Configuration et dépannage de Syslog dans l'ACI

Introduction

Ce document décrit comment configurer, vérifier et dépanner la journalisation système (syslog) dans l'infrastructure axée sur les applications (ACI) de Cisco. Il couvre l'ensemble du workflow de configuration, la vérification programmatique à l'aide du modèle d'objet géré APIC (Application Policy Infrastructure Controller) et un workflow de dépannage structuré pour les contrôleurs APIC et les commutateurs Leaf et Spine.

Aperçu

Le syslog ACI est entièrement piloté par des politiques. Contrairement au logiciel Cisco NX-OS® autonome, il n'existe pas de commandes **logging server** CLI sur les commutateurs Leaf ou Spine de l'ACI. Toute la configuration Syslog est effectuée via des politiques APIC que l'APIC envoie automatiquement à chaque noeud de fabric.

Composants clés

Le sous-système syslog de l'ACI est construit à partir des objets gérés suivants :

- Syslog Destination Group (syslogGroup) : conteneur de niveau supérieur pour toutes les destinations Syslog. Il contrôle le format du message (de type ACI ou NX-OS) et les options d'horodatage. Il peut contenir une ou plusieurs destinations distantes, une destination de fichier local et une destination de console.
- Profil Syslog (syslogProf) : enfant du groupe de destination qui contrôle l'état administratif au niveau du groupe et le protocole de transport (UDP, TCP ou SSL).
- Syslog Remote Destination (syslogRemoteDest) : enfant du groupe de destinations représentant un serveur syslog distant. Contrôle l'adresse IP ou le nom d'hôte du serveur, le port, le filtre de gravité, l'utilitaire Syslog et le groupe de terminaux de gestion (EPG) utilisés pour atteindre le serveur.
- Fichier local Syslog (syslogFile) : enfant du groupe de destinations qui contrôle l'écriture des messages Syslog dans le fichier local /var/log/external/messages sur chaque noeud de fabric.
- Syslog Source (syslogSrc) : associé à une stratégie de surveillance. Contrôle les types de messages (audit, événements, pannes, session) et la gravité minimale envoyés, et établit des liens vers le groupe de destination via une syslogRsDestGroup relation.

Points de connexion source Syslog

L'ACI utilise quatre étendues de politiques de surveillance qui contrôlent quels noeuds et objets génèrent des messages syslog :

- Politique commune de surveillance (monCommonPol, uni/fabric/moncommon) - Portée à l'échelle du fabric. Stratégie de surveillance de base qui s'applique à tous les pannes et événements et qui est automatiquement déployée sur tous les noeuds (commutateurs Leaf et Spine) et tous les contrôleurs (APIC) du fabric. Couvre toutes les hiérarchies de fabric, d'accès et de locataire. Dans Fabric > Fabric Policies > Policies > Monitoring > Common Policy.
- Politique de surveillance du fabric (monInfraPol, uni/infra/moninfra-default) : étendue du fabric. Génère un journal système pour les objets au niveau du fabric : les ports de matrice, les cartes, les composants du châssis et les unités de ventilation. Dans Fabric > Fabric Policies > Policies > Monitoring > default.
- Access Monitoring Policy (monFabricPol, uni/fabric/monfab-default) : étendue de l'accès (infrastructure). Génère un journal système pour les composants d'accès : les ports d'accès, les périphériques Fabric Extender (FEX) et les événements de contrôleur de machine virtuelle (VM). Dans Fabric > Access Policies > Policies > Monitoring Policies > default.
- Stratégie de surveillance du locataire (monEPGPol, uni/tn-common/monepg-default) — Étendue du locataire. Génère le syslog pour les objets étendus par les locataires : groupes de terminaux (EPG), profils d'application et services. Trouvé sous chaque locataire à l'adresse [Locataire] > Stratégies de surveillance > par défaut.

Remarque : La stratégie de surveillance commune est le point de départ recommandé pour la configuration Syslog, car elle fournit une couverture à l'échelle du fabric sur toutes les hiérarchies et est automatiquement déployée sur tous les noeuds. Les stratégies de surveillance de structure et d'accès peuvent être configurées en plus de la stratégie commune pour un contrôle plus granulaire sur des hiérarchies d'objets spécifiques, ou à la place de la stratégie commune pour limiter Syslog à une portée plus étroite.

Format de message Syslog

Les messages syslog ACI suivent le format RFC 3164 quand le format de groupe est défini sur aci (le format par défaut) :

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

Exemple :

```
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
```

Le corps du message inclut le code d'erreur ACI, l'état du cycle de vie (par exemple, soaking, retaining, cleared), la gravité et le nom distinctif (DN) de l'objet affecté, ce qui rend les messages autodescriptifs.

Trois options de format de message sont disponibles :

- aci (par défaut) : format compatible RFC 3164. Recommandé pour la plupart des déploiements.
- nxos — Format de style NX-OS. Utilisez cette option si la plate-forme syslog attend des messages formatés NX-OS.
- Journal amélioré (APIC 5.2(8) et versions ultérieures) : format conforme à la norme RFC 5424 avec horodatages améliorés qui incluent l'année.

Mappage de gravité

Le champ de gravité Syslog est composé d'un seul chiffre compris entre 0 (le plus grave) et 7 (le moins grave). Le tableau suivant présente le mappage entre les niveaux de gravité Syslog et la terminologie de gravité ACI / ITU (International Telecommunication Union) :

Gravité Syslog	Niveau ACI/ITU	Description
0 — urgence	—	Système inutilisable
1 — alerte	Critical (critique)	Action immédiate requise
2 - critique	Major (important)	État critique
3 — Erreur	Minor (mineur)	Condition d'erreur
4 — avertissement	Avertissement	Condition d'avertissement
5 — notification	Indéterminé / Effacé	État normal mais significatif
6 — à titre d'information	—	Message d'information uniquement
7 — débogage	—	Sortie de débogage uniquement

Options de transport

L'ACI prend en charge trois protocoles de transport pour syslog distant :

- UDP (par défaut) : disponible dans toutes les versions du contrôleur APIC. Livraison standard sans interruption.
- TCP : disponible à partir de la version 5.2(3) et ultérieure du contrôleur APIC. Fournit une livraison fiable avec un transport orienté connexion.
- SSL : disponible à partir de la version 5.2(4) et ultérieure du contrôleur APIC. Fournit un

