Configure Syslog Server on Wireless LAN Controllers

Contents

Introduction

This document describes how to configure the Wireless LAN Controller for syslog servers.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Knowledge of how to configure the Wireless LAN Controller (WLC) and Lightweight Access Point (LAP) for basic operation.
- Basic knowledge of Control And Provisioning of Wireless Access Point (CAPWAP) protocol.

Components Used

The information in this document is based on these software and hardware versions:

- Wireless LAN Controllers running AireOS 8.8.111.0 Software.
- Wave 1 APs: 3500,1600/2600/3600 (these are limited to 8.5 software version and can miss some of the next features that were added afterwards),1700/2700/3700.
- Wave 2 APs: 1800/2800/3800/4800, 1540 and 1560.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Information About Syslog on WLCs

System logging allows controllers to log their system events to up to three remote syslog servers.

The WLC sends a copy of each syslog message as it is logged to each syslog server configured on the controller.

Being able to send the syslog messages to multiple servers ensures that the messages are not lost due to the temporary unavailability of one syslog server.

Message logging allows system messages to be logged to the controller buffer or console.

For more information about system messages and trap logs, see Error and System Messages

Syslog on APs

As from AireOS 8.4 you have the ability to disable syslog server per AP and/or global via the WLC CLI.

On version 8.8 it was introduced the support for syslog facility on Wave 2 APs.

Configure

You can enable and configure the controller to log system events to up to three remote syslog servers. The controller sends a copy of each syslog message as it is logged to each syslog server configured on the controller. Because it is able to send the syslog messages to multiple servers, it ensures that the messages are not lost due to the temporary unavailability of one syslog server.

This type of configuration helps in these situations:

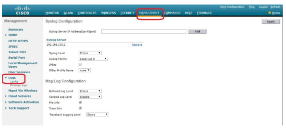
- One of the configured syslog servers is not available.
- Multiple administrator groups can monitor different message types.
- Large deployments can want syslog messages sent to servers across different time-zones for extended visibility.

Note: Syslog messages are sent on UDP Port 514; additional server configuration can require a proper configuration of firewall rules.

Note: When a primary WLC port link goes down, messages can get logged internally only and not be posted to a syslog server. It can take up to 40 seconds to restore logging to the syslog server.

Configurations of Syslog on WLC (GUI)

Step 1. Go to **Management > Logs > Config**. The Syslog Configuration page appears:



Syslog Configuration

Syslog Server IP Address(Ipv4/Ipv6)

Syslog Server

192.168.100.2

Syslog Level: Errors

Syslog Facility: Local Use 0

IPSec: □

IPSec Profile Name: none

Msg Log Configuration

Buffered Log Level: Errors

Console Log Level: Disable

File Info: ☑

Trace Info: ☑

Traceback Logging Level: Errors

Step 2. Enter the **Syslog Server IP Address** and click **Add.** You can add up to three syslog servers to the controller. The list of syslog servers that have already been added to the controller appears under this text box. If you want to remove a syslog server from the controller, click **Remove** to the right of the desired server.

Step 3. To set the **Syslog Level** (severity) for filtering syslog messages to the syslog servers, choose one of the next options from the **Syslog Level** drop-down list:

- **Emergencies**= Severity level 0
- **Alerts**= Severity level 1 (default value)
- **Critical**= Severity level 2
- **Errors**= Severity level 3
- **Warnings**= Severity level 4
- **Notifications**= Severity level 5
- **Informational**= Severity level 6
- **Debugging**= Severity level 7

If you set a syslog level, only those messages whose severity is equal to or less than that level are sent to the syslog servers. For example, if you set the syslog level to Notifications (severity level 5), only those messages whose severity is betwen 0 and 5 are sent to the syslog servers.

Note: If you have enabled logging of **Debugging** messages to the logging buffer, some messages from application debug could be listed in message log with severity that is more than the level set. For example, if you execute the `debug client mac-addr` command, the client event log could be listed in message log even though the message severity level is set to **Errors**.

