ACIでのsyslogの設定およびトラブルシューティング

はじめに

このドキュメントでは、シスコアプリケーションセントリックインフラストラクチャ(ACI)のシステムロギング(syslog)を設定、確認、およびトラブルシューティングする方法について説明します。 完全な設定ワークフロー、Application Policy Infrastructure Controller(APIC)マネージドオブジェクト(MO)モデルを使用したプログラムによる検証、およびAPICコントローラとリーフスイッチおよびスパインスイッチの両方に関する構造化されたトラブルシューティングワークフローについて説明します。

概要

ACI syslogは完全にポリシー駆動型です。スタンドアロンCisco NX-OS®ソフトウェアとは異なり、ACIリーフ/スパイン型スイッチには**logging server** CLIコマンドはありません。すべてのsyslog設定は、APICがすべてのファブリックノードに自動的にプッシュするAPICポリシーを通じて行われます。

主なコンポーネント

ACIのsyslogサブシステムは、次の管理対象オブジェクトから構築されます。

- Syslog Destination Group(syslogGroup)：すべてのsyslog宛先の最上位のコンテナ。メッセージフォーマット（ACIまたはNX-OSスタイル）とタイムスタンプオプションを制御します。これには、1つ以上のリモート接続先、ローカルファイルの接続先、およびコンソールの接続先を含めることができます。
- syslogプロファイル(syslogProf)：宛先グループの子であり、グループレベルの管理状態とトランスポートプロトコル（UDP、TCP、またはSSL）を制御します。
- Syslog Remote Destination(syslogRemoteDest)：リモートsyslogサーバを表す宛先グループの子。サーバに到達するために使用されるサーバIPまたはホスト名、ポート、重大度フィルタ、syslogファシリティ、および管理エンドポイントグループ(EPG)を制御します。
- syslogローカルファイル(syslogFile)：各ファブリックノードのローカルファイル /var/log/external/messagesへのsyslogメッセージの書き込みを制御する宛先グループの子。
- syslog Source(syslogSrc)：モニタリングポリシーに添付されます。送信するメッセージタイプ（監査、イベント、障害、セッション）と最小重大度を制御し、syslogRsDestGroup関係を介して宛先グループにリンクします。

Syslogソースの添付ポイント

ACIは、syslogメッセージを生成するノードとオブジェクトを制御する4つのモニタリングポリシースコープを使用します。

- Common Monitoring Policy(monCommonPol、uni/fabric/moncommon)：ファブリック全体の範囲。すべての障害とイベントに適用され、ファブリック内のすべてのノード（リーフスイッチとスパインスイッチ）とすべてのコントローラ(APIC)に自動的に導入される基本的なモニタリングポリシー。すべてのファブリック、アクセス、およびテナント階層をカバーこれは、Fabric > Fabric Policies > Policies > Monitoring > Common Policyの順に選択すると表示されます。
- Fabric Monitoring Policy(monInfraPol、uni/infra/moninfra-default)：ファブリックスコープ。ファブリックレベルのオブジェクト（ファブリックポート、カード、シャーシコンポーネント、ファントレイ）のsyslogを生成します。これは、Fabric > Fabric Policies > Policies > Monitoring > defaultの順に選択すると表示されます。
- Access Monitoring Policy(monFabricPol, uni/fabric/monfab-default)：アクセス（インフラストラクチャ）スコープ。アクセスポート、ファブリックエクステンダ(FEX)デバイス、仮想マシン(VM)コントローライベントなど、アクセスに面したコンポーネントのsyslogを生成します。これは、Fabric > Access Policies > Policies > Monitoring Policies > defaultの順に選択すると表示されます。
- テナントモニタリングポリシー(monEPGPol、uni/tn-common/monepg-default)：テナントスコープ。テナントスコープのオブジェクト(エンドポイントグループ(EPG)、アプリケーションプロファイル、およびサービス)のsyslogを生成します。[Tenant] > Monitoring Policies > defaultの順に選択すると、各テナントの下にあります。

注:Common Monitoring Policyは、すべての階層にわたってファブリック全体のカバレッジを提供し、すべてのノードに自動的に展開されるため、syslog設定の開始点として推奨されます。特定のオブジェクト階層に対するより詳細な制御を行うにはCommon Policyに加えて、ファブリックおよびアクセスモニタリングポリシーを設定できます。または、Common Policyの代わりに、より狭い範囲にsyslogを制限することもできます。

Syslogメッセージの形式

グループ形式がaci（デフォルト）に設定されている場合、ACI syslogメッセージはRFC 3164形式に従います。

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

例：

```
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
```

メッセージ本文には、ACIエラーコード、該当オブジェクトのライフサイクル状態(例：浸す、保持する、クリアするなど)、重大度、および識別名(DN)が含まれ、メッセージは自己記述形式になります。

次の3つのメッセージ形式オプションを使用できます。

- aci（デフォルト）:RFC 3164準拠の形式。ほとんどの導入に推奨されます。
- nxos:NX-OS形式。syslogプラットフォームがNX-OS形式のメッセージを想定している場合は、これを使用します。
- 拡張ログ(APIC 5.2(8)以降)：年を含む拡張タイムスタンプ付きのRFC 5424準拠フォーマット。

重大度のマッピング

syslog重大度フィールドは、0（最も重大）から7（最も重大）までの1桁の数字です。 次の表に、syslog重大度レベルとACI/International Telecommunication Union（ITU；国際電気通信連合）の重大度の用語とのマッピングを示します。

Syslogの重大度	ACI/ITUレベル	説明
0：緊急	—	システムが使用できない
1：アラート	Critical	即時対応が必要
2：重大	メジャー	重大な状態
3：エラー	マイナー	エラー状態
4：警告	warning	警告状態
5：通知	不確定/クリア	正常だが重要な状態
6：情報	—	情報メッセージのみ
7：デバッグ	—	デバッグ出力のみ

転送オプション

ACIでは、リモートsyslog用に次の3つの転送プロトコルがサポートされています。

- UDP（デフォルト）：すべてのAPICリリースで使用できます。標準的な完全自動配送。
- TCP:APICリリース5.2(3)以降で使用できます。コネクション型の転送により、信頼性の高い配信を実現します。
- SSL:APICリリース5.2(4)以降で使用できます。TLSを使用して暗号化された転送を提供します。各ACIノード（APICまたはスイッチ）はTLSクライアントとして機能し、syslogサーバへのアウトバウンド接続を開始します。Admin > AAA > Security > Public Key Management