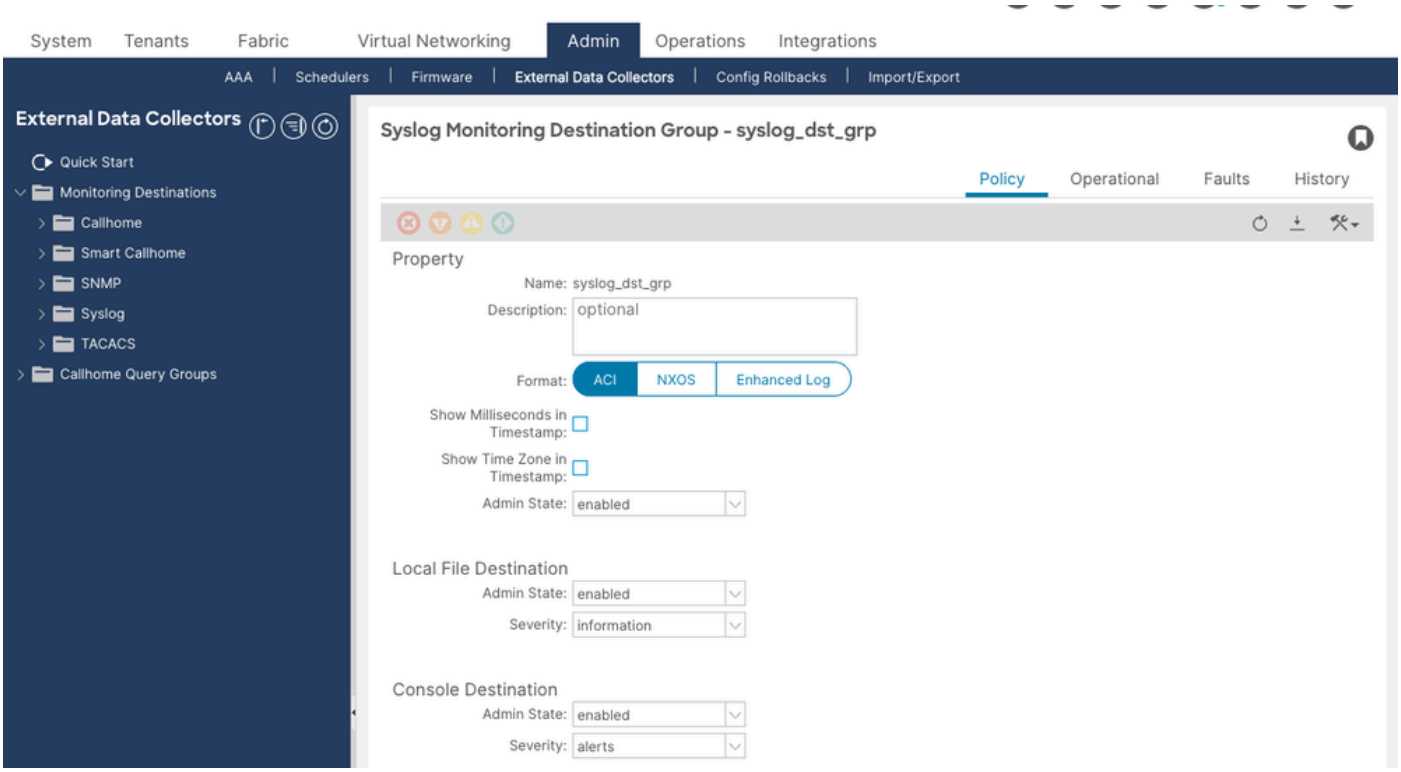
transport chiffré à l'aide de TLS. Chaque noeud ACI (APIC ou commutateur) agit en tant que client TLS et initie une connexion sortante au serveur Syslog. Le certificat du serveur doit être téléchargé vers le contrôleur APIC à l'adresse Admin > AAA > Security > Public Key Management > Certificate Authorities.

Remarque : Si une destination distante est configurée avec le transport SSL et que le contrôleur APIC est rétrogradé à une version qui ne prend pas en charge SSL, le protocole de transport revient automatiquement au protocole UDP. Assurez-vous que le serveur Syslog peut également accepter les connexions UDP comme secours.

Configuration

Les étapes suivantes permettent de configurer le syslog ACI de bout en bout. Exécutez toutes les étapes afin d'activer le transfert syslog à partir des contrôleurs APIC et des commutateurs Leaf et Spine.

Étape 1: Créer le groupe de destinations Syslog



Le groupe de destination définit où les messages Syslog sont envoyés et dans quel format. Créez-le d'abord, car les sources syslog configurées dans les étapes ultérieures font référence à ce groupe par son nom.

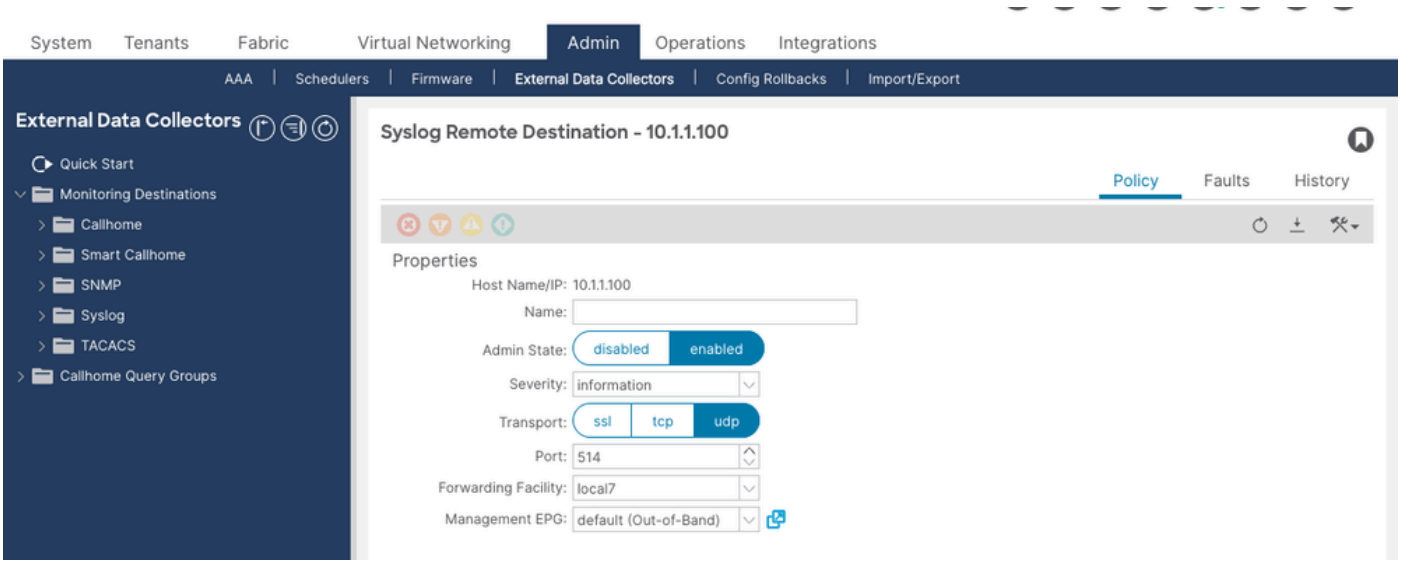
Accédez à Admin > External Data Collectors > Monitoring Destinations > Syslog. Cliquez avec le bouton droit sur Syslog et sélectionnez Créer un groupe de destinations de surveillance Syslog.