Step 4. To set the **Syslog Facility** for outgoing syslog messages to the syslog servers, choose one of these options from the **Syslog Facility** drop-down list:

- **Kernel**= Facility level 0
- **User Process**= Facility level 1
- **Mail**= Facility level 2
- **System Daemons**= Facility level 3
- **Authorization**= Facility level 4
- **Syslog** = Facility level 5 **(default value)**
- **Line Printer**= Facility level 6
- **USENET**= Facility level 7
- **Unix-to-Unix Copy**= Facility level 8
- **Cron**= Facility level 9
- **FTP Daemon**= Facility level 11
- **System Use 1**= Facility level 12
- **System Use 2**= Facility level 13
- **System Use 3**= Facility level 14
- **System Use 4**= Facility level 15
- **Local Use 0**= Facility level 16
- **Local Use 2**= Facility level 17
- **Local Use 3**= Facility level 18
- **Local Use 4**= Facility level 19
- **Local Use 5**= Facility level 20
- **Local Use 5**= Facility level 21
- **Local Use 5**= Facility level 22
- **Local Use 5** = Facility level 23

For example, selecting **Kernel** makes only kernel related messages to be sent. **Authorization**, makes only

AAA related messages to be sent, and so on.

Step 5. Click **Apply**.

Configuring Syslog on WLC (CLI)

Step 1. Enable system logging and set the IP address of the syslog server to which to send the syslog messages by entering this command:

```
(Cisco Controller) >config logging syslog host server_IP_address
```

Step 2. To remove a syslog server from the controller by entering this command:

```
(Cisco Controller) >config logging syslog host server_IP_address delete
```

Step 3. Set the severity level for filtering syslog messages to the syslog server by entering this command:

```
(Cisco Controller) >config logging syslog level severity_level
```

Note: As **severity_level** you can enter the word or number. For example: **debugging** or **7**.

Sending WLC CLI Debugs to Syslog Server

Using this command the WLC logs the debug output to the syslog server. However, if the CLI session is terminiated, the debug ends and there is no more output sent to the syslog server.

```
(Cisco Controller) >config logging debug syslog enable
```

Configuring Syslog for APs From the WLC (CLI only)

Step 1.To configure the syslog server ip address, you must use the CLI. You can set the ip address globaly for all APs or for a specific AP.

```
(Cisco Controller) >config ap syslog host ?
```

```
global        Configures the global system logging host for all Cisco AP
specific      Configures the system logging host for a specific Cisco AP.

(Cisco Controller) >config ap syslog host global ?

<ip_address> IP address of the global system logging host for all Cisco AP

(Cisco Controller) >config ap syslog host global 10.0.0.1
Setting the AP Global Syslog host will overwrite all AP Specific Syslog host configurations!
Are you sure you would like to set the AP Global Syslog host? (y/n) y


AP Global Syslog host has been set.

(Cisco Controller) >show ap config global

AP global system logging host.................... 10.0.0.1
AP global system logging level................... debugging
AP Telnet Settings............................... Globally Configured (Disabled)
AP SSH Settings.................................. Globally Configured (Disabled)
Diminished TX power Settings..................... Globally Configured (Disabled)
```

Step 2. Via the CLI we can also set the syslog and severity level for filtering syslog messages for a particular access point or for all access points by entering these commands:

```
(Cisco Controller) >config ap logging syslog level severity_level
```

Note: As **severity_level** you can enter the word or number. For example: **debugging**or *7*.

Step 3. Set the facility for outgoingsyslogmessages to thesyslogserver by entering this command:

```
(Cisco Controller) >config logging syslog facility facility-code
```

where facility-code is one of these:

- **ap** = AP related traps.

- au**t**horization = Authorization system. Facility level = 4.