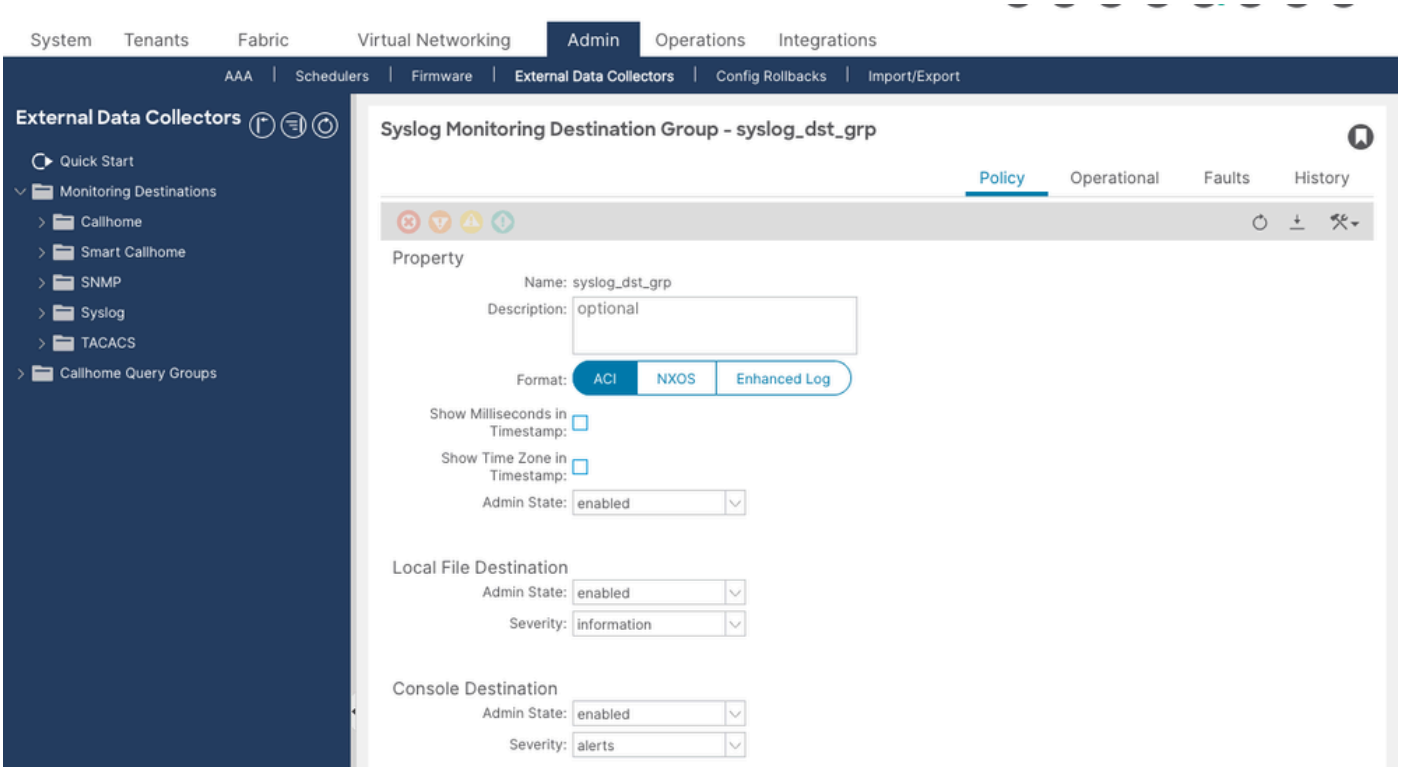
> Certificate Authoritiesの順に選択し、サーバ証明書をAPICにアップロードする必要があります。

注：リモート接続先でSSLトランスポートが設定されている場合、APICをSSLをサポートしないリリースにダウングレードすると、トランスポートプロトコルは自動的にUDPに戻ります。syslogサーバがフォールバックとしてUDP接続も受け入れることができることを確認します。

コンフィギュレーション

次の手順では、エンドツーエンドでACI syslogを設定します。APICコントローラとリーフスイッチおよびスパインスイッチの両方からsyslog転送を有効にするには、すべての手順を実行します。

ステップ1:syslog宛先グループの作成



宛先グループは、syslogメッセージの送信先および形式を定義します。このグループを最初に作成します。これは、後の手順で設定するsyslogソースがこのグループを名前で参照するためです。

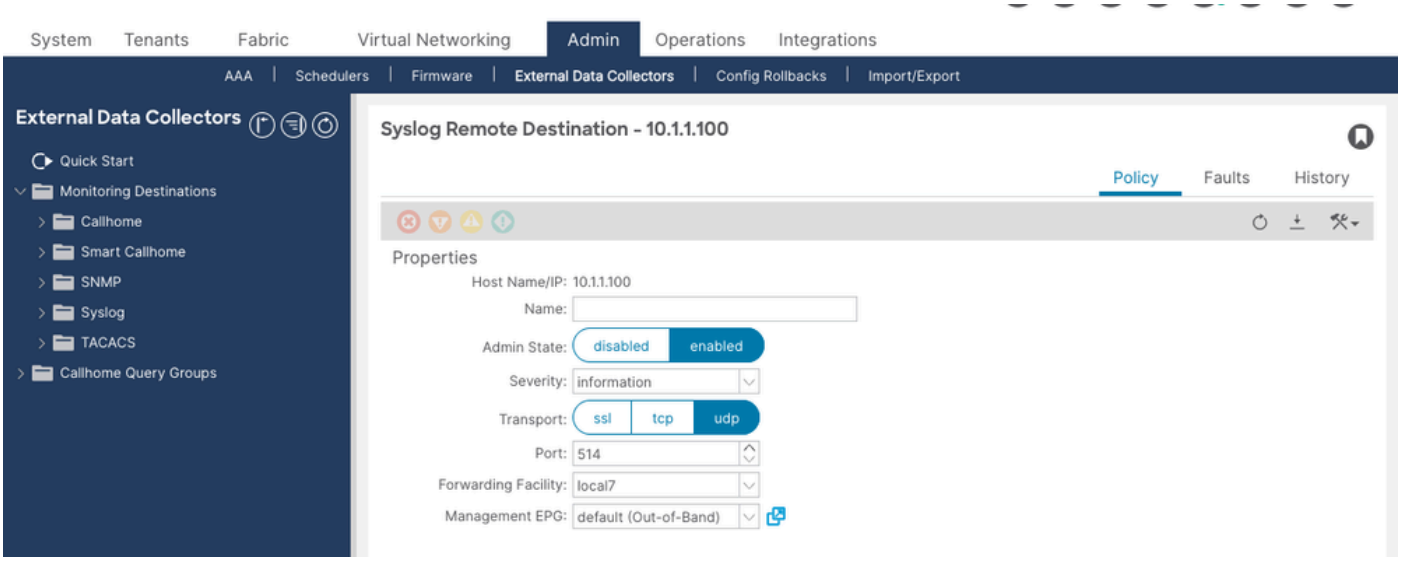
Admin > External Data Collectors > Monitoring Destinations > Syslogの順に移動します。Syslogを右クリックし、Create Syslog Monitoring Destination Groupを選択します。