Dans l'assistant, configurez les éléments suivants sur la première page (profil de groupe) :

- Nom : nom descriptif tel que Syslog-Dest-Group.
- Format : aci (par défaut, compatible RFC 3164) ou nxos.
- État admin — enabled.
- Local File Destination Admin State : enabled (recommandé). Cette fonction écrit des messages à /var/log/external/messages sur chaque noeud de fabric et est essentielle pour le dépannage local, même lorsqu'un serveur distant est inaccessible.
- Gravité de la destination du fichier local — information.
- Console Destination Admin State — disabled (recommandé pour les environnements de production).

Cliquez sur Suivant. Sur la deuxième page, cliquez sur + dans la zone Create Remote Destinations pour ajouter un serveur syslog distant.

Étape 2: Ajouter une destination distante



Configurez le serveur Syslog distant dans la boîte de dialogue Créer une destination distante Syslog :

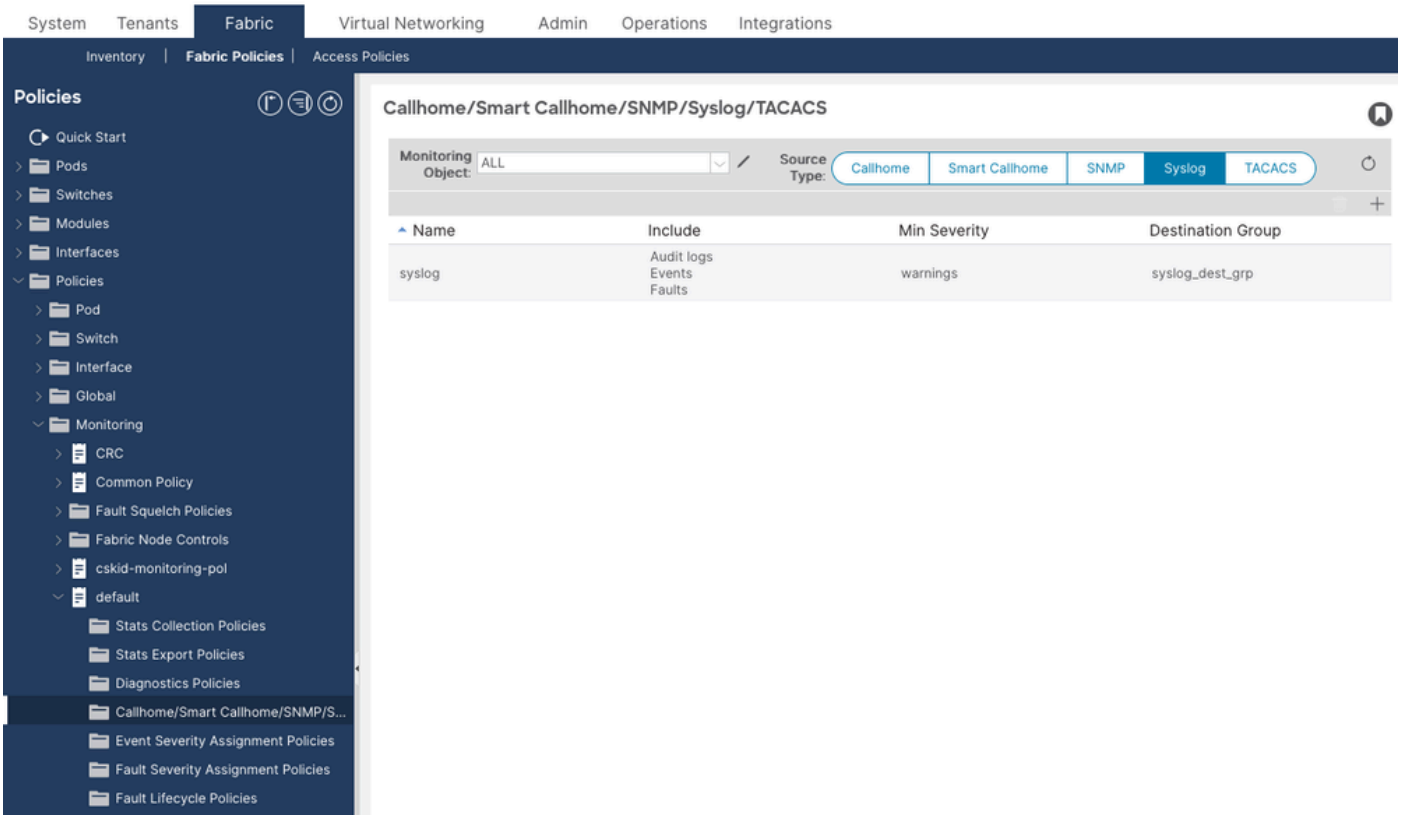
- Host : adresse IP du serveur syslog. Utilisez une adresse IP plutôt qu'un nom d'hôte. Si vous utilisez un nom d'hôte, vous devez vous assurer que le serveur DNS (Domain Name System) est accessible via l'interface de gestion hors bande. Les serveurs DNS accessibles

uniquement via la connectivité intrabande peuvent ne pas être résolus lorsque des messages syslog sont générés pendant une interruption du réseau.
- État admin — enabled.
- Gravité — information (recommandé). Il s'agit de la gravité minimale envoyée à ce serveur distant spécifique.
- Port : 514 (valeur par défaut).
- Facilité — local7 (valeur par défaut). Définissez cette option pour qu'elle corresponde à la valeur de fonction que votre serveur Syslog est configuré pour accepter et router.
- Transport — udp (valeur par défaut). À utiliser tcp pour une livraison fiable (nécessite APIC 5.2(3) ou version ultérieure), ou ssl pour un transport chiffré (nécessite APIC 5.2(4) ou version ultérieure et un certificat téléchargé sur l'APIC).
- Management EPG — Sélectionnez l'EPG de gestion accessible au serveur Syslog. Pour la gestion OOB : uni/tn-mgmt/mgmtp-default/oob-default. Pour l'administration intrabande, sélectionnez l'EPG intrabande approprié. Ce champ ne doit pas être vide.

