

CISCO APPLICATION CENTRIC INFRASTRUCTURE

BuzzfeedNEWS



SYSLOG Configuration by Tomas de Leon

Table of Contents

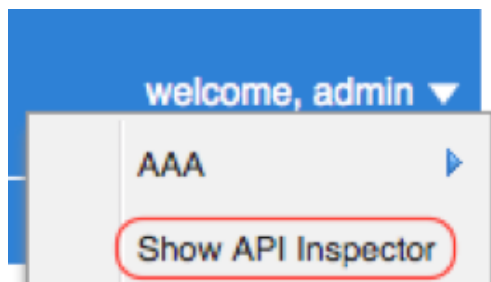
Introduction	3
Configure Syslog Policy for the ACI Fabric	4
Troubleshooting Syslog Policy for the ACI Fabric	15
Reference Material	28

Introduction

The **ACI BuzzfeedNEWS** Technote will introduce you to configuring SYSLOG Services for Controllers and Leaf/Spine Switches in the ACI fabric. The Cisco ACI system sends system log (syslog) messages to the console (and, optionally, to a logging server on another system) during operation. Not all system messages indicate problems with your system. Some messages are purely informational, while others may help diagnose problems with communications lines, internal hardware, or the system software.

The following examples will use the "syslog" utility to gather information about your Cisco ACI fabric system. This Technote will show examples of configuring syslog utilizing the APIC Admin GUI and REST API (using POSTMAN).

In regards to the REST API examples listed in this Technote, there is an assumption made that you have a REST CLIENT (like POSTMAN) installed on your workstation. POSTMAN can be used for executing REST API requests to an APIC Controller. Also, while executing listed configuration tasks, you may want to open the API inspector console from the APIC GUI. The API inspector displays the API POST requests used for the tasks performed. The Post Requests in the API inspector can be used for sending requests to APIC controllers.



For this Technote, an application server that is running a Syslog utility application. The KIWI Syslog Server is installed so that the Cisco ACI Fabric system can send syslog messages to.



KIWI SYSLOG WEB ACCESS

KIWI Syslog Server

Version 9.4.1

<http://www.kiwisyslog.com/downloads.aspx>

Note: This Technote example will show you how to config the Cisco APIC for syslog external data collectors. For more information on this feature, please refer to the "Cisco ACI System Messages Reference Guide".

For this Technote example, refer to the following information about the ACI Fabric topology and the Application Server. The sample set of parameters were used to demonstrate configuring Syslog in an ACI Pod.

Device\Entity	NodeID	Fabric - OOB Mgmt Address
APIC 1	1	10.122.254.141
APIC 2	2	10.122.254.142
APIC 3	3	10.122.254.143
Spine 1	201	10.122.254.130
Spine 2	202	10.122.254.131
Leaf 1	101	10.122.254.128
Leaf 2	102	10.122.254.135
Leaf 3	103	10.122.254.136
Leaf 4	104	10.122.254.137
Default Gateway for Nodes		10.122.254.1 / 24
Application Server (SYSLOG)	ACI-P1-Server	10.122.254.77

Configure Syslog Policy for the ACI Fabric

This Section of the Technote can be used as a reference example for configuring Syslog in your ACI Fabric Solution. Simply replace the sample topology information with your own and you can configure SYSLOG Services for Controllers and Leaf\Spine Switches in your ACI Fabric Solution.

This Section will:

- [Create Syslog Monitoring Destination Group.](#)
- [Configure FABRIC > FABRIC POLICIES to send SYSLOG messages to Syslog Remote Destinations.](#)
- [Configure FABRIC > ACCESS POLICIES to send SYSLOG messages to Syslog Remote Destinations.](#)

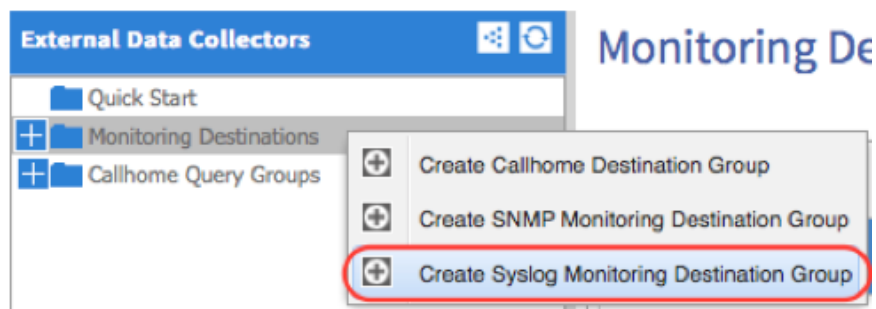
Note: As mentioned above, Please refer to the Table above to use for a reference for the Technote Fabric and Application Server.

STEP 1: Create Syslog Monitoring Destination Group.

The Syslog monitoring destination group will be used by the Cisco ACI Fabric for sending syslog messages. Use the GUI to create syslog monitoring destination group. Use the API Inspector to capture the API POST information from this configuration.

Task 1.1 Use the APIC ADMIN GUI to a create syslog monitoring destination group.

- On the menu bar, choose **ADMIN > EXTERNAL DATA COLLECTORS**. In the Navigation pane, select **MONITORING DESTINATIONS**. Right-click and click **CREATE SYSLOG MONITORING DESTINATION GROUP**. In the Create Syslog monitoring destination group dialog box, perform the following actions:



Task 1.1.1 DEFINE A GROUP NAME AND PROFILE

- Enter **Name** (`fab-syslog-destGrp`)
- Enter **Description** (`ACI Bootcamp Lab for SYSLOG`)
- For the **REMAINING** Fields, accept the **DEFAULT** settings.
- Click **NEXT**

CREATE SYSLOG MONITORING DESTINATION GROUP

STEP 1 > PROFILE

1. PROFILE

Define Group Name and Profile

Name:

Description:

Admin State:

LOCAL FILE DESTINATION

Admin State:

Severity:

CONSOLE DESTINATION

Admin State:

Severity:

Task 1.1.2 CREATE SYSLOG MONITORING DESTINATION GROUP

From the "Create Syslog Monitoring Destination Group" wizard, Create Syslog Remote Destinations. Click on the "+" to **CREATE A SYSLOG REMOTE DESTINATION**. In the Create Syslog Remote Destination dialog box, perform the following actions:

- Enter **Host** (10.122.254.77 for ACI-P1-Server. Refer to your Application Server address)
- Enter **Name** (ACI-P1-Server)
- Select **Admin State** (enabled)
- Select **Severity** (information)
- Select **Forwarding Facility** (local7)
- Select **Management EPG** (default (Out-of-Band))

Note: The Host can be an IP Address or DNS Name. DNS Services for the Fabric must be configured to use DNS Host Names.

- Click **OK**

CREATE SYSLOG REMOTE DESTINATION

Define syslog remote destination

Host: 10.122.254.77
Name: ACI-P1-Server

Admin State: enabled
 disabled

Severity: information

Port: 514

Forwarding Facility: local7

Management EPG: default (Out-of-Band)

- Click **FINISH**

CREATE SYSLOG MONITORING DESTINATION GROUP

STEP 2 > REMOTE DESTINATIONS

1. PROFILE 2. REMOTE DESTINATIONS

Create Remote Destinations

Host	Name	Admin State	Severity	Port	Forwarding Facility	Management EPG
10.122.254.77	ACI-P1-Server	enabled	information	514	local7	default (Out-of-B...