ウィザードの最初のページ（グループプロファイル）で、次のように設定します。

- Name：わかりやすい名前(Syslog-Dest-Groupなど)。
- 形式:aci（デフォルト、RFC 3164互換）またはnxos。
- Admin State:enabled。
- ローカルファイルの宛先の管理状態:enabled（推奨）。 これは、すべてのファブリックノードの/var/log/external/messagesにメッセージを書き込むので、リモートサーバに到達できない場合でも、ローカルのトラブルシューティングに不可欠です。
- ローカルファイルの宛先の重大度:情報。
- Console Destination Admin State:disabled（実稼働環境に推奨）。

[Next] をクリックします。2ページ目のCreate Remote Destinations領域で+をクリックし、リモートsyslogサーバを追加します。

ステップ2：リモート接続先の追加



Create Syslog Remote Destinationダイアログでリモートsyslogサーバを設定します。

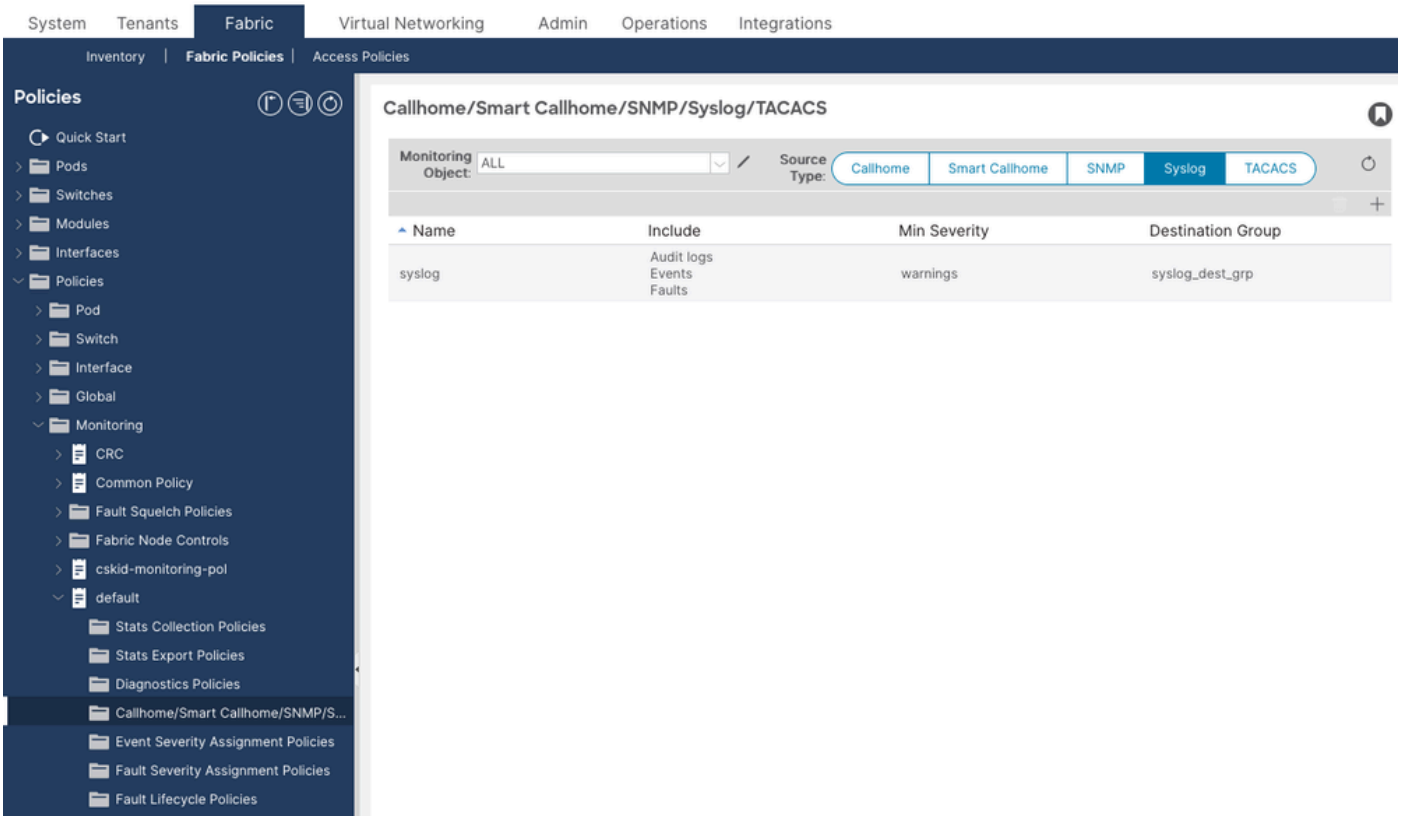
- Host:syslogサーバのIPアドレス。ホスト名ではなくIPアドレスを使用してください。ホスト名を使用する場合は、ドメインネームシステム(DNS)サーバがアウトオブバンド(OOB)管理インターフェイス経由で到達可能であることを確認する必要があります。インバンド接続を介してのみ到達可能なDNSサーバは、ネットワークの停止中にsyslogメッセージが生成されると、解決に失敗する可能性があります。
- Admin State:enabled。
- 重大度:情報（推奨）。 これは、この特定のリモートサーバに送信される最小限の重大度です。
- Port:514（デフォルト）。
- Facility:local7（デフォルト）。 これを、syslogサーバが受け入れてルーティングするように

