Accenture MDR Quick Start Guide for Cisco® Nexus™ and Cisco® APIC™

This quick start guide will help Accenture MDR customers configure Cisco® Nexus™ to send logs to the Log collection Platform (LCP).

The document includes the following topics:

Supported Versions

A list of supported versions is available in the Accenture MDR Supported Products List document *(Accenture_MDR_Supported_Products_List.*xlsx*)* which can be found in Accenture MDR Portal.

Port Requirements

Table 1-1: Port requirements for LCP communication.

Source	Destination	Port	Description
Cisco Nexus	LCP	514 (UDP)	Default port
Cisco APIC	LCP	6514 (TCP) or 514 (UDP) or 601 (TCP)	Default port

Configuring Cisco Nexus

To configure Cisco Nexus to send syslog messages to the LCP, follow the steps below.

Note: You can configure up to three syslog servers to forward logs to remote systems.

Connect the Virtual Device Context (VDC).

1. Login to the CLI.
2. To view all the VDCs, enter the command: show vdc
3. To view the existing VDC, enter the command: show vdc current-vdc
4. To change the VDC, enter the command: switchto vdc

Configure Cisco Nexus in CLI.

1. Login to the CLI.
2. Enter the following commands in the same sequence:

   switch# *configure terminal*

   switch(config)# *logging server <lcp_ip_address> <severity-level> use-vrf <vrf-name> facility <local7>*

   switch# *copy running-config startup-config*

Note:

- Please refer the vendor documentation for more information on severity levels.

- The use vrf vrf-name keyword argument identifies the default or management values for the VRF name. If a specific VRF is not identified, management is the default value. However, if management is configured, it will not be listed in the output of the *show-running* command because it is the default value. If a specific VRF is configured, the *show-running* command output will list the VRF for each server.

```
Nexus-7000# show vdc

Switchwide mode is m1 f1 m1x1 f2 m2x1 f2e

vdc_id  vdc_name                        state            mac               type        lc
------  --------                        -----            ----------        ----------  ------
1       Nexus-7000                      active           d8:67:d9:09:09:c1 Admin       None
2       MyVDC                           active           d8:67:d9:09:09:c2 Ethernet    f2 f2e

Nexus-7000# show vdc current-vdc
Current vdc is 1 - Nexus-7000
Nexus-7000# switchto vdc MyVDC
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2013, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
Nexus-7000-MyVDC# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Nexus-7000-MyVDC(config)# logging server 192.0.2.0 5 use-vrf default facility local7
Nexus-7000-MyVDC(config)# copy running-config startup-config
[########################################] 100%
Copy complete.
Nexus-7000-MyVDC(config)#
```

Note:

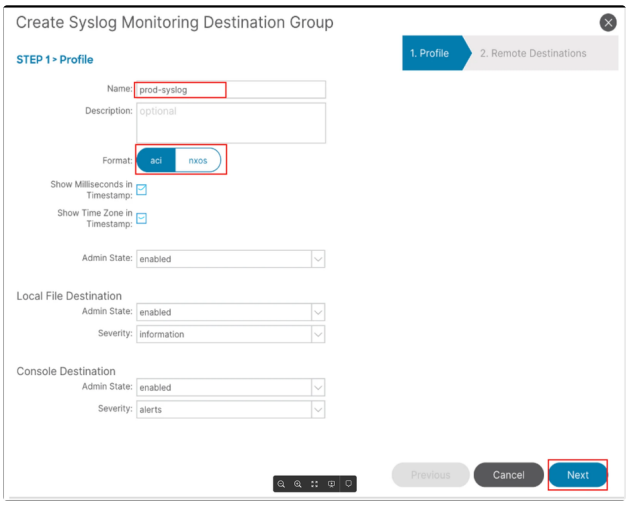
- Cisco Nexus configuration does not provide any option to configure logging through TCP and/or a non-standard port even though collector support has been provided.
- When Cisco Nexus is configured to forward logs to the LCP through ArcSight SmartConnector, the logging device IP is the IP of the ArcSight SmartConnector.
- When multiple Cisco Nexus switches forward logs through the same ArcSight SmartConnector, the logs gathered from all the switches will have the IP of ArcSight SmartConnector as the logging device IP.
- The Cisco Nexus collector supports log forwarding from ArcSight Smart connector. Please contact a Accenture MDR onboarding engineer if you need assistance with the configuration.