< PREVIOUS **FINISH** CANCEL

AAA | SCHEDULERS | HISTORICAL RECORD POLICIES | FIRMWARE | EXTERNAL DATA COLLECTORS | IMPORT/EXPORT

Monitoring Destinations

CALLHOME SNMP **SYSLOG**

ACTIONS

NAME	DESCRIPTION	ADMIN STATE	LOCAL FILE SEVERITY	CONSOLE SEVERITY
fab-syslog-destGrp	ACI Bootcamp Lab for SYSL...	enabled	information	alerts

Using the **APIC API Inspector**, this API Example was captured from the POST request to Create Syslog Monitoring Destination Group. You can use this APIC Example and use POSTMAN REST Client to create the Syslog Monitoring Destination Group.

API EXAMPLE

method: **POST**

url: <https://10.122.254.141/api/node/mo/uni/fabric/slgroup-fab-syslog-destGrp.json>

payload

```
{
  "syslogGroup": {
    "attributes": {
      "dn": "uni/fabric/slgroup-fab-syslog-destGrp",
      "name": "fab-syslog-destGrp",
      "descr": "ACI Bootcamp Lab for SYSLOG",
      "rn": "slgroup-fab-syslog-destGrp",
      "status": "created"
    },
    "children": [
      {
        "syslogConsole": {
          "attributes": {
            "dn": "uni/fabric/slgroup-fab-syslog-destGrp/console",
            "rn": "console",
            "status": "created"
          },
          "children": []
        },
        "syslogFile": {
          "attributes": {
            "dn": "uni/fabric/slgroup-fab-syslog-destGrp/file",
            "rn": "file",
            "status": "created"
          },
          "children": []
        },
        "syslogProf": {
          "attributes": {
            "dn": "uni/fabric/slgroup-fab-syslog-destGrp/prof",
            "rn": "prof",
            "status": "created"
          },
          "children": []
        },
        "syslogRemoteDest": {
          "attributes": {
            "dn": "uni/fabric/slgroup-fab-syslog-destGrp/rdst-10.122.254.77",
            "host": "10.122.254.77",
            "name": "ACI-P1-Server",
            "severity": "information",
            "rn": "rdst-10.122.254.77",
            "status": "created"
          },
          "children": [
            {
              "fileRsARemoteHostToEpg": {
                "attributes": {
                  "tDn": "uni/tn-mgmt/mgmt-default/oob-default",
                  "status": "created"
                },
                "children": []
              }
            }
          ]
        }
      ]
    }
  }
}
```

STEP 2: Configure FABRIC > FABRIC POLICIES to send SYSLOG messages to Syslog Remote Destinations.

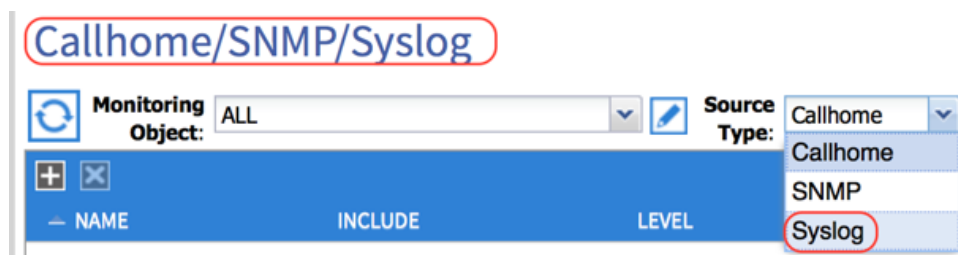
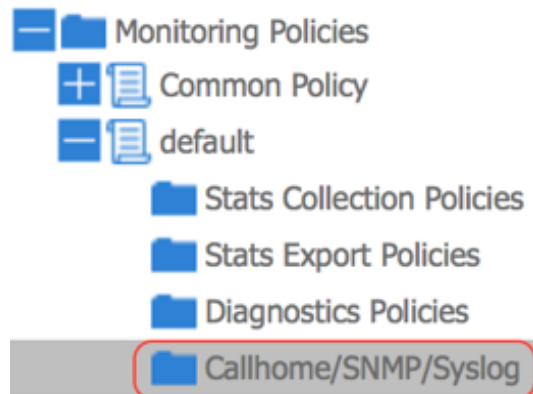
Fabric policies govern the operation of internal fabric interfaces. The system provides default fabric policies. Fabric policies enable configuring various functions or protocols. Administrators who have fabric administrator privileges can create new fabric policies according to their requirements. The APIC enables administrators to select the pods, leaf switches, and interfaces to which they will apply access policies.

Fabric policies configure interfaces that connect spine and leaf switches. Fabric policies can enable features such as monitoring (statistics collection and statistics export), troubleshooting (on-demand diagnostics and SPAN), or NTP.

Fabric Syslog Sources need to be configured in the **DEFAULT** and **COMMON** monitoring policies in the **Fabric Policies** configuration. Use the APIC ADMIN GUI to configure the **DEFAULT** and **COMMON** syslog monitoring policies. Use the API Inspector to capture the API POST information from this configuration.

Task 2.1 Use the APIC ADMIN GUI to a configure the "DEFAULT" monitoring policy for syslog.

- On the menu bar, choose **FABRIC > FABRIC POLICIES**. In the Navigation pane, expand **MONITORING POLICIES**.
- Expand **default**
- Select "**Callhome/SNMP/Syslog**"
- In the "Callhome/SNMP/Syslog" Work Pane, **Select the SOURCE TYPE "SYSLOG"** from the Source Type drop down list.
- Click on the " + " sign to **CREATE SYSLOG SOURCE**. In the Create Syslog Source dialog box, perform the following actions:
 - ➔ Enter **Name** (*fab-syslog-source*)
 - ➔ Select **Min Severity** (*information*)
 - ➔ For **Include** (*Check boxes for Events, Audit logs, and Faults*)
 - ➔ Select **Dest Group** (*fab-syslog-destGrp*)
 - ➔ Click **SUBMIT**



Callhome/SNMP/Syslog

Monitoring Object: ALL Source Type: Syslog

NAME	INCLUDE	MIN SEVERITY	DESTINATION GROUP
fab-syslog-source	All Audit logs Events Faults	information	fab-syslog-destGrp

Using the **APIC API** Inspector, this API Example was captured from the POST request to create Syslog Source for the "**DEFAULT**" monitoring policy for syslog. You can use this APIC Example and use POSTMAN REST Client to create Syslog Source for the "**DEFAULT**" monitoring policy.