設定されているファシリティ値と一致するように設定します。
- Transport:udp（デフォルト）。 信頼性の高い配信(APIC 5.2(3)以降が必要)にはtcpを、暗号化された転送(APIC 5.2(4)以降とAPICにアップロードされた証明書が必要)にはsslを使用します。
- Management EPG:syslogサーバに到達可能な管理EPGを選択します。OOB管理：uni/tn-mgmt/mgmtp-default/oob-default。インバンド管理の場合は、適切なインバンドEPGを選択します。このフィールドを空にすることはできません。

OKをクリックし、次にFinishをクリックします。

注：同じ宛先グループに複数のリモート宛先を追加できます。各宛先には、異なる重大度しきい値、ファシリティ、およびトランスポートプロトコルを設定できます。

ステップ3：ファブリックモニタリングポリシーでのSyslogソースの作成



この手順では、ファブリックオブジェクト階層（ファブリックポート、カード、シャーシコンポーネント、ファントレイ）のsyslogを設定します。これにより、階層固有の制御で共通モニタリングポリシー（ステップ4）が補完されます。

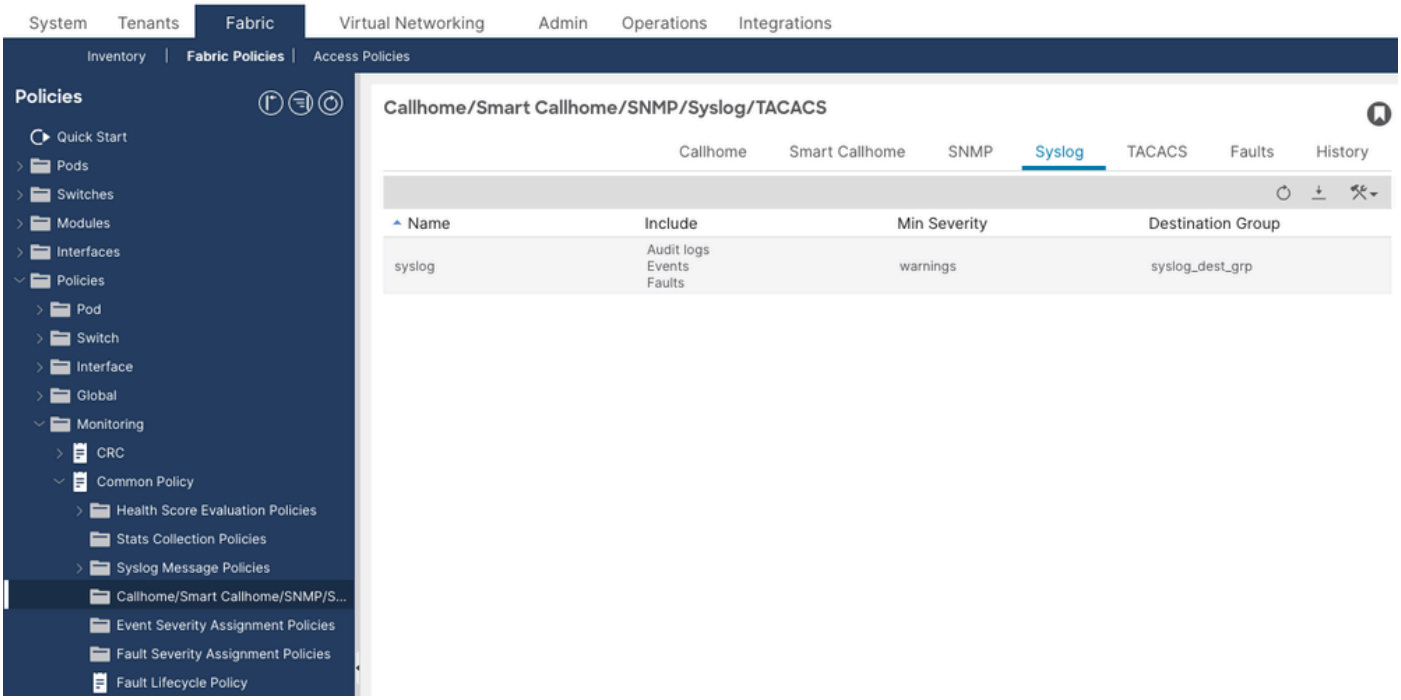
Fabric > Fabric Policies > Policies > Monitoring > default > Callhome/Smart Callhome/SNMP/Syslog/TACACSの順に移動します。

右側のペインで、Source TypeをSyslogに設定します。+をクリックして、syslogソースを作成します。

- Name：わかりやすい名前(Syslog-Source-Fabricなど)。
- Min Severity:情報（完全なカバレッジに推奨）。
- Include:audit、events、およびfaultsをチェックします。オプションで、ログインイベントとログアウトイベントにsessionを追加します。
- 宛先グループ：ステップ1で作成した宛先グループを選択します。

