

Configuración del servidor Syslog en controladores LAN inalámbricos

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Información sobre Syslog en WLC](#)

[Syslog en AP](#)

[Configurar](#)

[Configuraciones de Syslog en WLC \(GUI\)](#)

[Configuración de Syslog en WLC \(CLI\)](#)

[Envío de depuraciones CLI de WLC al servidor Syslog](#)

[Configuración de Syslog para APs desde el WLC \(sólo CLI\)](#)

[Configuración de Syslog en puntos de acceso FlexConnect](#)

[Restricciones](#)

[Verificación](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar el Wireless LAN Controller para los servidores syslog.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento de cómo configurar el controlador de LAN inalámbrica (WLC) y el punto de acceso ligero (LAP) para un funcionamiento básico.
- Conocimiento básico del protocolo de control y aprovisionamiento de puntos de acceso inalámbricos (CAPWAP).

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Controladores de LAN inalámbrica que ejecutan el software AireOS 8.8.111.0.

- AP de onda 1: 3500.1600/2600/3600 (limitados a la versión de software 8.5 y que pueden pasar desapercibidos algunas de las siguientes funciones añadidas posteriormente).1700/2700/3700.
- AP de onda 2: 1800/2800/3800/4800, 1540 y 1560.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Información sobre Syslog en WLC

El registro del sistema permite a los controladores registrar sus eventos del sistema en hasta tres servidores syslog remotos.

El WLC envía una copia de cada mensaje syslog cuando se registra en cada servidor syslog configurado en el controlador.

El poder enviar los mensajes de syslog a varios servidores garantiza que los mensajes no se pierdan debido a la indisponibilidad temporal de un servidor de syslog.

El registro de mensajes permite que los mensajes del sistema se registren en el buffer del controlador o en la consola.

Para obtener más información acerca de los mensajes del sistema y los registros de capturas, vea [Mensajes de error y del sistema](#)

Syslog en AP

A partir de AireOS 8.4 usted tiene la capacidad de inhabilitar el servidor syslog por AP y/o global vía el WLC CLI.


En la versión 8.8 se introdujo el soporte para la función syslog en los AP de Wave 2.


Configurar

Puede habilitar y configurar el controlador para registrar eventos del sistema en hasta tres servidores syslog remotos. El controlador envía una copia de cada mensaje syslog cuando se registra en cada servidor syslog configurado en el controlador. Dado que puede enviar los mensajes de syslog a varios servidores, garantiza que los mensajes no se pierdan debido a la indisponibilidad temporal de un servidor de syslog.

Este tipo de configuración ayuda en las siguientes situaciones:

- Uno de los servidores syslog configurados no está disponible.
- Varios grupos de administradores pueden supervisar distintos tipos de mensajes.
- Las grandes implementaciones pueden desear que los mensajes de registro del sistema se envíen a los servidores en diferentes zonas horarias para obtener una mayor visibilidad.

 Nota: los mensajes de Syslog se envían en el puerto UDP 514; la configuración adicional del servidor puede requerir una configuración adecuada de las reglas del firewall.

 Nota: Cuando un link de puerto WLC primario deja de funcionar, los mensajes pueden registrarse internamente solamente y no ser publicados en un servidor syslog. Puede tardar hasta 40 segundos en restaurar el registro en el servidor syslog.

Configuraciones de Syslog en WLC (GUI)


Paso 1. Vaya a Management > Logs > Config. Aparecerá la página Configuración de Syslog: 

Paso 2. Ingrese la dirección IP del servidor Syslog y haga clic en Agregar. Puede agregar hasta tres servidores syslog al controlador. La lista de servidores syslog que ya se han agregado al controlador aparece debajo de este cuadro de texto. Si desea quitar un servidor syslog del controlador, haga clic en Remove a la derecha del servidor deseado.

Paso 3. Para establecer el nivel de registro del sistema (gravedad) para filtrar los mensajes de registro del sistema a los servidores de registro del sistema, elija una de las siguientes opciones de la lista desplegable Nivel de registro del sistema:

- Emergencias= nivel de gravedad 0
- Alertas= nivel de gravedad 1 (valor predeterminado)
- Crítico= nivel de gravedad 2
- Errores= nivel de gravedad 3
- Advertencias= Nivel de gravedad 4
- Notifications= Nivel de gravedad 5
- Informativo= nivel de gravedad 6
- Depuración= nivel de gravedad 7

Si establece un nivel de syslog, sólo se envían a los servidores de syslog los mensajes cuya gravedad sea igual o inferior a dicho nivel. Por ejemplo, si establece el nivel de registro del sistema en Notificaciones (nivel de gravedad 5), sólo se enviarán a los servidores de registro del sistema los mensajes cuya gravedad esté entre 0 y 5.