API EXAMPLE

method: POST

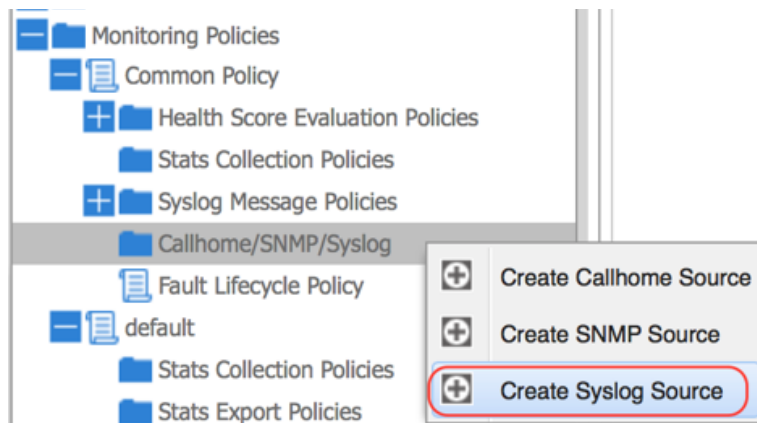
url: <https://10.122.254.141/api/node/mo/uni/fabric/monfab-default/slsrc-fab-syslog-source.json>

payload

```
{
  "syslogSrc": {
    "attributes": {
      "dn": "uni/fabric/monfab-default/slsrc-fab-syslog-source",
      "name": "fab-syslog-source",
      "minSev": "information",
      "incl": "events,audit,faults",
      "rn": "slsrc-fab-syslog-source",
      "status": "created"
    },
    "children": [
      {
        "syslogRsDestGroup": {
          "attributes": {
            "tDn": "uni/fabric/slgroup-fab-syslog-destGrp",
            "status": "created"
          },
          "children": []
        }
      }
    ]
  }
}
```

Task 2.2 Use the APIC ADMIN GUI to a configure the "COMMON" monitoring policy for syslog.

- On the menu bar, choose **FABRIC > FABRIC POLICIES**. In the Navigation pane, expand **MONITORING POLICIES**.
- Expand **Common Policy**
- Select "**Callhome/SNMP/Syslog**"
- **Right Click** on "Callhome/SNMP/Syslog" and Select the **CREATE SYSLOG SOURCE**. In the Create Syslog Source dialog box, perform the following actions:
 - ➔ Enter **Name** (*fab-syslog-source*)
 - ➔ Select **Min Severity** (*information*)
 - ➔ For **Include** (*Check boxes for Events, Audit logs, and Faults*)
 - ➔ Select **Dest Group** (*fab-syslog-destGrp*)
 - ➔ Click **SUBMIT**



The screenshot shows the 'CREATE SYSLOG SOURCE' dialog box. The title bar reads 'CREATE SYSLOG SOURCE'. The main area is titled 'Define Syslog Source' and contains the following fields:

- Name:** fab-syslog-source
- Min Severity:** information
- Include:** Events, Audit logs, Faults
- Dest Group:** fab-syslog-destGrp

At the bottom of the dialog box, there are two buttons: 'SUBMIT' and 'CANCEL'.

Callhome/SNMP/Syslog i

CALLHOME | SNMP | **SYSLOG**

ACTIONS ▾

NAME	INCLUDE	MIN SEVERITY	DESTINATION GROUP
fab-syslog-source	All Audit logs Events Faults	information	fab-syslog-destGrp

Using the **APIC API** Inspector, this API Example was captured from the POST request to create Syslog Source for the "**COMMON**" monitoring policy for syslog. You can use this APIC Example and use POSTMAN REST Client to create Syslog Source for the "**COMMON**" monitoring policy.

API EXAMPLE

method: **POST**

url: <https://10.122.254.141/api/node/mo/uni/fabric/moncommon/slsrc-fab-syslog-source.json>

payload

```
{
  "syslogSrc": {
    "attributes": {
      "dn": "uni/fabric/moncommon/slsrc-fab-syslog-source",
      "name": "fab-syslog-source",
      "minSev": "information",
      "incl": "events,audit,faults",
      "rn": "slsrc-fab-syslog-source",
      "status": "created"
    },
    "children": [
      {
        "syslogRsDestGroup": {
          "attributes": {
            "tDn": "uni/fabric/slgroup-fab-syslog-destGrp",
            "status": "created"
          },
          "children": []
        }
      }
    ]
  }
}
```

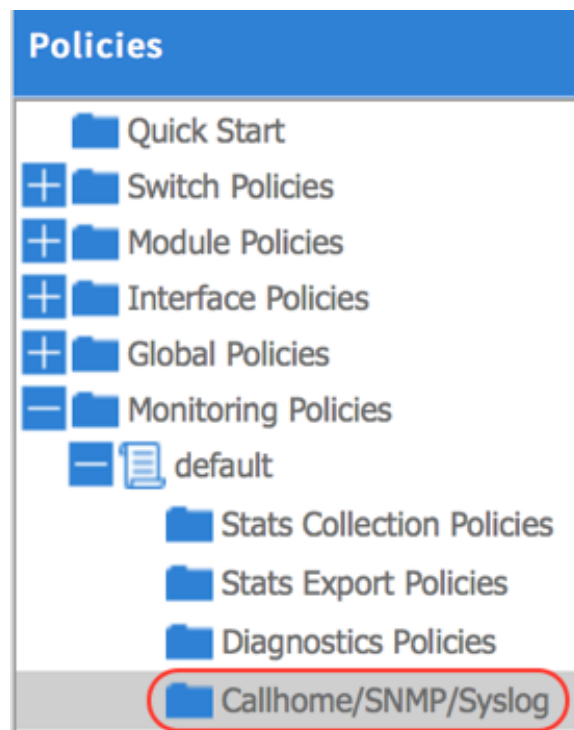
STEP 3: Configure FABRIC > ACCESS POLICIES to send SYSLOG messages to Syslog Remote Destinations.

Access policies govern the operation of interfaces that provide external access to the fabric. The system provides default access policies. Access policies enable configuring various functions or protocols. Administrators who have fabric administrator privileges can create new access policies according to their requirements. The APIC enables administrators to select the pods, leaf switches, and interfaces to which they will apply access policies.

Fabric Syslog Sources need to be configured in the **DEFAULT** monitoring policies configured in the **Access Policies** configuration. Use the GUI to configure the **DEFAULT** Syslog monitoring policies. Use the API Inspector to capture the API POST information from this configuration.

Task 3.1 Use the APIC ADMIN GUI to a configure the "DEFAULT" monitoring policy for syslog.

- On the menu bar, choose **FABRIC > ACCESS POLICIES**. In the Navigation pane, expand **MONITORING POLICIES**.
- Expand **default**
- Select "**Callhome/SNMP/Syslog**"
- In the "Callhome/SNMP/Syslog" Work Pane, **Select the SOURCE TYPE "SYSLOG"** from the Source Type drop down list.
- Click on the " + " sign to **CREATE SYSLOG SOURCE**. In the Create Syslog Source dialog box, perform the following actions:
 - ➔ Enter **Name** (fab-syslog-source)
 - ➔ Select **Min Severity** (information)
 - ➔ For **Include** (Check boxes for Events, Audit logs, and Faults)
 - ➔ Select **Dest Group** (fab-syslog-destGrp)
 - ➔ Click **SUBMIT**



Callhome/SNMP/Syslog

Monitoring Object: ALL Source Type: Callhome

Callhome
SNMP
Syslog

NAME	INCLUDE	LEVEL
------	---------	-------

CREATE SYSLOG SOURCE

Define Syslog Source

Name: fab-syslog-source

Min Severity: information

Include: Events
 Audit logs
 Faults

Dest Group: fab-syslog-destGrp

SUBMIT CANCEL

Callhome/SNMP/Syslog

Monitoring Object: ALL Source Type: Syslog

NAME	INCLUDE	MIN SEVERITY	DESTINATION GROUP
fab-syslog-source	All Audit logs Events Faults	information	fab-syslog-destGrp

Using the **APIC API Inspector**, this API Example was captured from the POST request to create Syslog Source for the "**DEFAULT**" monitoring policy for syslog. You can use this APIC Example and use POSTMAN REST Client to create Syslog Source for the "**DEFAULT**" monitoring policy.