[Submit] をクリックします。

ステップ4：共通モニタリングポリシーの設定（システム全体のSyslog）

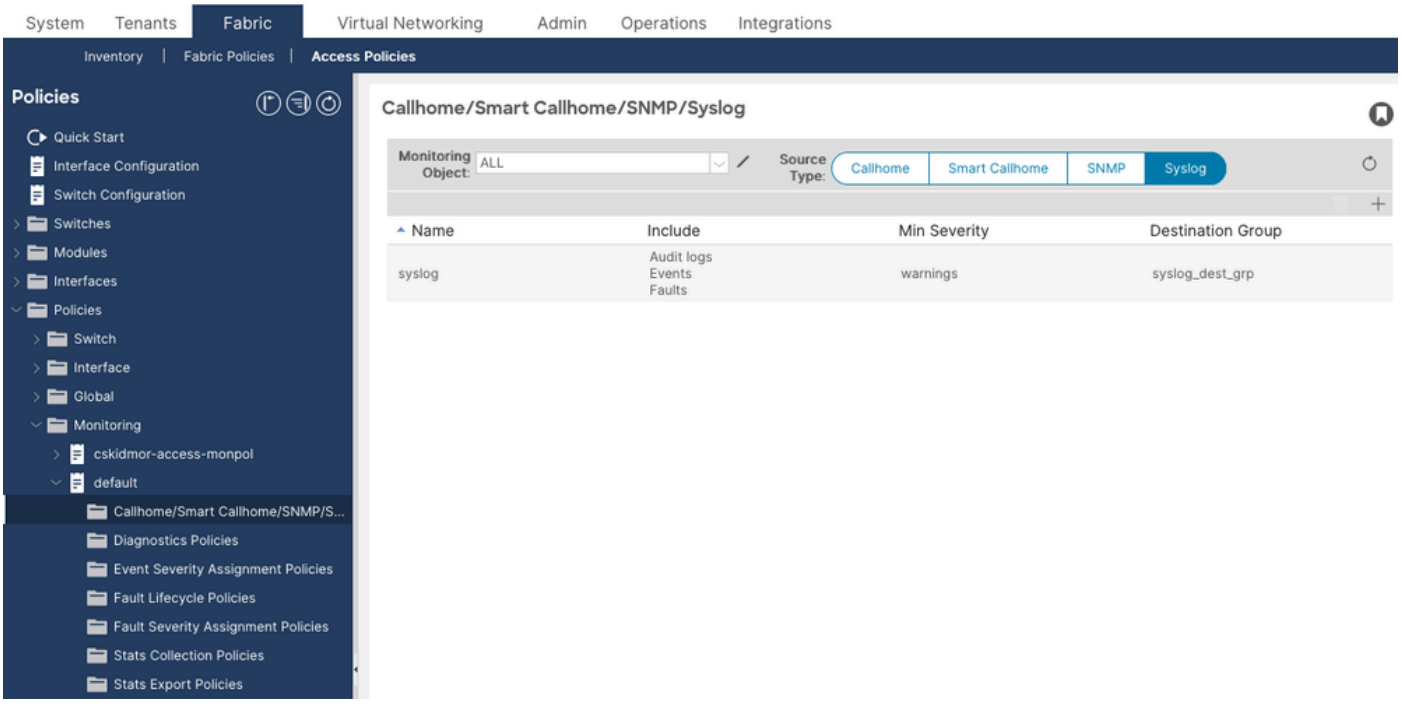


共通モニタリングポリシーは、システム全体のsyslogカバレッジを提供します。これは、ファブリック内のすべてのノードとコントローラに自動的に導入されます。この手順では、システムのsyslog送信元を宛先グループにリンクします。

Fabric > Fabric Policies > Policies > Monitoring > Common Policyの順に移動します。Syslogセクションで、システムのsyslog送信元を、ステップ1で作成した宛先グループにリンクします。

Common Policyシステムのsyslogソースでは、DN uni/fabric/moncommon/systemslsrc/rssystemDestGroupのMO syslogRsSystemDestGroupを使用します。

ステップ5：アクセスモニタリングポリシーでのsyslogソースの作成



この手順では、アクセスオブジェクト階層(アクセスポート、ファブリックエクステンダ(FEX)デバイス、および仮想マシン(VM)コントローライベント)のsyslogを設定します。これにより、階層固有の制御で共通モニタリングポリシー（ステップ4）が補完されます。

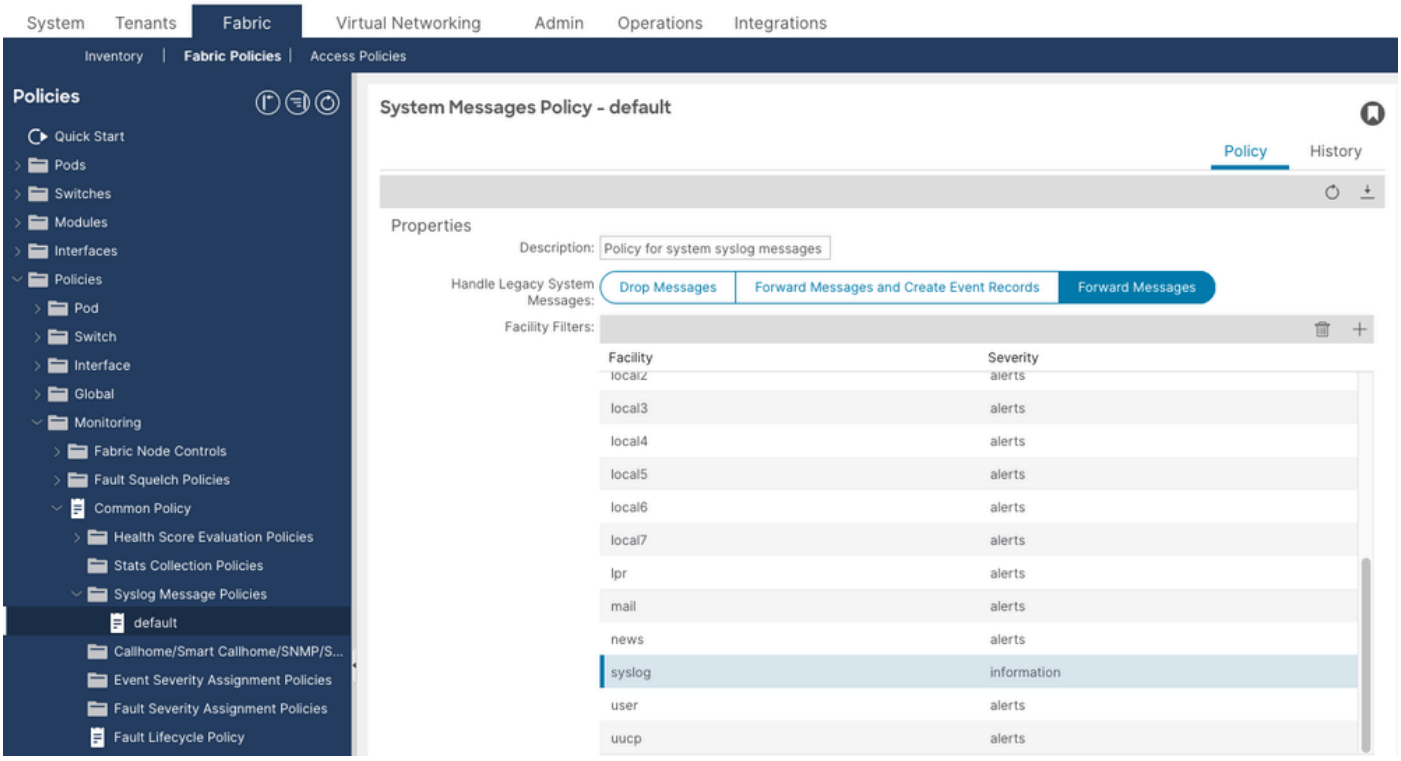
Fabric > Access Policies > Policies > Monitoring Policies > default > Callhome/SNMP/Syslogの順に移動します。

