvío de syslog. Se corrige en la versión APIC 6.0(6) y posteriores.

Solución: Actualice a la versión APIC 6.0(6c) o posterior. Como solución alternativa para las versiones afectadas, elimine el grupo de destino renombrado y vuelva a crearlo con el nombre deseado, luego vuelva a asociar los orígenes de syslog.

Escenario 10: Syslog excesivo que causa lentitud en la GUI de APIC

Problema: La GUI de APIC se ralentiza y la utilización de la CPU de APIC es alta. Esto puede

ocurrir cuando el registro de ACL de contrato se deja habilitado durante las operaciones normales, lo que genera un gran volumen de mensajes de syslog informativos que se convierten en eventRecord objetos en la base de datos APIC.

Causa raíz: Cuando Common Policy Syslog Message Policy severity se establece en information, cada mensaje de syslog informativo, incluidos los registros de ACL de gran volumen, genera un error eventRecord en el APIC. Esto puede saturar la base de datos APIC y causar lentitud en la GUI.

Solución:

- Inhabilite el registro de ACL de contrato durante las operaciones normales. Actívela sólo durante las fases de solución de problemas o mantenimiento.
- Si el registro de ACL debe permanecer habilitado, establezca la gravedad de la política de mensajes de Syslog en alertsFabric > Fabric Policies > Policies > Monitoring > Common Policy > Syslog Message Policies > default. Esto evita que los mensajes de syslog informativos se conviertan en eventos, al tiempo que permite que se reenvíen al servidor syslog remoto.
- Aplique códigos de eventos ruidosos que no sean útiles desde el punto de vista operativo. Un código de evento se puede silenciar para evitar que genere registros de eventos sin afectar al reenvío de syslog.

Error de funcionamiento conocido

Los siguientes defectos de software conocidos afectan a la funcionalidad de syslog de ACI:

- Cisco bug ID CSCwj23752: al cambiar el nombre del grupo de destino de syslog se detiene la entrega de syslog. Se ha corregido en la versión 6.0(6c) y posteriores de APIC.

Criterios de escalado

Recopile un soporte técnico e involucre al TAC de Cisco cuando:

- Los mensajes de Syslog aparecen en /var/log/external/messages forma local en los nodos de fabric, los estados de administración del grupo de destino y del destino remoto son ambos enabled, el EPG de administración es correcto, se confirma la disponibilidad de la red (ping y paso de comprobación del firewall), pero los mensajes siguen sin llegar al servidor remoto.
- Los mensajes de Syslog proceden de algunos nodos de fabric, pero no de otros, sin diferencias de configuración entre ellos, lo que sugiere una incoherencia en la implementación de políticas.
- El perfil de grupo de destino o el destino remoto se volvieron a habilitar, pero los mensajes

no se reanudan a los pocos minutos del cambio de configuración.
- Los mensajes de Syslog dejaron de llegar después de una actualización de APIC, lo que sugiere un posible defecto de software.

Datos que se deben recopilar antes de abrir un caso TAC:

- Asistencia técnica a demanda desde el APIC afectado y un nodo de hoja afectado.
- Salida de `moquery -c syslogGroup`, `moquery -c syslogProf`, `moquery -c syslogRemoteDest`, y `moquery -c syslogSrc` del APIC.
- Salida de `moquery -d uni/fabric/moncommon/systemslsrc/rssystemDestGroup` para verificar el enlace de Política común.
- Cola de `/var/log/external/messages` desde un APIC y una hoja afectada.
- Captura de paquetes desde el servidor syslog que confirma si los paquetes UDP/TCP 514 llegan desde las direcciones OOB del fabric.

Referencias

- Guía de configuración básica de Cisco APIC, versión 6.1(x) — Gestión
- Guía de referencia de mensajes del sistema Cisco ACI
- Guía de administración de fallos, eventos y mensajes del sistema de Cisco ACI
- Informe técnico de la guía de contratos de Cisco ACI
- Resolución de problemas de una GUI de Slow APIC

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).