API EXAMPLE

method: **POST**

url: <https://10.122.254.141/api/node/mo/uni/infra/moninfra-default/slsrc-fab-syslog-source.json>

payload

```
{"syslogSrc":{"attributes":{"dn":"uni/infra/moninfra-default/slsrc-fab-syslog-source","name":"fab-syslog-source","minSev":"information","incl":"events,audit,faults","rn":"slsrc-fab-syslog-source","status":"created"},"children":[{"syslogRsDestGroup":{"attributes":{"tDn":"uni/fabric/slgroup-fab-syslog-destGrp","status":"created"},"children":[]}]}}
```

Troubleshooting Syslog Policy for the ACI Fabric

Verify the configuration of SYSLOG Services for Controllers and Leaf\Spine Switches in your designated ACI fabric. This section will provide references for CLI commands and tools that may be helpful in troubleshooting the configuration and application of the Syslog policies for Controllers and Leaf\Spine Switches in your designated ACI fabric.

This section will:

- **Access the Console of your SYSLOG Server to verify SYSLOG messages are being sent from the Cisco ACI Fabric System & being received by the SYSLOG Server.**
- **Verify configuration of Syslog on APIC Controllers.**
- **Verify configuration of Syslog on Leaf\Spine Node Switches.**

Note: The examples given in this section of the Technote are not totally inclusive. These are just some examples that I have gathered while troubleshooting Syslog Services for the ACI Fabric.

- **Access the Console of your SYSLOG Server to verify SYSLOG messages are being sent from the Cisco ACI Fabric System & being received by the SYSLOG Server.**
 - ➔ Remote desktop to your Application Server and review the Kiwi Syslog Service Manager Console.

Date	Time	Priority	Hostname	Message
01-08-2015	21:56:33	Local7.Info	10.122.254.141	<190> Jan 08 21:37:08 fab2-apic1 %LOG_LOCAL7-6-SYSTEM_MSG [E4204935][transition][info][topology/pod-1/lnkcnt-104/lnk-202-1-5-t-o-104-1-98] Fabric Link
01-08-2015	21:56:33	Local7.Info	10.122.254.141	<190> Jan 08 21:37:08 fab2-apic1 %LOG_LOCAL7-6-SYSTEM_MSG [E4204935][transition][info][topology/pod-1/lnkcnt-104/lnk-202-1-5-t-o-104-1-98] Fabric Link
01-08-2015	21:56:33	Local7.Info	10.122.254.141	<190> Jan 08 21:37:08 fab2-apic1 %LOG_LOCAL7-6-SYSTEM_MSG [E4204935][transition][info][topology/pod-1/lnkcnt-104/lnk-201-1-5-t-o-104-1-97] Fabric Link
01-08-2015	21:56:33	Local7.Info	10.122.254.141	<190> Jan 08 21:37:08 fab2-apic1 %LOG_LOCAL7-6-SYSTEM_MSG [E4204935][transition][info][topology/pod-1/lnkcnt-104/lnk-201-1-5-t-o-104-1-97] Fabric Link
01-08-2015	21:56:33	Local7.Info	10.122.254.128	<190> Jan 08 21:37:08 fab2-leaf1 %LOG_LOCAL7-6-SYSTEM_MSG [E4208070][oper-state-change][info][sys/tunnel-[tunnel6]] Interface tunnel6 is down reason Destination unreachable
01-08-2015	21:56:33	Local7.Info	10.122.254.128	<190> Jan 08 21:37:08 fab2-leaf1 %LOG_LOCAL7-6-SYSTEM_MSG [E4208070][oper-state-change][info][sys/tunnel-[tunnel6]] Interface tunnel6 is down reason Destination unreachable
01-08-2015	21:56:33	Local7.Error	10.122.254.128	<187> Jan 08 21:37:08 fab2-leaf1 %LOG_LOCAL7-3-SYSTEM_MSG [F0475][soaking][dest-unreach][major][sys/tunnel-[tunnel6]/fault-F0475] Tunnel destination is not reachable.
01-08-2015	21:56:33	Local7.Error	10.122.254.128	<187> Jan 08 21:37:08 fab2-leaf1 %LOG_LOCAL7-3-SYSTEM_MSG [F0475][soaking][dest-unreach][major][sys/tunnel-[tunnel6]/fault-F0475] Tunnel destination is not reachable.

- **Verify configuration of Syslog on APIC Controllers.**

★ CLI Commands

- ➔ `cat /etc/rsyslog.conf`
- ➔ `ps -A | grep rsyslog`
- ➔ `cat /var/log/external/message`
- ➔ (root) `netstat -p | grep syslog`
- ➔ (root) `tcpdump -i oobmgmt -f port 514`

★ Visore

syslogGroup - The syslog destination group, which contains all information required to send syslog messages to a group of destinations.

syslogRemoteDest - The syslog remote destination host enables you to specify syslog servers to which messages from the APIC and fabric nodes should be forwarded.

syslogProf - Represents the configuration parameters used for this protocol.

syslogRtDestGroup - A target relation to the syslog destination group.

★ REST API

[/api/node/mo/uni/fabric/slgroup-fab-syslog-destGrp.xml](#) - The syslog destination group, which contains all information required to send syslog messages to a group of destinations.

[/api/node/class/syslogRemoteDest.xml](#) - The syslog remote destination host enables you to specify syslog servers to which messages from the APIC and fabric nodes should be forwarded.

[/api/node/class/syslogProf.xml](#) - Represents the configuration parameters used for this protocol.

[/api/node/class/syslogRtDestGroup.xml](#) - A target relation to the syslog destination group.