Source TypeをSyslogに設定します。+をクリックして、ステップ3と同じ設定を行います。

- Name：例：Syslog-Source-Access。
- Min Severity:情報。
- Include:audit、events、およびfaultsをチェックします。
- 宛先グループ：同じ宛先グループを選択します。

[Submit] をクリックします。

ステップ6（オプション）：コントラクトACLロギングのsyslogメッセージポリシーを調整します



コントラクトACLの許可または拒否パケットログ(ACLLOG_PKTLOG_PERMIT/ACLLOG_PKTLOG_DENY)をリモートsyslogサーバに表示する必要がある場合は、syslogメッセージファシリティフィルタを情報の重大度に設定する必要があります。

Fabric > Fabric Policies > Policies > Monitoring > Common Policy > Syslog Message Policies > defaultの順に移動します。ファシリティフィルタリストで、syslogファシリティを選択し、最小重大度を情報に設定します。これはDN uni/fabric/moncommon/sysmsgp/ff-syslogのsyslogFacilityFilter MOです。

注：コントラクトACLの許可ログと拒否ログがリモートsyslogサーバに到達するには、次の4つの条件をすべて満たす必要があります。(1)syslog送信元のminSevが情報である、(2)リモート宛先の重大度が情報である、(3)syslogメッセージポリシーのsyslogファシリティフィルタminSevが情報である、(4)コントラクトのフィルタエントリでLogディレクティブがである必要です。3つの条件がすべて満たされると、ACLログメッセージは（APICからではなく）リーフスイッチから発信されるため、メッセージは最初にリーフの/var/log/external/messagesに表示されます。コントラクトACLパケットログレートは、CoPPによって制限されます。拒否ログのデフォルトは500 pps（パケット/秒）で、許可ログのデフォルトは300 pps（リーフあたり）です。

注：管理コントラクトのフィルタでLogディレクティブを使用することはサポートされておらず、これによりゾーン分割ルールの展開が失敗します。テナントデータプレーンコントラクトだけにコントラクトロギングを適用します。

設定の検証

運用上の問題のトラブルシューティングを行う前に、設定を確認します。syslogメッセージが表示されない根本的な原因として最も一般的なのは、ネットワークやソフトウェアの障害ではなく、設定の誤りです。

宛先グループとプロファイルの確認

APICで**moquery -c syslogGroup**を実行し、宛先グループが存在することを確認して、それらの属性をチェックします。

<#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
```

次に**moquery -c syslogProf**を使用して、プロファイル（グループレベルの管理状態）を確認します。

<#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
```

プロファイルが無効になっている宛先グループを検索するには、次のコマンドを実行します。

<#root>

```
apic1#
```

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

この結果、宛先グループは、リモートの宛先管理ステートに関係なく、syslogトラフィックを転送しません。

リモート接続先の確認

moquery -c syslogRemoteDestを実行して、各リモートサーバの設定を確認します。

<#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
```

次の3つの属性には特別な注意が必要です。

- adminState:enabledである必要があります。無効にした場合、この特定のリモートサーバーは何も受信しません。
- epgDn：空にすることはできません。epgDnが空の場合、ファブリックではsyslogトラフィックの送信元のインターフェイスが認識されないため、ファブリックからメッセージが発信されることはありません。
- operState: unknown：この値は予期されたものであり、問題を示すものではありません。ACIは、syslogサーバの到達可能性をアクティブにプローブしません。

syslogソースの確認

moquery -c syslogSrcを実行して、送信元が正しいモニタリングポリシーの下に存在することを確認します。

<#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
```

ソースが適切なモニタリングポリシーの下に存在することを確認します。

- uni/fabric/moncommonの下のソース：すべてのノードとすべてのオブジェクト階層をファブリック全体でカバーする共通のモニタリングポリシー。
- uni/infra/moninfra-defaultの下のソース：ファブリックレベルのオブジェクト（ファブリックポート、カード、シャーシ）のファブリックモニタリングポリシー。
- uni/fabric/monfab-defaultの下の送信元（アクセスポート、FEX、VMコントローラ）アクセスレベルオブジェクト（アクセスポート、FEX、VMコントローラ）のアクセスモニタリングポリシー。

また、Common Monitoring Policyシステムのsyslogソースがリンクされていることを確認します。

<#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
```

コントラクトACLロギングが必要な場合は、**moquery -d uni/fabric/moncommon/sysmsgp/ff-syslog**を使用してsyslogメッセージポリシーファシリティフィルタの重大度を確認します。

<#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
```

ローカルログファイルの確認

/var/log/external/messagesのローカルファイルを参照するのが、リモートサーバに到達できない場合であっても、syslogメッセージがすべてのファブリックノードで生成されていることを確認する最も直接的な方法です。APICとリーフスイッチの両方で確認します。

<#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
```

このファイルが空の場合、またはノード上で更新されない場合、メッセージはソースで生成されません。ファイルに内容が含まれていても、リモートsyslogサーバがメッセージを受信していない場合、問題はメッセージの生成ではなく、転送（宛先グループ、ネットワーク、またはファイアウォール）にあります。

Syslogサーバへの到達可能性の確認

APICからsyslogサーバにpingを実行して、管理ネットワーク上のIP到達可能性を確認します。

<#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

リーフ/スパインスイッチから、ipingコマンドで-Vフラグを指定してVRFを指定します。syslogの宛先に割り当てられている管理EPGに応じて、アウトオブバンドにはmanagementを、インバンドにはmgmt:inbを使用します。

<#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

pingが成功するとIP到達可能性は確認されますが、UDPまたはTCPポート514が許可されているかどうかは確認されません。インターネット制御メッセージプロトコル(ICMP)とsyslogは、異なるプロトコルを使用します。

トラブルシューティング

トリアージワークフロー

syslogメッセージがリモートサーバに届かない場合は、次のDecision Treeを使用します。