- **auth-private** = Authorization system (private). Facility level = 10.
- **cron** = Cron/at facility. Facility level = 9.
- **daemon** = System daemons. Facility level = 3.
- **ftp** = FTP daemon. Facility level = 11.
- **kern** = Kernel. Facility level = 0.
- **local0** = Local use. Facility level = 16.
- **local1** = Local use. Facility level = 17.
- **local2** = Local use. Facility level = 18.
- **local3** = Local use. Facility level = 19.

- **local4** = Local use. Facility level = 20.
- **local5** = Local use. Facility level = 21.
- **local6** = Local use. Facility level = 22.
- **local7** = Local use. Facility level = 23.
- **lpr** = Line printer system. Facility level = 6.
- **mail** = Mail system. Facility level = 2.
- **news** = USENET news. Facility level = 7.
- **sys12** = System use. Facility level = 12.
- **sys13** = System use. Facility level = 13.
- **sys14** = System use. Facility level = 14.
- **sys15** = System use. Facility level = 15.
- **syslog**= Thesyslogitself. Facility level = 5.
- **user** = User process. Facility level = 1.
- **uucp** = Unix-to-Unix copy system. Facility level = 8.

Step 3. Configure the syslog facility for AP using the next command:

```
(Cisco Controller) >config logging syslog facility AP
```

where AP can be:

- **associate =** Associated syslog for AP.
- **disassociate =** Disassociate syslog for AP.

Step 4. Configure the syslog facility for an AP or all APs by entering this command:

```
(Cisco Controller) >config ap logging syslog facility facility-level {Cisco_AP| all}
```

where **facility-level** is one of these:

- **auth** = Authorization system
- **cron** = Cron/at facility
- **daemon** = System daemons
- **kern** = Kernel
- **local0** = Local use
- **local1** = Local use
- **local2** = Local use
- **local3** = Local use
- **local4** = Local use
- **local5** = Local use
- **local6** = Local use
- **local7** = Local use
- **lpr** = Line printer system
- **mail** = Mail system
- **news** = USENET news
- **sys10** = System use
- **sys11** = System use
- **sys12** = System use

- **sys13** = System use
- **sys14** = System use
- **sys9** = System use
- **syslog** = Syslog itself
- **user** = User process
- **uucp** = Unix-to-Unix copy system

Configuring Syslog on FlexConnect Access Points

FlexConnect client-based debugging allows client-specific debugging to be enabled for an AP or groups of APs. It also allows syslog server configuration to log the debug messages.

Using FlexConnect client-based debugging:

- You can debug client connectivity issue of AP by entering a particular MAC address of a client from either WLC or AP console.
- You can debug client connectivity issue across FlexConnect site without entering debug commands on multiple APs or enabling multiple debugs. A single debug command enables the debugs.
- You need not enter debug command on multiple APs depending on where the client can roam to. By applying debug at the FlexConnect group level, all APs that are part of the FlexConnect group get this debug request.
- The logs are collected centrally at syslog server by providing the IP address of the server from the WLC.
- If you configure a FlexConnect access point with a syslog server configured on the access point, after the access point is reloaded and the native VLAN other than 1, at time of initialization, few syslog packets from the access point are tagged with VLAN ID 1. This is a known issue.

Note: The AP driver debugs are not enabled on the WLC. If you have access to the AP console, the driver debugs can be enabled.

These are the debugging commands on the WLC CLI:

```
(Cisco Controller) >debug flexconnect client ap ap-name{add|delete}mac-addr1 mac-addr2 mac-addr3 mac-ad
(Cisco Controller) >debug flexconnect client apap-namesyslog{server-ip-address|disable}
(Cisco Controller) >debug flexconnect client groupgroup-name{add|delete}mac-addr1 mac-addr2 mac-addr3 m
(Cisco Controller) >debug flexconnect client groupgroup-namesyslog{server-ip-address|disable}
(Cisco Controller) >show debug
```

The debugging commands that can be entered on the AP console are listed here. These commands are applicable for debugging the client AP console when it is accessible. If you enter these commands on the AP console, the commands are not communicated to the WLC.

```
AP#[no]debug condition mac-address mac-addr
AP#[no]debug dot11 client
```

Restrictions

- AP configuration is not saved across reboots.
- Adding an AP to and deleting an AP from a FlexConnectGroup impacts the AP FlexConnect debug state.