APIC CLI EXAMPLES

```
apic1:~> ps -A | grep rsyslog
```

```
356 ?    00:00:00 rsyslogd
```

Note: ps command gives a snapshot of the current processes

```
apic1:~# netstat -p | grep syslog
```

```
unix 17  []    DGRAM          55220 32084/svc_ifc_event /var/run/mgmt/syslog_socket
```

```
unix 11  []    DGRAM          74872 356/rsyslogd      /dev/log
```

```
apic1:~# tcpdump -i oobmgmt -f port 514
```

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode

listening on oobmgmt, link-type EN10MB (Ethernet), capture size 65535 bytes

```
22:23:46.677388 IP tsi-pod2-apic1-141.cisco.com.55713 > aci-p1-server.cisco.com.syslog: SYSLOG local7.info, length: 177
```

```
22:23:49.095558 IP tsi-pod2-apic1-141.cisco.com.55713 > aci-p1-server.cisco.com.syslog: SYSLOG local7.info, length: 177
```

```
22:24:09.189169 IP tsi-pod2-apic1-141.cisco.com.55713 > aci-p1-server.cisco.com.syslog: SYSLOG local7.info, length: 213
```

```
22:24:09.189424 IP tsi-pod2-apic1-141.cisco.com.55713 > aci-p1-server.cisco.com.syslog: SYSLOG local7.info, length: 213
```

```
22:24:09.189588 IP tsi-pod2-apic1-141.cisco.com.55713 > aci-p1-server.cisco.com.syslog: SYSLOG local7.info, length: 213
```

22:24:09.189880 IP tsi-pod2-apic1-141.cisco.com.55713 > aci-p1-server.cisco.com.syslog: SYSLOG local7.info, length: 213

apic1:~> **cat /var/log/external/messages | grep "fault"**

<1030> Jan 08 21:21:52 fab2-apic1 %LOG_LOCAL0-6-SYSTEM_MSG [E4207412][transition][info][subj-[uni/infra/moninfra-default/slsrc-fab-syslog-source]/mod-4294967832] Src fab-syslog-source created by user admin, change set: incl:all,audit,events,faults, minSev:information, name:fab-syslog-source









<1026> Jan 08 21:38:05 fab2-apic1 %LOG_LOCAL0-2-SYSTEM_MSG [F1543][soaking][node-inactive][critical][topology/pod-1/node-104/fault-F1543] Node 104 is inactive and not reachable.




<1026> Jan 08 21:38:05 fab2-apic1 %LOG_LOCAL0-2-SYSTEM_MSG [F1543][soaking][node-inactive][critical][topology/pod-1/node-104/fault-F1543] Node 104 is inactive and not reachable.

























<1026> Jan 08 21:40:35 fab2-apic1 %LOG_LOCAL0-2-SYSTEM_MSG [F1543][raised][node-inactive][critical][topology/pod-1/node-104/fault-F1543] Node 104 is inactive and not reachable.

VISORE EXAMPLES

<u>syslogGroup</u>	
childAction	
descr	ACI Bootcamp Lab for SYSLOG
dn	uni/fabric/slgroup-fab-syslog-destGrp < > !H
lcOwn	local
modTs	2015-01-08T18:08:22.114-04:00
monPolDn	uni/fabric/monfab-default < > !H
name	fab-syslog-destGrp
status	
uid	15374

syslogRemoteDest	
adminState	enabled
childAction	
descr	
dn	uni/fabric/slgroup-fab-syslog-destGrp/rdst-10.122.254.77 < >   
epgDn	uni/tn-mgmt/mgmtmp-default/oob-default < >  
forwardingFacility	local7
host	10.122.254.77
ip	
lcOwn	local
modTs	2015-01-08T18:08:22.114-04:00
monPolDn	uni/fabric/monfab-default < >   
name	ACI-P1-Server
operState	unknown
port	514
severity	information
status	
uid	15374
vrflD	0
vrflName	

syslogProf	
adminState	enabled
childAction	
descr	
dn	uni/fabric/slgroup-fab-syslog-destGrp/prof < >   
lcOwn	local
modTs	2015-01-08T18:08:22.114-04:00
name	syslog
port	514
status	
transport	udp
uid	15374

syslogRtDestGroup	
childAction	
dn	uni/fabric/slgroup-fab-syslog-destGrp/rtdestGroup-[uni/fabric/monfab-default/s/src-fab-syslog-source] < >    
lcOwn	local
modTs	2015-01-08T21:19:31.610-04:00
status	
tCl	syslogSrc
tDn	uni/fabric/monfab-default/s/src-fab-syslog-source < >    
syslogRtDestGroup	
childAction	
dn	uni/fabric/slgroup-fab-syslog-destGrp/rtdestGroup-[uni/fabric/moncommon/s/src-fab-syslog-source] < >    
lcOwn	local
modTs	2015-01-08T21:52:37.731-04:00
status	
tCl	syslogSrc
tDn	uni/fabric/moncommon/s/src-fab-syslog-source < >    
syslogRtDestGroup	
childAction	
dn	uni/fabric/slgroup-fab-syslog-destGrp/rtdestGroup-[uni/infra/moninfra-default/s/src-fab-syslog-source] < >    
lcOwn	local
modTs	2015-01-08T22:20:32.407-04:00
status	
tCl	syslogSrc
tDn	uni/infra/moninfra-default/s/src-fab-syslog-source < >    

REST API EXAMPLES

SYSLOG Destination Groups

The syslog destination group, which contains all information required to send syslog messages to a group of destinations.

<https://10.122.254.141/api/node/mo/uni/fabric/slgroup-fab-syslog-destGrp.xml?query-target=children> GET

Send Save Preview Pre-request script Tests Add to collection

Body Cookies Headers (9) Tests STATUS 200 OK TIME 40 ms

Pretty Raw Preview XML

```
childAction="" descr="" dn="uni/fabric/slgroup-fab-syslog-destGrp/console" lcOwn="local" modTs="2015-01-08"
childAction="" descr="" dn="uni/fabric/slgroup-fab-syslog-destGrp/file" lcOwn="local" modTs="2015-01-08"
childAction="" descr="" dn="uni/fabric/slgroup-fab-syslog-destGrp/prof" lcOwn="local" modTs="2015-01-08"
" childAction="" descr="" dn="uni/fabric/slgroup-fab-syslog-destGrp/rdst-10.122.254.77" epgDn="uni/
uni/fabric/slgroup-fab-syslog-destGrp/rtdestGroup-[uni/fabric/monfab-default/slsrc-fab-syslog-sour
uni/fabric/slgroup-fab-syslog-destGrp/rtdestGroup-[uni/fabric/moncommon/slsrc-fab-syslog-source]"
uni/fabric/slgroup-fab-syslog-destGrp/rtdestGroup-[uni/infra/moninfra-default/slsrc-fab-syslog-sou
```

SYSLOG Protocol Params

Represents the configuration parameters used for this protocol.

<https://10.122.254.141/api/node/class/syslogProf.xml> GET

Send Save Preview Pre-request script Tests Add to collection

Body Cookies Headers (9) Tests STATUS 200 OK TIME 198 ms

Pretty Raw Preview XML

```
--04:00" name="syslog" port="514" status="" transport="udp" uid="15374" />
```

SYSLOG Sources for Monitoring Policies

A target relation to the syslog destination group.