```
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
```

一般的なシナリオ

シナリオ1：リモートサーバでsyslogメッセージを受信しない

問題： syslog宛先グループとリモート宛先が設定されていますが、メッセージがリモートサーバ

に到着しません。APICおよびスイッチのローカルファイル/var/log/external/messagesには、最近のエントリが含まれています。

設定チェック：

<#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：リモート接続先の管理状態が無効になっています。これは、宛先が作成されたにもかかわらず誤って無効のままになっている場合、またはメンテナンス中に無効にされ、再度有効にされなかった場合に発生する可能性があります。

解決策：Admin > External Data Collectors > Monitoring Destinations > Syslog > [group name] > Remote Destinations > [server]の順に移動します。リモート接続先を編集し、Admin Stateをenabledに設定します。

シナリオ2:Syslog宛先グループプロファイルが無効である

問題：リモート接続先のAdmin状態が有効な場合でも、どのノードからもメッセージが転送されません。

設定チェック：

<#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：宛先グループ全体がsyslogProf admin stateによって制御されます。無効にすると、個々のリモート接続先の状態に関係なく、どのノードからもメッセージが転送されなくなります。

解決策：Admin > External Data Collectors > Monitoring Destinations > Syslog > [group name]の順に移動します。プロファイルを編集し、Admin Stateをenabledに設定します。

シナリオ3：イベントが見つからない – 共通のモニタリングポリシーがリンクされていない

問題：syslogソースがファブリックまたはアクセスモニタリングポリシーの下で設定されていても、一部のノードまたはオブジェクト階層からのsyslogメッセージがリモートサーバに到達していない。

設定チェック：

<#root>

apic1#

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

Total Objects shown: 0

Common Monitoring Policy(CMO)システムのsyslogソースが宛先グループにリンクされていない。

根本原因：共通監視ポリシー(uni/fabric/moncommon)は、すべての階層にファブリック全体のsyslogカバレッジを提供し、すべてのノードとコントローラに自動的に導入されます。このコマンドを使用しない場合、特定のファブリックまたはアクセスモニタリングポリシー階層に一致するイベントのみが転送されます。ファブリックモニタリングポリシー(uni/infra/moninfra-default)はファブリックレベルのオブジェクトを対象とし、アクセスモニタリングポリシー(uni/fabric/monfab-default)はアクセスレベルのオブジェクトを対象としますが、どちらも共通ポリシーが提供するファブリック全体のカバレッジを提供しません。

解決策：Fabric > Fabric Policies > Policies > Monitoring > Common Policyの順に移動します。Syslogセクションで、システムのsyslog送信元を宛先グループにリンクします。**moquery -d uni/fabric/moncommon/systemslsrc/rssystemDestGroup**を使用して、tDnが宛先グループを指していることを確認します。

シナリオ4：重大度が制限しすぎている – 想定されるメッセージが欠落している

問題：一部のメッセージがsyslogサーバに到着したが、情報イベント、監査ログエントリ、またはセッションログインイベントが欠落している。重大な障害と重大な障害のみが表示されます。

設定チェック：

<#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： Syslogフィルタリングは、送信元(minSev)とリモート宛先(重大度)の2つのポイントで発生します。 両方のフィルタを通過するメッセージだけが転送されます。どちらかのパラメータが上記の情報に設定されると、情報メッセージはドロップされます。

解決方法： syslogソースを編集し、Min Severityをinformationに設定して、Includeフィールドのaudit、events、faultsにチェックマークを入れます。リモート接続先を編集し、重大度を情報に設定します。

シナリオ5：リモート接続先に管理EPGが割り当てられていない

問題：リモートサーバでsyslogメッセージが受信されない。宛先グループが有効で、リモート宛先が有効で、ローカルログファイルに内容があります。

設定チェック：

<#root>

```
apic1#

moquery -c syslogRemoteDest

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

根本原因：管理EPGがないと、APICとスイッチはsyslogメッセージの送信に使用する物理インターフェイスを認識できません。メッセージは生成されるが、転送できない。

解決策：リモート接続先を編集し、適切な管理EPGを選択します。OOB管理には、uni/tn-mgmt/mgmtp-default/oob-defaultを選択します。インバンド管理の場合は、適切なインバンドEPGを選択します。

シナリオ6：誤った管理EPG（インバンドとアウトオブバンド）

問題：syslogメッセージが断続的に、または一部のノードからのみ到着する。syslogサーバにはOOB管理を介してのみ到達できますが、リモートの宛先はインバンドEPGを参照します。

設定チェック：

<#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
```

syslogサーバがOOBネットワーク経由でのみ到達可能な場合、インバンドEPGではメッセージの送信元がインバンドインターフェイスであるため、サーバに到達できません。

解決策：リモート接続先を編集し、管理EPGをuni/tn-mgmt/mgmtp-default/oob-defaultに変更します。APIC bashから**ping -c 3 10.1.1.100**を実行してOOB到達可能性を確認します。

シナリオ7：ファイアウォールがSyslogトラフィックをブロックしている

問題：ローカルログファイルには、APICとリーフノードの両方の内容が含まれています。設定は正しく、syslogサーバへのICMP pingは成功しますが、メッセージはサーバに到達しません。

動作確認：APICからsyslogサーバにpingを実行して、IP到達可能性を確認します。

<#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は成功するが、syslogメッセージが届かない。ICMP(ping)は通過するが、UDPポート514はブロックされる。

根本原因：管理ネットワークとsyslogサーバの間のファイアウォールまたはACLが、UDPポート514（TCPトランスポートが設定されている場合はTCP 514）をブロックしています。 ICMPとUDPは独立しています。ICMPを渡しても、UDP 514が許可されているかどうかの確認は行われません。さらに、各リーフおよびスパインは、自身のOOB IPアドレスから直接syslogを送信します。APIC OOB IPだけを許可するファイアウォールは、スイッチノードから発信されたsyslogパケットをドロップします。

解決策：すべてのAPIC、すべてのリーフスイッチ、およびすべてのスパインスイッチを含む、すべてのファブリックノードのOOB IPアドレス範囲からのUDP/TCPポート514がファイアウォールで許可されていることを確認します。syslogサーバのパケットキャプチャにより、UDP 514パケットが到着しているかどうかが確認されます。

シナリオ8：契約ACLの許可/拒否ログが到達しない

問題：コントラクトの許可または拒否パケットログ(ACLLOG_PKTLOG_PERMIT / ACLLOG_PKTLOG_DENY)がsyslogサーバに到達していない。

設定チェック：

1. syslogソースの重大度が情報であることを確認します。
   <#root>

   apic1#