Cliquez sur OK, puis sur Finish.

Remarque : Vous pouvez ajouter plusieurs destinations distantes au même groupe de destinations. Chaque destination peut avoir un seuil de gravité, une installation et un protocole de transport différents.

Étape 3: Créer une source Syslog sous la stratégie de surveillance du fabric



Cette étape configure syslog pour la hiérarchie d'objets de fabric : ports de fabric, cartes, composants de châssis et unités de ventilation. Cela complète la politique de surveillance commune (étape 4) par un contrôle spécifique à la hiérarchie.

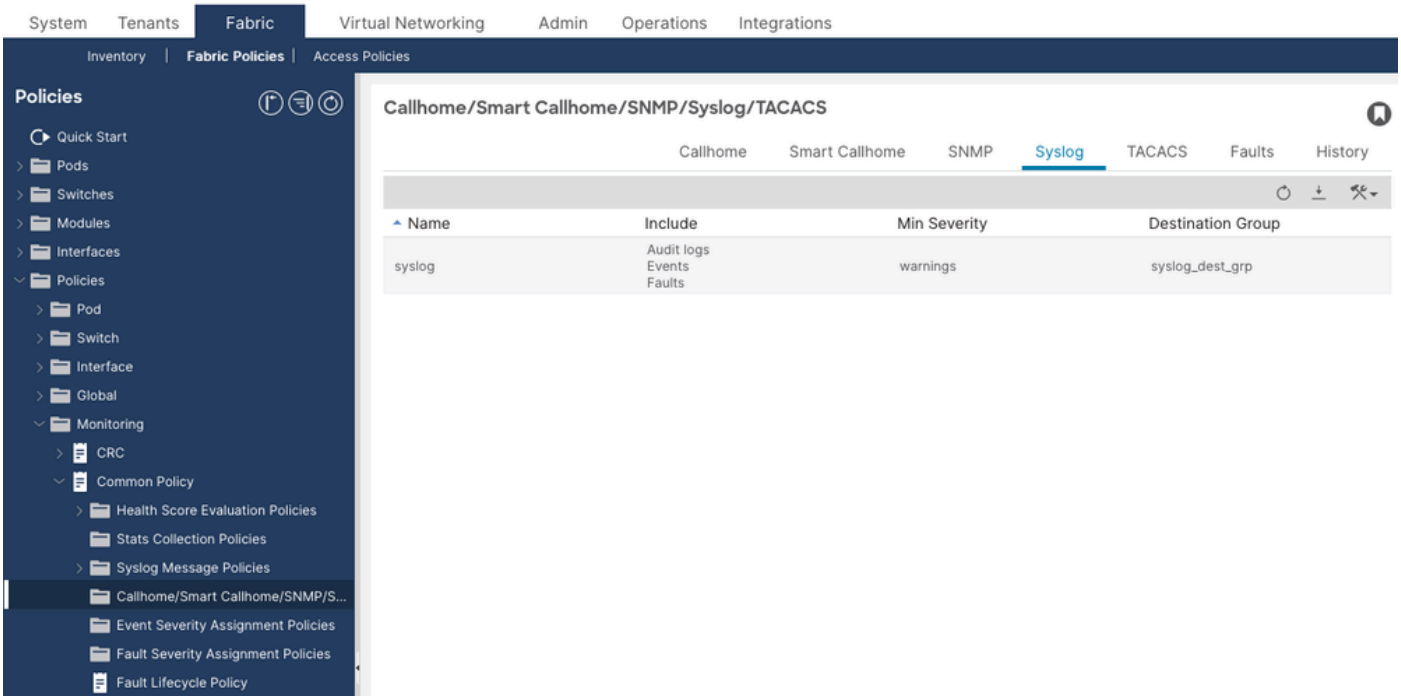
Accédez à Fabric > Fabric Policies > Policies > Monitoring > default > Callhome/Smart Callhome/SNMP/Syslog/TACACS.

Dans le volet droit, définissez Type de source sur Syslog. Cliquez sur + pour créer une source Syslog :

- Nom : nom descriptif tel que Syslog-Source-Fabric.
- Gravité minimale — information (recommandée pour une couverture complète).
- Inclure — Vérifier l'audit, les événements et les défaillances. Ajoutez éventuellement une session pour les événements de connexion et de déconnexion.
- Dest Group : sélectionnez le groupe de destinations créé à l'étape 1.

Cliquez sur Submit.

Étape 4: Configuration de la stratégie de surveillance commune (Syslog système)