<https://10.122.254.141/api/node/class/syslogRtDestGroup.xml> GET

Send Save Preview Pre-request script Tests Add to col

Body Cookies Headers (9) Tests STATUS 200 OK TIME 240 ms

Pretty Raw Preview XML

```
= "syslogSrc" tDn="uni/fabric/monfab-default/slsrc-fab-syslog-source" />  
logSrc" tDn="uni/fabric/moncommon/slsrc-fab-syslog-source" />  
l="syslogSrc" tDn="uni/infra/moninfra-default/slsrc-fab-syslog-source" />
```

SYSLOG Destination Groups

List SYSLOG Destination Groups

<https://10.122.254.141/api/node/class/syslogRemoteDest.xml> GET

Send Save Preview Pre-request script Tests Add to co

Body Cookies Headers (9) Tests STATUS 200 OK TIME 43 ms

Pretty Raw Preview XML

```
fault/oob-default" forwardingFacility="local7" host="10.122.254.77" ip=""
```

- **Verify configuration of Syslog on Leaf\Spine Switches.**

- ★ **CLI Commands**

- ➔ **cat /etc/syslog-startup.conf**
- ➔ **cat /etc/syslog-startup.conf.busybox**
- ➔ **cat /etc/syslog.conf**
- ➔ **cat /var/log/external/message**
- ➔ **(root) netstat -p | grep syslog**
- ➔ **(root) tcpdump -i eth0 -f port 514**
- ➔ **(root) tcpdump -nnvXS dst 10.122.254.77**

SWITCH CLI EXAMPLES

```
fab2-leaf1# cat /etc/syslog-startup.conf
# This configuration file is used by the busybox syslog init script,
# /etc/init.d/syslog[.busybox] to set syslog configuration at start time.
```

```
DESTINATION=file           # log destinations (buffer file remote)
LOGFILE=/var/log/messages  # where to log (file)
REMOTE=loghost:514        # where to log (syslog remote)
REDUCE=no                  # reduce-size logging
DROPDUPLICATES=no        # whether to drop duplicate log entries
#ROTATESIZE=0             # rotate log if grown beyond X [kByte]
#ROTATEGENS=3             # keep X generations of rotated logs
BUFFERSIZE=64             # size of circular buffer [kByte]
FOREGROUND=no             # run in foreground (don't use!)
#LOGLEVEL=5               # local log level (between 1 and 8)
```

```
fab2-leaf1# cat /etc/syslog-startup.conf.busybox
# This configuration file is used by the busybox syslog init script,
# /etc/init.d/syslog[.busybox] to set syslog configuration at start time.
```

```
DESTINATION=file           # log destinations (buffer file remote)
LOGFILE=/var/log/messages  # where to log (file)
REMOTE=loghost:514        # where to log (syslog remote)
REDUCE=no                  # reduce-size logging
DROPDUPLICATES=no        # whether to drop duplicate log entries
#ROTATESIZE=0             # rotate log if grown beyond X [kByte]
#ROTATEGENS=3             # keep X generations of rotated logs
BUFFERSIZE=64             # size of circular buffer [kByte]
FOREGROUND=no             # run in foreground (don't use!)
#LOGLEVEL=5               # local log level (between 1 and 8)
```

```
fab2-leaf1# cat /var/log/external/messages | grep "fault"
```

```
<1027> Jan 08 21:37:08 fab2-leaf1 %LOG_LOCAL0-3-SYSTEM_MSG [F0475][soaking][dest-unreach][major][sys/tunnel-[tunnel6]/fault-F0475] Tunnel destination is not reachable.
```

```
<187> Jan 08 21:37:08 fab2-leaf1 %LOG_LOCAL7-3-SYSTEM_MSG [F0475][soaking][dest-unreach][major][sys/tunnel-[tunnel6]/fault-F0475] Tunnel destination is not reachable.
```

```
<1027> Jan 08 21:39:16 fab2-leaf1 %LOG_LOCAL0-3-SYSTEM_MSG [F0475][raised][dest-unreach][major][sys/tunnel-[tunnel6]/fault-F0475] Tunnel destination is not reachable.
```

```
<1027> Jan 08 21:39:16 fab2-leaf1 %LOG_LOCAL0-3-SYSTEM_MSG [F0475][raised][dest-unreach][major][sys/tunnel-[tunnel6]/fault-F0475] Tunnel destination is not reachable.
```

```
fab2-leaf1# netstat -p | grep syslog
```

```
unix 138 [ ] DGRAM 61139 4085/svc_ifc_eventm /
var/run/mgmt/syslog_socket
```

```
fab2-leaf1# tcpdump -i eth0 -f port 514
```

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
```

```
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
```

```
01:08:11.461622 IP fab2-leaf1-oob.cisco.com.47213 > aci-p1-
```

```
server.cisco.com.syslog: SYSLOG local7.info, length: 176
```

```
01:08:28.128769 IP fab2-leaf1-oob.cisco.com.47213 > aci-p1-
```

```
server.cisco.com.syslog: SYSLOG local7.error, length: 172
```

```
01:08:28.129261 IP fab2-leaf1-oob.cisco.com.47213 > aci-p1-
```

```
server.cisco.com.syslog: SYSLOG local7.error, length: 172
```

```
01:08:28.130650 IP fab2-leaf1-oob.cisco.com.47213 > aci-p1-
```

```
server.cisco.com.syslog: SYSLOG local7.info, length: 178
```

```
01:08:28.131084 IP fab2-leaf1-oob.cisco.com.47213 > aci-p1-
```

```
server.cisco.com.syslog: SYSLOG local7.info, length: 178
```

```
fab2-leaf1# tcpdump -nnvvXS dst 10.122.254.77
```

```
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
```

```
01:09:39.771729 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has
```

```
10.122.254.77 tell 10.122.254.137, length 46
```

```
0x0000: 0001 0800 0604 0001 88f0 31bf 45f0 0a7a .....1.E..z
```

```
0x0010: fe89 0000 0000 0000 0a7a fe4d 0000 0000 .....z.M....
```

```
0x0020: 0000 0000 0000 0000 0000 0000 0000 .....z.M....
```

```
01:09:41.106426 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has
```

```
10.122.254.77 tell 10.122.254.130, length 46
```

```
0x0000: 0001 0800 0604 0001 0022 bdfb fffa 0a7a ....."......z
```

```
0x0010: fe82 0000 0000 0000 0a7a fe4d 0000 0000 .....z.M....
```

```
0x0020: 0000 0000 0000 0000 0000 0000 0000 .....z.M....
```



```

01:09:41.107655 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has
10.122.254.77 tell 10.122.254.131, length 46
    0x0000:  0001 0800 0604 0001 0022 bdfc 047a 0a7a  ....."....z.z
    0x0010:  fe83 0000 0000 0000 0a7a fe4d 0000 0000  .....z.M....
    0x0020:  0000 0000 0000 0000 0000 0000 0000  .....

01:09:41.876270 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has
10.122.254.77 tell 10.122.254.135, length 46
    0x0000:  0001 0800 0604 0001 0022 bdf8 af90 0a7a  ....."......z
    0x0010:  fe87 0000 0000 0000 0a7a fe4d 0000 0000  .....z.M....
    0x0020:  0000 0000 0000 0000 0000 0000 0000  .....