```
moquery -c syslogSrc

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

2. リモート接続先の重大度がinformationであることを確認します。
   <#root>

```
apic1#

moquery -c syslogRemoteDest

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

3. syslogメッセージポリシーファシリティフィルタの重大度が情報であることを確認します。
   <#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. 契約フィルタでlogディレクティブが有効になっていることを確認します。Tenants > [tenant] > Contracts > [contract] > Subject > [subject] > Filtersの順に移動し、Directives列に該当するフィルタエントリのlogが表示されていることを確認します。
5. ACLログがリーフスイッチで生成されていることを確認します（ACLログは、APICからではなく、リーフから生成されます）。
   <#root>

```
leaf1#

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

   <#root>

```
leaf1#

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

   ACLLOGエントリが表示されない場合、logディレクティブはリーフでのログ生成をトリガーしていません。これは、contractディレクティブの設定が誤っているか、一致するトラフィックがコントラクトにヒットしていないか、CoPPレート制限によってパケットがログに記録される前にドロップされていることを示しています。

根本原因：契約ACLログの重大度レベルは情報です（syslogレベル6）。 syslogチェーン(送信元minSev、リモート宛先severity、またはSyslogメッセージポリシーファシリティフィルタ

(uni/fabric/moncommon/sysmsgp/ff-syslogでのsyslogFacilityFilter))内のいずれかのフィルタがinformationよりも上に設定されている場合、ACLログメッセージは、ファブリックノードから出る前に、通知されることなく廃棄されます。

解決方法：minSevをsyslog送信元の情報に、重大度をリモート宛先の情報に設定し、syslog facility filter minSevをinformation under Common Policy > Syslog Message Policies > defaultに設定し、コントラクトフィルタでLogディレクティブが有効になっていることを確認し、ファイアウォールがAPIC IPだけでなく、リーフスイッチOOB IPアドレスからのsyslogトラフィックを許可することを確認します。

シナリオ9：宛先グループの名前を変更した後にSyslogが停止する

問題： syslog宛先グループの名前を変更すると、syslogメッセージがリモートサーバに届かなくなります。ポートまたはファシリティを変更してもこの問題は発生しません。ポリシーを無効にしてから再度有効にしても、メッセージの配信は再開されません。

根本原因：これは既知のソフトウェア不具合です。Cisco Bug ID CSCwj23752を参照してください。宛先グループの名前を変更すると、内部syslog転送の関連付けが解除されます。この問題は、APICリリース6.0(6)以降で修正されています。

解決策：APICリリース6.0(6c)以降にアップグレードします。影響を受けるバージョンでの回避策としては、名前を変更した宛先グループを削除し、目的の名前で再作成してから、syslogソースを再度関連付けます。

シナリオ10：過剰なSyslogが原因でAPIC GUIの速度が低下する

問題：APIC GUIが低速になり、APIC CPU使用率が高くなる。これは、コントラクトACLロギングが通常の動作中に有効なままになっていると発生し、大量の情報syslogメッセージが生成されて、APICデータベースのeventRecordオブジェクトに変換されます。

根本原因：共通ポリシーのsyslogメッセージポリシーの重大度がinformationに設定されている場合、大量のACLログを含むすべての情報syslogメッセージでAPICにeventRecordが生成されます。これにより、APICデータベースに過大な負荷がかかり、GUIの速度が低下する可能性があります。

ソリューション：

- 通常の動作中は、コントラクトACLロギングを無効にします。トラブルシューティングまたはメンテナンスの時間帯にのみ有効にします。
- ACLロギングを有効にしておく必要がある場合は、Fabric > Fabric Policies > Policies > Monitoring > Common Policy > Syslog Message Policies > defaultの順に選択し、Syslogメッセージポリシーの重大度をalertsに設定します。これにより、情報syslogメッセージがイベントに変換されるのを防ぎな

がら、リモートsyslogサーバへの転送を許可できます。
- 動作上役に立たないノイズの多いイベントコードをスケルチします。イベントコードをスケルチして、syslog転送に影響を与えずにイベントレコードが生成されないようにすることができます。

既知のバグ

次の既知のソフトウェア不具合がACI syslog機能に影響を与えます。

- Cisco Bug ID CSCwj23752:syslog宛先グループの名前を変更すると、syslog配信が停止します。APICリリース6.0(6c)以降で修正されています。

エスカレーション基準

次の場合には、テクニカルサポートを収集して、Cisco TACに連絡してください。

- syslogメッセージは/var/log/external/messagesにファブリックノードでローカルに表示され、宛先グループとリモート接続先のadmin状態はどちらもenabledになっています。管理EPGは正しく、ネットワーク到達可能性は確認されていますが（pingとfirewall check pass）、メッセージはまだリモートサーバに到達していません。
- syslogメッセージは一部のファブリックノードから到着しますが、他のファブリックノードからは到着しません。これらのファブリックノード間の設定には違いがないため、ポリシー導入の不整合が示唆されます。
- 宛先グループのプロファイルまたはリモートの宛先が再度有効にされましたが、設定変更から数分以内にメッセージが再開されません。
- APICのアップグレード後にsyslogメッセージの到着が停止した場合、ソフトウェアに不具合がある可能性があります。

TACケースをオープンする前に収集するデータ：

- 該当するAPICと該当するリーフノード1つからのオンデマンドtechsupport。
- APICからのmoquery -c syslogGroup、 moquery -c syslogProf、 moquery -c syslogRemoteDest、 moquery -c syslogSrcの出力。
- 共通ポリシーリンクを確認するためのmoquery -d uni/fabric/moncommon/systemslsrc/rssystemDestGroupの出力。
- APICと影響を受けるリーフの両方からの/var/log/external/messagesのテール。
- Syslogサーバからのパケットキャプチャにより、UDP/TCP 514パケットがファブリックOOBアドレスから到着しているかどうかが確認されます。

参照資料

- Cisco APIC基本設定ガイド、リリース6.1(x)：管理
- Cisco ACIシステムメッセージリファレンスガイド
- Cisco ACI障害、イベント、およびシステムメッセージ管理ガイド
- Cisco ACI契約ガイドのホワイトペーパー
- 低速のAPIC GUIのトラブルシューティング

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。