Device configuration for Cisco APIC

1. Creating a **Syslog Destination and Destination Group:**
   a. In the menu bar, click **Admin**.
   b. In the submenu bar, click **External Data Collectors**.
   c. In the **Navigation** pane, expand **Monitoring Destinations**.
   d. Right-click **Syslog** and choose **Create Syslog Monitoring Destination Group**.
   e. In the **Create Syslog Monitoring Destination Group** dialog box, perform the following actions:
      i. In the group and profile **Name** field, enter a name for the monitoring destination group and profile.
      ii. In the group and profile **Format** field, choose the format for Syslog messages. The default value is “**aci**”, you need to use the default value.
      iii. Enable "Show Milliseconds in Timestamp" and "Show time Zone in Timestamp".
      iv. In the group and profile **Admin State** drop-down list, choose **enabled**.
      v. To enable sending of syslog messages to a local file, choose **enabled** from the Local File Destination **Admin State** drop-down list and choose a minimum severity from the Local File Destination **Severity** drop-down list. Choose **severity** as “**Information”.**

vi. To enable sending of syslog messages to the console, choose **enabled** from the Console Destination **Admin State** drop-down list and choose a minimum severity from the Console Destination **Severity** drop-down list. Choose **severity** as "**Alerts**".

vii. Click **Next.**



2. **In the Create Syslog Remote Destination dialog box, perform the following actions:**

a. In the **Host** field, enter an "**LCP IP"** or a fully qualified domain name for the destination host.

b. (Optional) In the **Name** field, enter a name for the destination host.

c. In the **Admin State** field, click the **enabled** radio button.

d. Select **severity** as "**warning".**

e. Select **transport** as ***ssl***

f. Select **port** as ***6514***

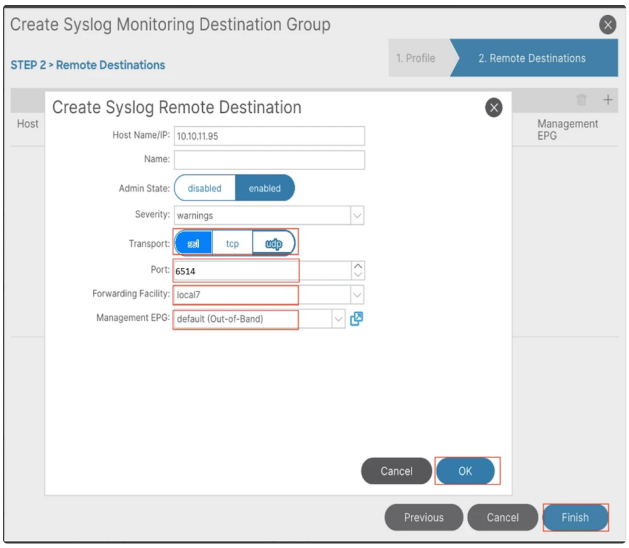
Note - You can use **transport** as **tcp**, have to mention **port** as **601** and use **transport** as **UDP**, have to mention **port** as **514.**

g. Select **Forwarding Facility** as **local7**.

h. Select **Management EPG** as **default(out-of-band)**.

i. Click **OK** & **Finish**.

j. Path to upload certificate - **Admin** > **AAA** > **Security** > **Public Key Management** > **Certificate Authorities**, then **Actions** > **Create Certificate Authority**