01:09:42.168913 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has
10.122.254.77 tell 10.122.254.128, length 28
    0x0000:  0001 0800 0604 0001 7c69 f610 5bc8 0a7a  .....|i...[...z
    0x0010:  fe80 0000 0000 0000 0a7a fe4d  .....z.M

01:09:42.169052 IP (tos 0x0, ttl 64, id 62066, offset 0, flags [none], proto UDP
(17), length 200)
  10.122.254.128.47213 > 10.122.254.77.514: [bad udp cksum a655!] SYSLOG,
length: 172
  Facility local7 (23), Severity error (3)
  Msg: <187> Jan 09 01:09:42 fab2-leaf1 %LOG_LOCAL7-3-SYSTEM_MSG [F0475]
[soaking][dest-unreach][major][sys/tunnel-[tunnel6]/fault-F0475] Tunnel
destination is not reachable.\0x0a
    0x0000:  3c31 3837 3e3c 3138 373e 204a 616e 2030
    0x0010:  3920 3031 3a30 393a 3432 2066 6162 322d
    0x0020:  6c65 6166 3120 254c 4f47 5f4c 4f43 414c
    0x0030:  372d 332d 5359 5354 454d 5f4d 5347 205b
    0x0040:  4630 3437 355d 5b73 6f61 6b69 6e67 5d5b
    0x0050:  6465 7374 2d75 6e72 6561 6368 5d5b 6d61
    0x0060:  6a6f 725d 5b73 7973 2f74 756e 6e65 6c2d
    0x0070:  5b74 756e 6e65 6c36 5d2f 6661 756c 742d
    0x0080:  4630 3437 355d 2054 756e 6e65 6c20 6465
    0x0090:  7374 696e 6174 696f 6e20 6973 206e 6f74
    0x00a0:  2072 6561 6368 6162 6c65 2e0a
    0x0000:  4500 00c8 f272 0000 4011 75f0 0a7a fe80  E....r...@.u...z..
    0x0010:  0a7a fe4d b86d 0202 00b4 1288 3c31 3837  .z.M.m.....<187
    0x0020:  3e3c 3138 373e 204a 616e 2030 3920 3031  ><187>.Jan.09.01
    0x0030:  3a30 393a 3432 2066 6162 322d 6c65 6166  :09:42.fab2-leaf
    0x0040:  3120 254c 4f47 5f4c 4f43 414c 372d 332d  1.%LOG_LOCAL7-3-
    0x0050:  5359 5354 454d 5f4d 5347 205b 4630 3437  SYSTEM_MSG.[F047
    0x0060:  355d 5b73 6f61 6b69 6e67 5d5b 6465 7374  5][soaking][dest
    0x0070:  2d75 6e72 6561 6368 5d5b 6d61 6a6f 725d  -unreach][major]
    0x0080:  5b73 7973 2f74 756e 6e65 6c2d 5b74 756e  [sys/tunnel-[tun
    0x0090:  6e65 6c36 5d2f 6661 756c 742d 4630 3437  nel6]/fault-F047
    0x00a0:  355d 2054 756e 6e65 6c20 6465 7374 696e  5].Tunnel.destin
    0x00b0:  6174 696f 6e20 6973 206e 6f74 2072 6561  ation.is.not.rea
    0x00c0:  6368 6162 6c65 2e0a  chable..

```

01:09:42.169861 IP (tos 0x0, ttl 64, id 62067, offset 0, flags [none], proto UDP (17), length 200)

10.122.254.128.47213 > 10.122.254.77.514: [bad udp cksum a655!] SYSLOG, length: 172

Facility local7 (23), Severity error (3)

Msg: <187> Jan 09 01:09:42 fab2-leaf1 %LOG_LOCAL7-3-SYSTEM_MSG [F0475]

[soaking][dest-unreach][major][sys/tunnel-[tunnel6]/fault-F0475] Tunnel destination is not reachable.\0x0a

0x0000: 3c31 3837 3e3c 3138 373e 204a 616e 2030

0x0010: 3920 3031 3a30 393a 3432 2066 6162 322d

0x0020: 6c65 6166 3120 254c 4f47 5f4c 4f43 414c

0x0030: 372d 332d 5359 5354 454d 5f4d 5347 205b

0x0040: 4630 3437 355d 5b73 6f61 6b69 6e67 5d5b

0x0050: 6465 7374 2d75 6e72 6561 6368 5d5b 6d61

0x0060: 6a6f 725d 5b73 7973 2f74 756e 6e65 6c2d

0x0070: 5b74 756e 6e65 6c36 5d2f 6661 756c 742d

0x0080: 4630 3437 355d 2054 756e 6e65 6c20 6465

0x0090: 7374 696e 6174 696f 6e20 6973 206e 6f74

0x00a0: 2072 6561 6368 6162 6c65 2e0a

0x0000: 4500 00c8 f273 0000 4011 75ef 0a7a fe80 E....s...@.u..z..

0x0010: 0a7a fe4d b86d 0202 00b4 1288 3c31 3837 .z.M.m.....<187

0x0020: 3e3c 3138 373e 204a 616e 2030 3920 3031 ><187>.Jan.09.01

0x0030: 3a30 393a 3432 2066 6162 322d 6c65 6166 :09:42.fab2-leaf

0x0040: 3120 254c 4f47 5f4c 4f43 414c 372d 332d 1.%LOG_LOCAL7-3-

0x0050: 5359 5354 454d 5f4d 5347 205b 4630 3437 SYSTEM_MSG.[F047

0x0060: 355d 5b73 6f61 6b69 6e67 5d5b 6465 7374 5][soaking][dest

0x0070: 2d75 6e72 6561 6368 5d5b 6d61 6a6f 725d -unreach][major]

0x0080: 5b73 7973 2f74 756e 6e65 6c2d 5b74 756e [sys/tunnel-[tun

0x0090: 6e65 6c36 5d2f 6661 756c 742d 4630 3437 nel6]/fault-F047

0x00a0: 355d 2054 756e 6e65 6c20 6465 7374 696e 5].Tunnel.destin

0x00b0: 6174 696f 6e20 6973 206e 6f74 2072 6561 ation.is.not.rea

0x00c0: 6368 6162 6c65 2e0a chable..

01:09:42.172023 IP (tos 0x0, ttl 64, id 62068, offset 0, flags [none], proto UDP (17), length 206)

10.122.254.128.47213 > 10.122.254.77.514: [bad udp cksum 700c!] SYSLOG, length: 178

Facility local7 (23), Severity info (6)

Msg: <190> Jan 09 01:09:42 fab2-leaf1 %LOG_LOCAL7-6-SYSTEM_MSG [E4208070]

[oper-state-change][info][sys/tunnel-[tunnel6]] Interface tunnel6 is down reason Destination unreachable\0x0a

0x0000: 3c31 3930 3e3c 3139 303e 204a 616e 2030

0x0010: 3920 3031 3a30 393a 3432 2066 6162 322d

0x0020: 6c65 6166 3120 254c 4f47 5f4c 4f43 414c

0x0030: 372d 362d 5359 5354 454d 5f4d 5347 205b

0x0040: 4534 3230 3830 3730 5d5b 6f70 6572 2d73

0x0050: 7461 7465 2d63 6861 6e67 655d 5b69 6e66

0x0060: 6f5d 5b73 7973 2f74 756e 6e65 6c2d 5b74