Note: It is not possible to change the syslog port being used.

Verify

To verify the syslog configuration on CLI enter the command **show logging**.

<#root>

```
(Cisco Controller) >show logging

Logging to Logger Queue :

- Logging of system messages to Logger Queue :
 - Effective Logging Queue filter level.......... debugging
- Number of Messages recieved for logging :
 - Emergency severity............................ 0
 - Alert Severity................................ 0
 - Critical Severity............................. 0
 - Error Severity................................ 9
 - Warning Severity.............................. 6
 - Notice Severity............................... 210
 - Information Severity.......................... 8963
 - Debug Severity................................ 5
 - Total messages recieved....................... 9193
 - Total messages enqueued....................... 2815
 - Total messages dropped........................ 6378
Logging to buffer :
- Logging of system messages to buffer :
 - Logging filter level.......................... errors
 - Number of system messages logged.............. 9
 - Number of system messages dropped.............
- Number of Messages dropped due to Facility .... 09195
- Logging of debug messages to buffer ........... Disabled
 - Number of debug messages logged............... 0
 - Number of debug messages dropped.............. 0
- Cache of logging ............................. Disabled
- Cache of logging time(mins) ................... 10080
- Number of over cache time log dropped ........ 0
Logging to console :
- Logging of system messages to console :
 - Logging filter level.......................... disabled
 - Number of system messages logged.............. 0
 - Number of system messages dropped............. 9204
 - Number of system messages throttled........... 0
- Logging of debug messages to console .......... Enabled
 - Number of debug messages logged............... 0
 - Number of debug messages dropped.............. 0
 - Number of debug messages throttled............ 0

Logging to syslog :

- Syslog facility................................ local0

- Logging of system messages to syslog :

 - Logging filter level.......................... debugging

 - Number of system messages logged.............. 2817

 - Number of system messages dropped............. 6387

- Logging of debug messages to syslog ........... Disabled

 - Number of debug messages logged............... 0

 - Number of debug messages dropped.............. 0
- Number of remote syslog hosts.................. 1

- syslog over tls................................ Disabled

- syslog over ipsec.............................. Disabled

- ipsec profile inuse for syslog................. none

 - Host 0....................................... 192.168.100.2

 - Host 1.......................................

 - Host 2.......................................
```

```
Logging of Debug messages to file :
- Logging of Debug messages to file.............. Disabled
- Number of debug messages logged................ 0
- Number of debug messages dropped............... 0
Logging of traceback............................. Enabled
- Traceback logging level........................ errors
Logging of source file informational............. Enabled
Timestamping of messages.........................
- Timestamping of system messages................ Enabled
 - Timestamp format.............................. Date and Time
- Timestamping of debug messages................. Enabled
 - Timestamp format.............................. Date and Time

[...]

(Cisco Controller) >
```

To see the global syslog server settings for all access points that join the controller by entering this command: **show ap config global**.

Information similar to this next text appears:

```
AP global system logging host.................... 10.0.0.1
```

To display the AP-specificsyslogserver settings for an AP use the command **show ap config generalap-name**.

Example:

<#root>

```
(Cisco Controller) >show ap config general testAP

Cisco AP Identifier............................... 1
Cisco AP Name..................................... testAP
[...]
Remote AP Debug .................................. Disabled

Logging trap severity level ...................... informational


KPI not configured ...............................

Logging syslog facility .......................... kern


S/W Version ..................................... 8.8.111.0
[...]
```

Related Information

- Cisco Wireless Controller Configuration Guide, Release 8.8
- Cisco Technical Support & Downloads