3. **Creating a Syslog Source:**

a. Under **Fabric > Fabric Policies > Monitoring Policies > Common Policy**

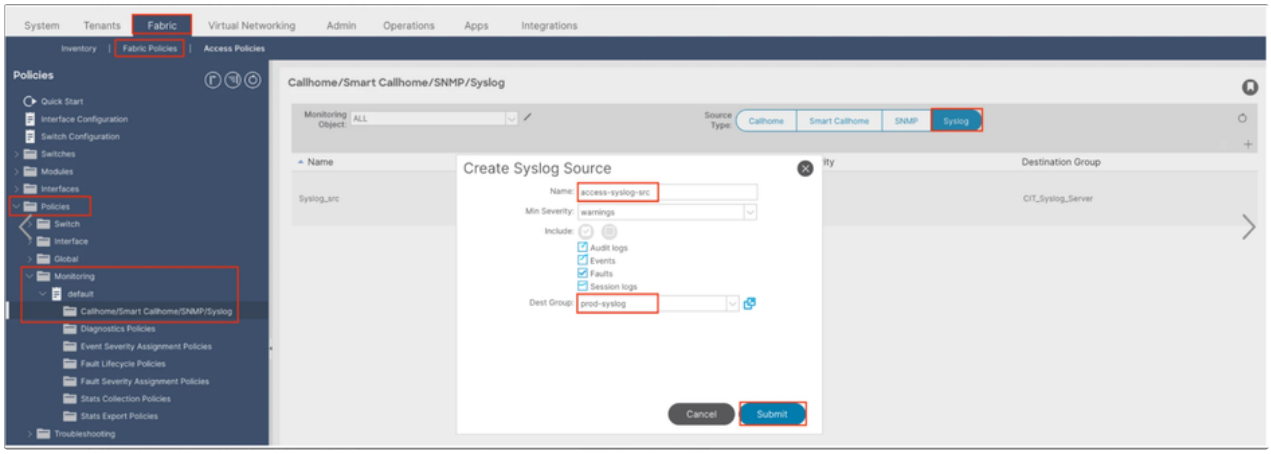
b. Under the Common policy, click **Callhome/Smart Callhome/SNMP/Syslog**

c. In the **Work** pane, choose **Syslog** from the **Source Type** drop-down list.

d. From the **Monitoring Object** list, select "**All**"

e. In a tenant monitoring policy, select "**All**"

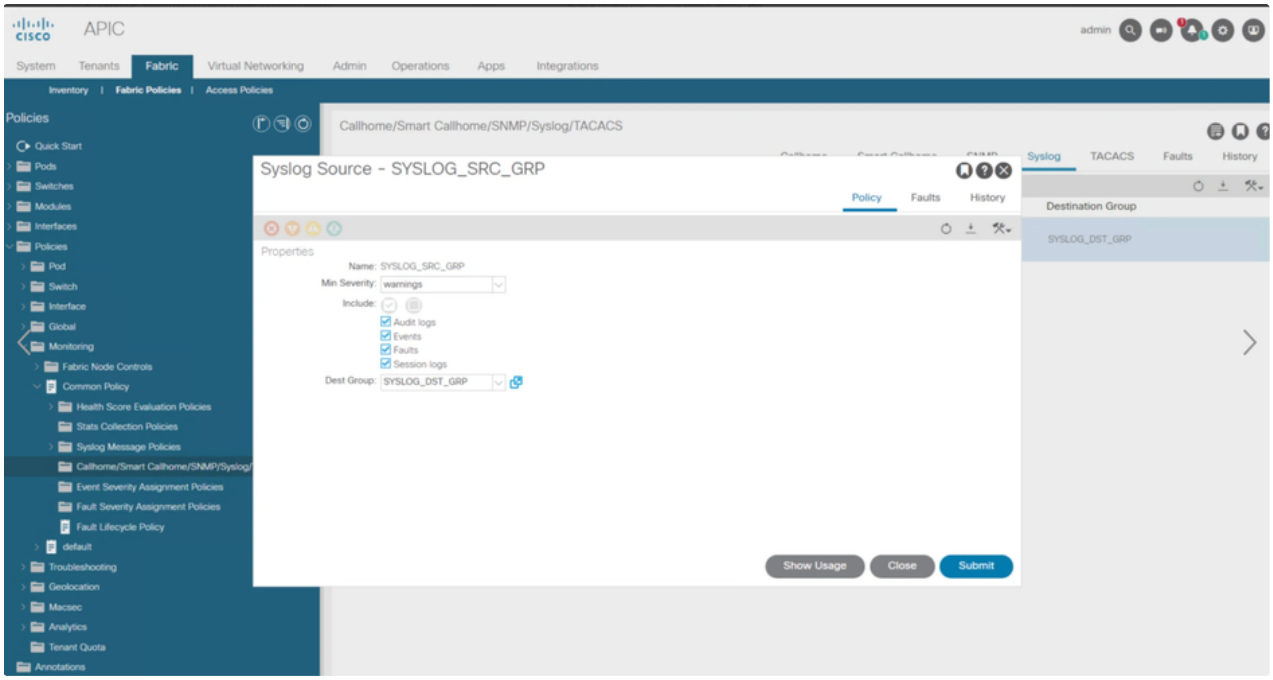
f. Click **+** to create a syslog source.