```

0x0070: 756e 6e65 6c36 5d5d 2049 6e74 6572 6661
0x0080: 6365 2074 756e 6e65 6c36 2069 7320 646f
0x0090: 776e 2072 6561 736f 6e20 4465 7374 696e
0x00a0: 6174 696f 6e20 756e 7265 6163 6861 626c
0x00b0: 650a
0x0000: 4500 00ce f274 0000 4011 75e8 0a7a fe80 E....t...@.u...z..
0x0010: 0a7a fe4d b86d 0202 00ba 128e 3c31 3930 .z.M.m.....<190
0x0020: 3e3c 3139 303e 204a 616e 2030 3920 3031 ><190>.Jan.09.01
0x0030: 3a30 393a 3432 2066 6162 322d 6c65 6166 :09:42.fab2-leaf
0x0040: 3120 254c 4f47 5f4c 4f43 414c 372d 362d 1.%LOG_LOCAL7-6-
0x0050: 5359 5354 454d 5f4d 5347 205b 4534 3230 SYSTEM_MSG.[E420
0x0060: 3830 3730 5d5b 6f70 6572 2d73 7461 7465 8070][oper-state
0x0070: 2d63 6861 6e67 655d 5b69 6e66 6f5d 5b73 -change][info][s
0x0080: 7973 2f74 756e 6e65 6c2d 5b74 756e 6e65 ys/tunnel-[tunne
0x0090: 6c36 5d5d 2049 6e74 6572 6661 6365 2074 l6]].Interface.t
0x00a0: 756e 6e65 6c36 2069 7320 646f 776e 2072 unnel6.is.down.r
0x00b0: 6561 736f 6e20 4465 7374 696e 6174 696f eason.Destinatio
0x00c0: 6e20 756e 7265 6163 6861 626c 650a n.unreachable.
    
```

01:09:42.172369 IP (tos 0x0, ttl 64, id 62069, offset 0, flags [none], proto UDP (17), length 206)

10.122.254.128.47213 > 10.122.254.77.514: [bad udp cksum 700c!] SYSLOG, length: 178

Facility local7 (23), Severity info (6)

Msg: <190> Jan 09 01:09:42 fab2-leaf1 %LOG_LOCAL7-6-SYSTEM_MSG [E4208070] [oper-state-change][info][sys/tunnel-[tunnel6]] Interface tunnel6 is down reason Destination unreachable\0x0a

```

0x0000: 3c31 3930 3e3c 3139 303e 204a 616e 2030
0x0010: 3920 3031 3a30 393a 3432 2066 6162 322d
0x0020: 6c65 6166 3120 254c 4f47 5f4c 4f43 414c
0x0030: 372d 362d 5359 5354 454d 5f4d 5347 205b
0x0040: 4534 3230 3830 3730 5d5b 6f70 6572 2d73
0x0050: 7461 7465 2d63 6861 6e67 655d 5b69 6e66
0x0060: 6f5d 5b73 7973 2f74 756e 6e65 6c2d 5b74
0x0070: 756e 6e65 6c36 5d5d 2049 6e74 6572 6661
0x0080: 6365 2074 756e 6e65 6c36 2069 7320 646f
0x0090: 776e 2072 6561 736f 6e20 4465 7374 696e
0x00a0: 6174 696f 6e20 756e 7265 6163 6861 626c
0x00b0: 650a
0x0000: 4500 00ce f275 0000 4011 75e7 0a7a fe80 E....u...@.u...z..
0x0010: 0a7a fe4d b86d 0202 00ba 128e 3c31 3930 .z.M.m.....<190
0x0020: 3e3c 3139 303e 204a 616e 2030 3920 3031 ><190>.Jan.09.01
0x0030: 3a30 393a 3432 2066 6162 322d 6c65 6166 :09:42.fab2-leaf
0x0040: 3120 254c 4f47 5f4c 4f43 414c 372d 362d 1.%LOG_LOCAL7-6-
0x0050: 5359 5354 454d 5f4d 5347 205b 4534 3230 SYSTEM_MSG.[E420
0x0060: 3830 3730 5d5b 6f70 6572 2d73 7461 7465 8070][oper-state
0x0070: 2d63 6861 6e67 655d 5b69 6e66 6f5d 5b73 -change][info][s
0x0080: 7973 2f74 756e 6e65 6c2d 5b74 756e 6e65 ys/tunnel-[tunne
0x0090: 6c36 5d5d 2049 6e74 6572 6661 6365 2074 l6]].Interface.t
    
```

```

0x00a0: 756e 6e65 6c36 2069 7320 646f 776e 2072 unnel6.is.down.r
0x00b0: 6561 736f 6e20 4465 7374 696e 6174 696f eason.Destinatio
0x00c0: 6e20 756e 7265 6163 6861 626c 650a n.unreachable.

```

Reference Material

- **Cisco APIC Faults, Events, and System Messages Management Guide**
http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/faults/guide/b_APIC_Faults_Errors.html
- **Cisco ACI System Messages Reference Guide**
http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/syslog/guide/aci_syslog/About.html
- **ACI System Messages**
http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/syslog/guide/aci_syslog/ACI_SysMsg.pdf

Class syslog:Group (CONCRETE)

Class ID:1719
Class Label: Syslog Monitoring Destination Group
Encrypted: false - **Exportable:** true - **Persistent:** true - **Configurable:** true
Write Access: [admin]
Read Access: [admin, fabric-protocol-ops, ops]
Semantic Scope: Fabric
Semantic Scope Evaluation Rule: Parent
Monitoring Policy Source: Parent
Monitoring Flags : [IsObservable: true, HasStats: false, HasFaults: false, HasHealth: true]

The syslog destination group, which contains all information required to send syslog messages to a group of destinations.

Class syslog:RemoteDest (CONCRETE)

Class ID:1716
Class Label: Syslog Remote Destination
Encrypted: false - **Exportable:** true - **Persistent:** true - **Configurable:** true
Write Access: [admin]
Read Access: [admin, ops]
Semantic Scope: Fabric
Semantic Scope Evaluation Rule: Parent
Monitoring Policy Source: Parent
Monitoring Flags : [IsObservable: true, HasStats: false, HasFaults: false, HasHealth: true]

The syslog remote destination host enables you to specify syslog servers to which messages from the APIC and fabric nodes should be forwarded.

Class syslog:Prof (CONCRETE)

Class ID:1712
Class Label: Protocol Profile
Encrypted: false - Exportable: true - Persistent: true - Configurable: true
Write Access: [admin]
Read Access: [admin, ops]
Semantic Scope: Fabric
Semantic Scope Evaluation Rule: Parent
Monitoring Policy Source: Parent
Monitoring Flags : [IsObservable: false, HasStats: false, HasFaults: false, HasHealth: false]

Represents the configuration parameters used for this protocol.

Class syslog:RtDestGroup (CONCRETE)

Class ID:1715
Class Label: Syslog Source
Encrypted: false - Exportable: false - Persistent: true - Configurable: false
Relationship Type: explicit
Relationship Cardinality: n-to-1
Relationship From: [syslog:Src](#)
Relationship From Rel: [syslog:RsDestGroup](#)
Relationship To: [syslog:Group](#)
Relationship To Rel: [syslog:RtDestGroup](#)
Enforceable: true
Resolvable: true
Write Access: [NON CONFIGURABLE]
Read Access: [admin, fabric-protocol-ops, ops]
Semantic Scope: Fabric
Semantic Scope Evaluation Rule: Parent
Monitoring Policy Source: Parent
Monitoring Flags : [IsObservable: false, HasStats: false, HasFaults: false, HasHealth: false]

A target relation to the syslog destination group.

End of Document