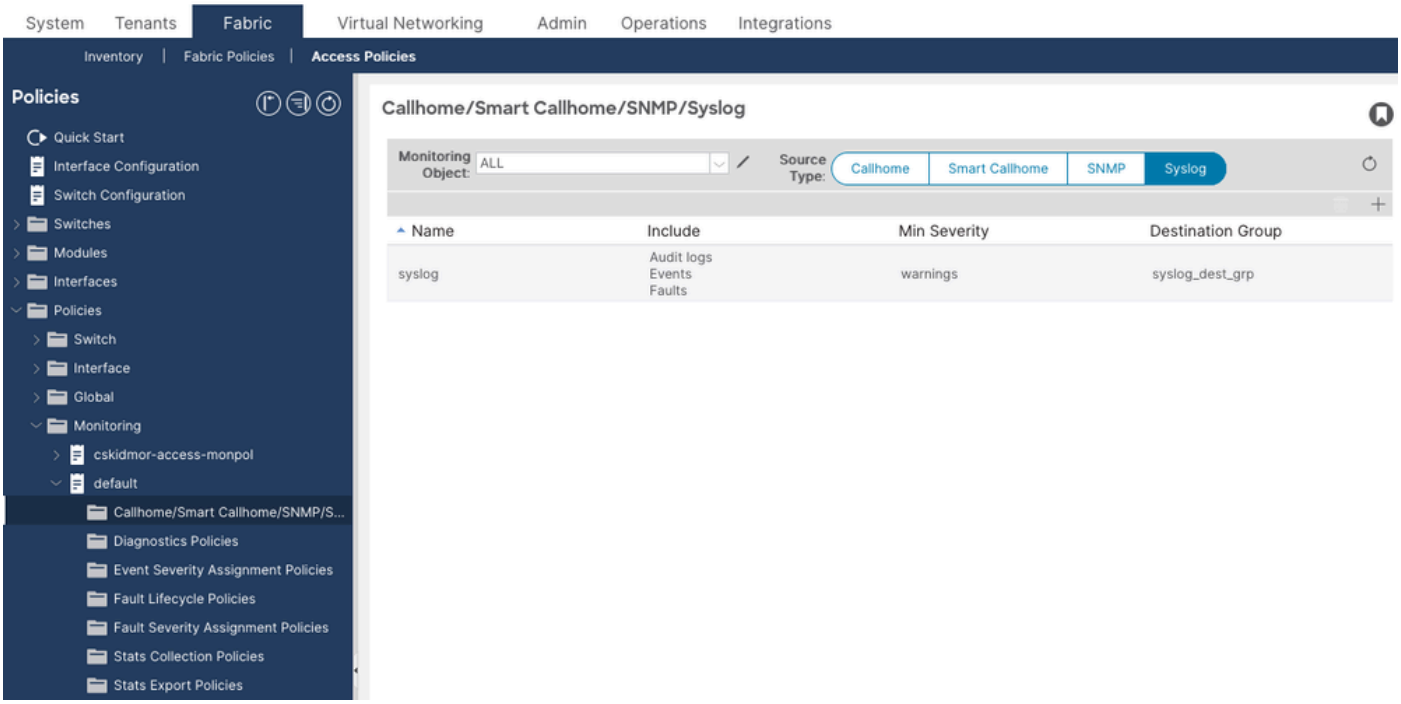


La politique de surveillance commune fournit une couverture syslog à l'échelle du système qui est automatiquement déployée sur tous les noeuds et contrôleurs du fabric. Cette étape relie la source syslog du système au groupe de destination.

Accédez à Fabric > Fabric Policies > Policies > Monitoring > Common Policy. Dans la section Syslog, liez la source syslog du système au groupe de destination créé à l'étape 1.

La source syslog du système Common Policy utilise le mode de gestion syslogRsSystemDestGroup au niveau du DN uni/fabric/moncommon/systemslsrc/rssystemDestGroup.

Étape 5: Créer une source Syslog sous la stratégie de surveillance des accès



Cette étape configure syslog pour la hiérarchie des objets d'accès : les ports d'accès, les périphériques Fabric Extender (FEX) et les événements de contrôleur de machine virtuelle (VM). Cela complète la politique de surveillance commune (étape 4) par un contrôle spécifique à la hiérarchie.

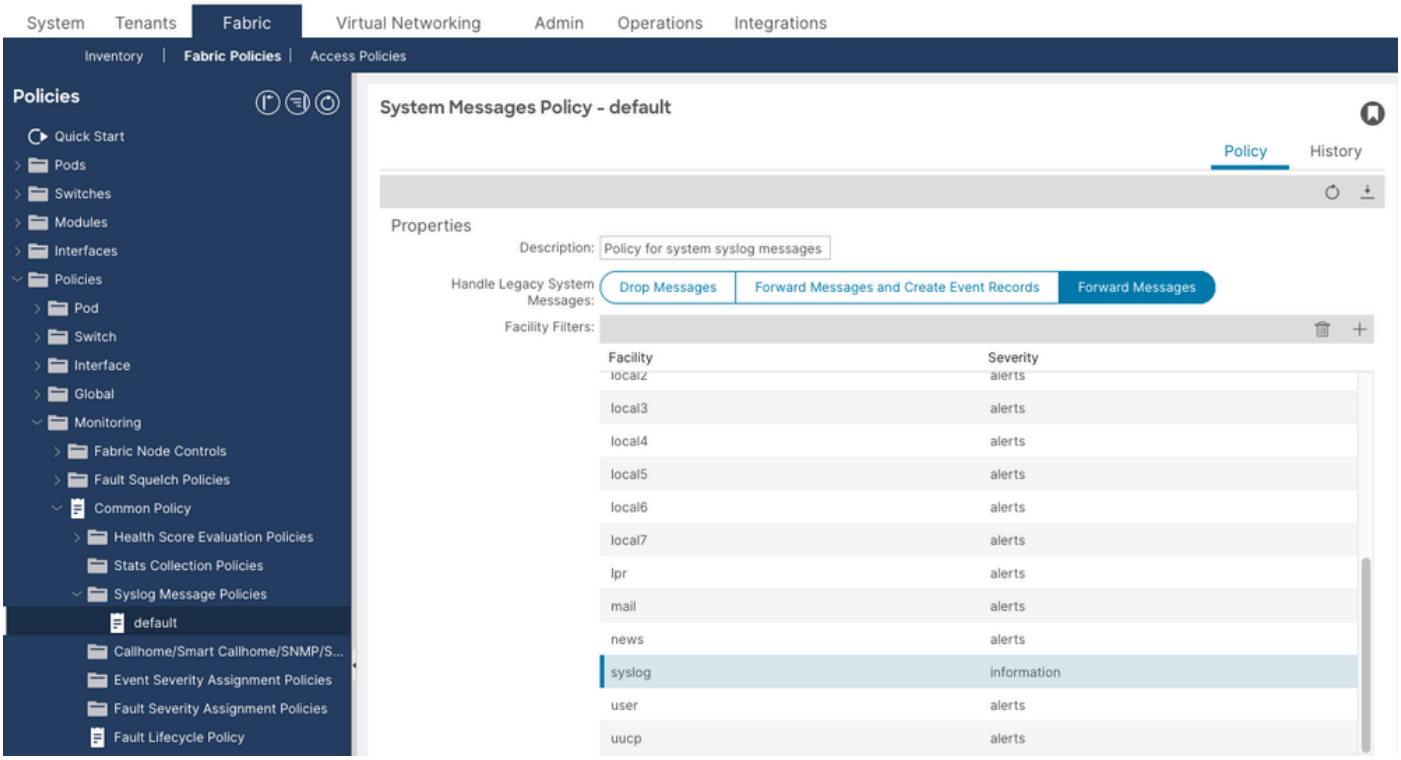
Accédez à Fabric > Access Policies > Policies > Monitoring Policies > default > Callhome/SNMP/Syslog.

Définissez le type de source sur Syslog. Cliquez sur + et configurez les mêmes paramètres que l'étape 3 :

- Name : par exemple, Syslog-Source-Access.
- Gravité minimale — information.
- Inclure — Vérifier l'audit, les événements et les défaillances.
- Dest Group : sélectionnez le même groupe de destinations.

Cliquez sur Submit.