g. Enter a **name** for the syslog source.

h. Select the minimum severity as "**Warning"** from drop-down list.

i. Select all type of messages to sent to syslog server(Audit logs, Events, Faults, Session logs).



j. Select **Dest Group** which you have created in step 1 & 2.

k. Click **Submit.**

LCP Configuration Parameters

Table 1-2: The Cisco Nexus and Cisco APCI event collector (Syslog -3734) properties to be configured by MDR are shown in the table.

Property	Default Value	Description
Protocol	UDP	The default protocol for syslog.

		Note: Cisco Nexus does not support TCP. Enable the TCP port only if CISCO APIC logs receiving in TCP port.
IP Address	Cisco Nexus and Cisco APIC Interface IP Address	Logging device IP address mentioned in the Pre-Installation Questionnaire (PIQ).
Signatures	%LOG_LOCAL,%STM,%IGMP,%FWM,%VPC,%VTP,%VLAN_MGR,%PVLAN,%SVI,%FCS,%SFP,%GLBP,%HSRP,%VRRP_CFG,%VRRP-NG,%VRRP_MGR,%VRRP_ENG,%EIGRP,%OSPF,%BGP,%PIM,%MSDP,%SSM,%AAA,%ACL,%CLTCAM,%ACLQOS,%ACLLOG,%ACLMGR,%DHCP_SNOOP,%ARP,%RADIUS,%TACACS,%DO1X,%IPACL,%SSH,%DIAGMGR,%SNMP,%SNMPD,%CTS,%MPLS,%ISSU,%SYSMGR,%CMPPRXY,%EOBC,%EPLD_UPGRADE,%PSS,%CFS,%MTS,%VSAN,%CDP,%SPAN,%STP,%NPV,%FCE_MGR,%FCOE,%QoS,%VEM_MGR,%VMS,%VEM,%BFDC,%BFD,%CERT_ENROLL,%PORT,%THPORT,%ASSOC_MGR,%CALL_HOME,%LLDP,%USER,%AUTH,%LOCAL7,%LICMGR,%MCASFWD,%SECURITYD,%MONITOR,%KERN,%FEX,%UDLD,%PLATFORM,%IM,%CARDCLIENT,%MDULE,%BIOS_DAEMON,%PIXM,%VDC_MGR,%ISIS_FABRICPATH,%ASCII,%ETH_PORT_CHANEL,%AMM,%NETSTACK,%FEATURE,%PFMA,%SENSOR,%CALLHOME,%VSHD_SYSLOG_CONIG_I,%AUTHPRIV,%DAEMON,%BOOTVAR,%L3VM,%SYSLOG,%NOHMS,%SATCTRL	MDR recommended signatures processed by the Cisco Nexus event collector.
Port Number	514	The default port for UDP. **Note:** 1. Cisco Nexus supports only 514 to send logs. 2. Cisco APIC supports bith TCP and UDP.