Étape 6 (facultative): Ajuster la stratégie des messages Syslog pour la journalisation des ACL contractuelles



Si vous avez besoin que la liste de contrôle d'accès contractuelle autorise ou refuse l'affichage des journaux de paquets (ACLLOG_PKTLOG_PERMIT / ACLLOG_PKTLOG_DENY) sur le serveur syslog distant, le filtre de l'utilitaire de messages syslog doit être défini sur la gravité informationnelle.

Accédez à Fabric > Fabric Policies > Policies > Monitoring > Common Policy > Syslog Message Policies > default. Dans la liste des filtres d'installation, sélectionnez l'installation syslog et définissez sa gravité minimale sur information. Voici le mode syslogFacilityFilter opératoire de DN uni/fabric/moncommon/sysmsgp/ff-syslog.

Remarque : Pour que les journaux d'autorisation et de refus de la liste de contrôle d'accès contractuelle puissent atteindre le serveur syslog distant, quatre conditions doivent être remplies : (1) la source syslog minSev doit être information, (2) le niveau de gravité de la destination distante doit être information, (3) le filtre d'installation syslog Syslog minSev doit être information, et (4) la directive Log doit être activée sur l'entrée de filtre de contrat. Lorsque les trois conditions sont remplies, les messages de journal de liste de contrôle d'accès proviennent du commutateur leaf (et non du contrôleur APIC), de sorte qu'ils apparaissent dans `/var/log/external/messages` sur le leaf en premier. Les taux de consignation des paquets ACL contractuels sont limités par CoPP : les journaux deny

---

prennent par défaut la valeur de 500 paquets par seconde (pps) et les journaux permit la valeur par défaut de 300 pps par leaf.

Remarque : L'utilisation de la directive Log sur les filtres dans les contrats de gestion n'est pas prise en charge et entraîne un échec du déploiement de la règle de zonage. Appliquez la journalisation de contrat uniquement aux contrats de plan de données du locataire.

Vérification de la configuration

Vérifiez la configuration avant de résoudre tout problème de fonctionnement. La cause la plus courante des messages Syslog manquants est une mauvaise configuration, et non une panne réseau ou logicielle.

Vérification du groupe et du profil de destination

Exécutez **moquery -c syslogGroup** sur le contrôleur APIC afin de confirmer l'existence de groupes de destinations et de vérifier leurs attributs :

```
<#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
```

Vérifiez ensuite le profil (état admin au niveau du groupe) avec **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
```

Pour rechercher un groupe de destinations dont le profil est désactivé, exécutez :

<#root>

```
apic1#

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

Un résultat signifie ici que le groupe de destination ne transfère aucun trafic Syslog quel que soit l'état de l'administrateur de destination distante.

Vérification de la destination distante

Exécutez **moquery -c syslogRemoteDest** pour vérifier chaque configuration de serveur distant :

<#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
```

Trois attributs nécessitent une attention particulière :

- adminState : doit être enabled. S'il est désactivé, ce serveur distant spécifique ne reçoit rien.

- epgDn : ne doit pas être vide. Une valeur vide epgDn signifie que le fabric ne sait pas à partir de quelle interface envoyer le trafic syslog. Par conséquent, aucun message ne quitte le fabric.
- ÉtatOpérateur : inconnu : cette valeur est attendue et n'indique pas de problème. L'ACI ne sonde pas activement les serveurs Syslog pour déterminer leur accessibilité.

Vérification des sources Syslog

Exécutez **moquery -c syslogSrc** pour confirmer que les sources existent sous les stratégies de surveillance correctes :

<#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
```

Confirmez l'existence de sources dans le cadre des stratégies de surveillance appropriées :

- Une source sous uni/fabric/moncommon — la politique de surveillance commune, pour la couverture à l'échelle du fabric de tous les noeuds et de toutes les hiérarchies d'objets.
- Une source sous uni/infra/moninfra-default — la politique de surveillance du fabric, pour les objets au niveau du fabric (ports de fabric, cartes, châssis).
- Une source sous uni/fabric/monfab-default — la politique de surveillance des accès, pour les objets de niveau accès (ports d'accès, FEX, contrôleurs de VM).

Vérifiez également que la source syslog du système Common Monitoring Policy est liée :

<#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 la journalisation de la liste de contrôle d'accès contractuelle est requise, vérifiez le niveau de gravité du filtre de l'utilitaire Syslog Message Policy avec **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
```

Vérification du fichier journal local

Le fichier local de /var/log/external/messages est le moyen le plus direct de confirmer que les messages Syslog sont générés sur n'importe quel noeud de fabric, même lorsqu'un serveur distant n'est pas accessible. Vérifiez-le à la fois sur le contrôleur APIC et sur un commutateur 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
```

Si ce fichier est vide ou ne se met pas à jour sur un noeud, les messages ne sont pas générés à la source. Si le fichier a du contenu mais que le serveur Syslog distant ne reçoit pas de messages, le problème est lié au transfert (groupe de destinations, réseau ou pare-feu) et non à la génération de messages.

Vérification de l'accessibilité au serveur Syslog

Exécutez une requête ping du contrôleur APIC vers le serveur Syslog afin de vérifier l'accessibilité IP sur le réseau de gestion :

```
<#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
```

À partir d'un commutateur Leaf ou Spine, utilisez la `commande ping` avec l'indicateur `-V` pour spécifier le VRF. Utilisez la `gestion` hors bande ou `mgmt:inb` pour l'intrabande, en fonction de l'EPG de gestion affecté à la destination 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
```

Une requête ping réussie confirme l'accessibilité IP mais ne confirme pas que le port UDP ou TCP 514 est autorisé. Les protocoles ICMP (Internet Control Message Protocol) et syslog utilisent des protocoles différents.

Dépannage

Workflow de triage

Utilisez l'arbre de décision suivant lorsque les messages syslog n'arrivent pas sur le serveur distant :

```
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
```

Scénarios courants

Scénario 1 : Aucun message Syslog reçu sur le serveur distant

Problème : Le groupe de destinations syslog et la destination distante sont configurés, mais aucun message n'arrive sur le serveur distant. Le fichier local /var/log/external/messages du contrôleur APIC et des commutateurs contient des entrées récentes.

Vérification de la configuration :

```
<#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
```

Cause première : L'état de l'administrateur de destination distante est disabled. Cela peut se produire si la destination a été créée mais laissée désactivée par inadvertance, ou si elle a été désactivée pendant la maintenance et n'a jamais été réactivée.

Solution : Accédez à Admin > External Data Collectors > Monitoring Destinations > Syslog > [nom du groupe] > Remote Destinations > [serveur]. Modifiez la destination distante et définissez Admin State sur enabled.

Scénario 2 : Le profil du groupe de destinations Syslog est désactivé

Problème : Aucun message n'est transféré à partir d'un noeud même si l'état d'administration de la destination distante est activé.

Vérification de la configuration :

<#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
```

Cause première : L'syslogProfétat admin contrôle l'ensemble du groupe de destinations. Lorsqu'elle est désactivée, aucun message n'est transféré à partir d'un noeud quel que soit l'état de destination distante.

Solution : Accédez à Admin > External Data Collectors > Monitoring Destinations > Syslog > [nom du groupe]. Modifiez le profil et définissez l'état Admin sur activé.

Scénario 3 : Événements manquants — Politique de surveillance commune non liée

Problème : Les messages Syslog de certains noeuds ou hiérarchies d'objets n'atteignent pas le serveur distant, même si une source Syslog est configurée sous la stratégie de surveillance du fabric ou des accès.

Vérification de la configuration :

<#root>

```
apic1#

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

Total Objects shown: 0
```

La source syslog du système de stratégie de surveillance commune n'est pas liée au groupe de destination.

Cause première : La politique de surveillance commune (uni/fabric/moncommonCPS) fournit une couverture syslog à l'échelle du fabric sur toutes les hiérarchies et est automatiquement déployée sur tous les noeuds et contrôleurs. Sans elle, seuls les événements correspondant aux hiérarchies de stratégie de surveillance de fabric ou d'accès spécifiques sont transférés. La politique de surveillance du fabric (uni/infra/moninfra-defaultFabric Monitoring Policy) couvre les objets de niveau

fabric, tandis que la politique de surveillance des accès (Access Monitoring Policyuni/fabric/monfab-default) couvre les objets de niveau accès, mais aucune de ces deux politiques ne fournit la couverture à l'échelle du fabric offerte par la politique commune.

Solution : Accédez à Fabric > Fabric Policies > Policies > Monitoring > Common Policy. Dans la section Syslog, liez la source syslog du système au groupe de destination. Vérifiez avec **moquery -d uni/fabric/moncommon/systemslsrc/rssystemDestGroup** que les tDn points pointent vers votre groupe de destinations.

Scénario 4 : Gravité trop restrictive — Messages attendus manquants

Problème : Certains messages arrivent sur le serveur Syslog, mais des événements d'information, des entrées de journal d'audit ou des événements de connexion à la session sont manquants. Seules les défaillances critiques et majeures sont visibles.

Vérification de la configuration :

<#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
```

Cause première : Le filtrage Syslog se produit en deux points : la source (minSev) et la destination distante (severity). Seuls les messages qui passent les deux filtres sont transférés. Si l'un des deux est défini ci-dessus information, les messages d'information sont abandonnés.

Solution : Modifiez la source syslog et définissez la gravité minimale sur informations, et cochez audit, événements, défaillances dans le champ Inclure. Modifiez la destination distante et définissez la gravité sur informations.

Scénario 5 : Aucun EPG de gestion attribué à la destination distante

Problème : Aucun message syslog n'est reçu sur le serveur distant. Le groupe de destinations est activé, la destination distante est activée et le fichier journal local a du contenu.

Vérification de la configuration :

<#root>

```
apic1#

moquery -c syslogRemoteDest

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

Cause première : Sans EPG de gestion, le contrôleur APIC et les commutateurs ne savent pas quelle interface physique utiliser pour envoyer des messages syslog. Les messages sont générés mais ne peuvent pas être transférés.

Solution : Modifiez la destination distante, puis sélectionnez l'EPG de gestion approprié. Pour la gestion OOB, sélectionnez uni/tn-mgmt/mgmtp-default/oob-default. Pour l'administration intrabande, sélectionnez l'EPG intrabande approprié.

Scénario 6 : EPG de gestion incorrect (intrabande ou hors bande)

Problème : Les messages Syslog arrivent par intermittence ou uniquement de certains noeuds. Le serveur Syslog est uniquement accessible via la gestion OOB, mais la destination distante fait référence à l'EPG intrabande.

Vérification de la configuration :

<#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 le serveur Syslog est uniquement accessible via le réseau OOB, l'EPG intrabande entraîne l'envoi de messages à partir de l'interface intrabande, qui ne peut pas atteindre le serveur.

Solution : Modifiez la destination distante et remplacez Management EPG par uni/tn-mgmt/mgmtp-default/oob-default. Vérifiez avec **ping -c 3 10.1.1.100** à partir du bash APIC pour confirmer l'accessibilité OOB.

Scénario 7 : Pare-feu bloquant le trafic Syslog

Problème : Le fichier journal local a du contenu sur les noeuds APIC et leaf, la configuration est correcte, la requête ping ICMP vers le serveur syslog réussit, mais aucun message n'arrive sur le serveur.

Contrôle opérationnel : Exécutez une requête ping du contrôleur APIC vers le serveur Syslog afin de vérifier l'accessibilité 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
```

La requête ping aboutit, mais les messages syslog n'arrivent pas. ICMP (ping) passe alors que le port UDP 514 est bloqué.

Cause première : Un pare-feu ou une liste de contrôle d'accès entre le réseau de gestion et le serveur Syslog bloque le port UDP 514 (ou TCP 514 si le transport TCP est configuré). ICMP et UDP sont indépendants : le passage ICMP ne confirme pas que le protocole UDP 514 est autorisé. En outre, chaque noeud leaf et spine envoie syslog directement depuis sa propre adresse IP OOB. Un pare-feu qui autorise uniquement les adresses IP OOB APIC abandonne les paquets Syslog provenant des noeuds de commutation.

Solution : Vérifiez que le pare-feu autorise le port UDP/TCP 514 à partir de la plage d'adresses IP OOB de tous les noeuds de fabric, y compris tous les APIC, tous les commutateurs Leaf et tous les commutateurs Spine. Une capture de paquets sur le serveur Syslog confirme si des paquets UDP 514 arrivent.

Scénario 8 : Les journaux d'autorisation/de refus ACL du contrat n'arrivent pas

Problème : Les journaux de paquets d'autorisation ou de refus de contrat (ACLLOG_PKTLOG_PERMIT / ACLLOG_PKTLOG_DENY) n'arrivent pas sur le serveur syslog.

Vérification de la configuration :

1. Vérifiez que le niveau de gravité de la source Syslog est information:
   <#root>

   ```
   apic1#

   moquery -c syslogSrc

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

2. Vérifiez que le niveau de gravité de la destination distante est information:
   <#root>

   ```
   apic1#

   moquery -c syslogRemoteDest

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

3. Vérifiez que la gravité du filtre de l'utilitaire Syslog Message Policy est 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. Vérifiez que la directive log est activée sur le filtre de contrat. Accédez à Locants > [tenant] > Contracts > [contract] > Subjects > [subject] > Filters et confirmez que la colonne Directives affiche le journal pour l'entrée de filtre appropriée.
5. Vérifiez que les journaux de liste de contrôle d’accès sont générés sur le commutateur Leaf (les journaux de liste de contrôle d’accès proviennent du Leaf et non du contrôleur APIC) :
   <#root>

```
leaf1#
show logging ip access-list internal packet-log deny
```

```
<#root>
leaf1#
cat /var/log/external/messages | grep ACLLOG | tail -20
```

Si aucune ACLLOG entrée n'apparaît, la directive log ne déclenche pas la génération de log sur le leaf. Cela peut indiquer une directive de contrat mal configurée, qu'aucun trafic correspondant n'atteint le contrat ou que la limitation de débit CoPP abandonne les paquets avant qu'ils ne soient consignés.

Cause première : Le niveau de gravité du journal de la liste de contrôle d'accès du contrat est informational (syslog niveau 6). Si un filtre de la chaîne syslog (source minSev, destination distante severityou filtre de l'utilitaire Syslog Message Policy (syslogFacilityFilterat uni/fabric/moncommon/sysmsgp/ff-syslog)) est défini ci-dessus information, les messages du journal de la liste de contrôle d'accès sont supprimés en silence avant de quitter le noeud de fabric.

Solution : Définissez minSev sur information sur la source syslog, définissez severity sur information sur la destination distante, définissez le filtre syslog facility minSev sur information sous Common Policy > Syslog Message Policies > default, confirmez que la directive Log est activée sur le filtre de contrat, et vérifiez que le pare-feu autorise le trafic syslog à partir des adresses IP OOB du commutateur leaf, et pas seulement les adresses IP APIC, car les journaux ACL sont envoyés à partir du commutateur.

Scénario 9 : Syslog s'arrête après avoir renommé le groupe de destinations

Problème : Les messages Syslog cessent d'arriver sur le serveur distant après la modification du nom du groupe de destination Syslog. La modification du port ou de l'installation n'entraîne pas ce problème. La désactivation et la réactivation de la stratégie ne reprennent pas la remise des messages.

Cause première : Il s'agit d'un défaut logiciel connu. Voir l'ID de bogue Cisco CSCwj23752. Renommer le groupe de destination brise l'association de transfert syslog interne. Elle est corrigée dans APIC version 6.0(6) et ultérieures.

Solution : Mise à niveau vers APIC version 6.0(6c) ou ultérieure. Pour contourner le problème des versions affectées, supprimez le groupe de destinations renommé et recréez-le avec le nom souhaité, puis réassociez les sources Syslog.

Scénario 10 : Syslog excessif entraînant la lenteur de l'interface graphique APIC

Problème : L'interface graphique du contrôleur APIC devient lente et l'utilisation du processeur APIC est élevée. Cela peut se produire lorsque la journalisation de la liste de contrôle d'accès du contrat est laissée activée pendant les opérations normales, générant un grand volume de messages syslog d'information qui sont convertis en objets dans la base de données APIC, eventRecord.

Cause première : Lorsque la gravité de la stratégie de messages Syslog de la stratégie Common Policy est définie sur information, chaque message syslog d'information, y compris les journaux de listes de contrôle d'accès volumineux, génère un message eventRecord dans le contrôleur APIC. Cela peut saturer la base de données APIC et ralentir l'interface utilisateur graphique.

Solution :

- Désactiver la journalisation des ACL de contrat pendant les opérations normales. Activez-la uniquement pendant les fenêtres de dépannage ou de maintenance.
- Si la journalisation de la liste de contrôle d'accès doit rester activée, définissez le niveau de gravité de la stratégie de messages Syslog sur alertsFabric > Stratégies de fabric > Stratégies > Surveillance > Stratégie commune > Stratégies de messages Syslog > par défaut. Ceci empêche les messages syslog d'information d'être convertis en événements, tout en permettant leur transfert vers le serveur syslog distant.
- Désactiver les codes d'événement bruyants qui ne sont pas utiles sur le plan opérationnel. Un code d'événement peut être désactivé pour l'empêcher de générer des enregistrements d'événements sans affecter le transfert Syslog.

Bogues connus

Les défauts logiciels connus suivants affectent la fonctionnalité syslog de l'ACI :

- ID de bogue Cisco CSCwj23752 — Renommer le groupe de destinations syslog arrête la livraison syslog. Correction dans APIC version 6.0(6c) et ultérieure.

Critères de remontée

Bénéficiez d'une assistance technique et contactez le TAC Cisco lorsque :

- Les messages Syslog apparaissent en /var/log/external/messages local sur les noeuds de fabric, les états du groupe de destinations et de l'administrateur de destination distante sont les deux

enabled, l'EPG de gestion est correct, l'accessibilité du réseau est confirmée (test ping et pare-feu réussi), mais les messages n'arrivent toujours pas au serveur distant.
- Les messages Syslog arrivent de certains noeuds de fabric, mais pas d'autres, sans différence de configuration entre eux, ce qui suggère une incohérence dans le déploiement des stratégies.
- Le profil de groupe de destinations ou la destination distante a été réactivé, mais les messages ne reprennent pas dans les minutes qui suivent la modification de la configuration.
- Les messages Syslog ont cessé d'arriver après une mise à niveau APIC, suggérant un défaut logiciel potentiel.

Données à collecter avant d'ouvrir un dossier TAC :

- Assistance technique à la demande du contrôleur APIC affecté et d'un noeud leaf affecté.
- Sortie de moquery -c syslogGroup, moquery -c syslogProf, moquery -c syslogRemoteDest, et moquery -c syslogSrc du contrôleur APIC.
- Résultat de la commande moquery -d uni/fabric/moncommon/systemslsrc/rssystemDestGroup permettant de vérifier le lien Politique commune.
- Queue d'/var/log/external/messagesun APIC et d'une feuille affectée.
- Capture de paquets à partir du serveur syslog confirmant si les paquets UDP/TCP 514 arrivent des adresses OOB de fabric.

Références

- Cisco APIC Basic Configuration Guide, version 6.1(x) — Gestion
- Guide de référence des messages système Cisco ACI
- Guide de gestion des défaillances, événements et messages système de l'ACI Cisco
- Livre blanc du guide des contrats Cisco ACI
- Dépannage d'une interface graphique APIC lente

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.