 Nota: Si ha habilitado el registro de los mensajes de depuración en el búfer de registro, algunos mensajes de depuración de la aplicación podrían aparecer en el registro de mensajes con una gravedad superior al nivel establecido. Por ejemplo, si ejecuta el `debug client mac-addr` comando, el registro de eventos del cliente podría aparecer en el registro de mensajes aunque el nivel de gravedad del mensaje esté establecido en **Errores**.

Paso 4. Para configurar la **Utilidad Syslog** para los mensajes syslog salientes en los servidores syslog, elija una de estas opciones de la lista desplegable **Utilidad Syslog**:

- **Kernel**= nivel de servicio 0
- **Proceso de usuario**= nivel de instalación 1
- **Mail**= nivel 2 de instalación
- **Demonios del sistema** = nivel de instalación 3
- **Autorización** = Nivel de instalación 4
- **Syslog** = Nivel de instalación 5 (**valor predeterminado**)
- **Impresora de línea** = nivel de instalación 6
- **USENET**= Nivel de instalación 7
- **Unix-to-Unix Copy**= Nivel de instalación 8
- **Cron**= nivel de instalación 9
- **FTP Daemon**= nivel de servicio 11
- **Uso del sistema 1**= nivel de instalación 12
- **Uso del sistema 2**= nivel de instalación 13
- **Uso del sistema 3**= nivel de instalación 14
- **Uso del sistema 4**= nivel de instalación 15
- **Uso local 0**= nivel de instalación 16
- **Uso local 2**= nivel de instalación 17
- **Uso local 3**= nivel de instalación 18
- **Uso local 4**= nivel de instalación 19
- **Uso local 5**= nivel de instalación 20
- **Uso local 5**= nivel de instalación 21
- **Uso local 5**= nivel de instalación 22
- **Uso local 5** = Nivel de instalación 23

Por ejemplo, al seleccionar **Kernel** sólo se envían mensajes relacionados con el núcleo. **Autorización**, hace que sólo se envíen mensajes relacionados con AAA, y así sucesivamente.

Paso 5. Haga clic en Apply (Aplicar).

Configuración de Syslog en WLC (CLI)

Paso 1. Habilite el registro del sistema y establezca la dirección IP del servidor syslog al cual enviar los mensajes syslog ingresando este comando:

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

Paso 2. Para quitar un servidor syslog del controlador ingresando este comando:

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

Paso 3. Establezca el nivel de gravedad para filtrar mensajes de syslog en el servidor de syslog ingresando este comando:

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

Nota: Como `severity_level`, puede introducir la palabra o el número. Por ejemplo: **debugging** o **7**.

Envío de depuraciones CLI de WLC al servidor Syslog

Con este comando, el WLC registra la salida de depuración en el servidor syslog. Sin embargo, si se termina la sesión CLI, la depuración finaliza y no se envía más salida al servidor syslog.

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

Configuración de Syslog para APs desde el WLC (sólo CLI)

Paso 1. Para configurar la dirección IP del servidor syslog, debe utilizar la CLI. Puede establecer la dirección IP globalmente para todos los AP o para un AP específico.

```
(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)
```

Paso 2. A través de la CLI, también podemos establecer el syslog y el nivel de gravedad para filtrar los mensajes de syslog para un punto de acceso determinado o para todos los puntos de acceso mediante la introducción de estos comandos:

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



Nota: Como **severity_level**, puede introducir la palabra o el número. Por ejemplo: debugging or 7.

Paso 3. Establezca el recurso para outgoing syslog messages en the syslog server ingresando este comando:

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

donde facility-code es uno de estos:

•

ap = Trampas relacionadas con AP.

•

authorization = Sistema de autorización. Nivel de instalación = 4.

• **auth-private** = Sistema de autorización (private). Nivel de instalación = 10.

• **cron** = instalación de cron/at. Nivel de instalación = 9.

• **daemon** = demonios del sistema. Nivel de instalación = 3.

• **ftp** = demonio FTP. Nivel de instalación = 11.

• **kern** = Kernel. Nivel de instalación = 0.

• **local0** = Uso local. Nivel de instalación = 16.

• **local1** = uso local. Nivel de instalación = 17.

• **local2** = Uso local. Nivel de instalación = 18.

• **local3** = Uso local. Nivel de instalación = 19.

• **local4** = Uso local. Nivel de instalación = 20.

• **local5** = Uso local. Nivel de instalación = 21.

• **local6** = Uso local. Nivel de instalación = 22.

• **local7** = Uso local. Nivel de instalación = 23.

• **lpr** = Sistema de impresora de línea. Nivel de instalación = 6.

• **mail** = Sistema de correo. Nivel de instalación = 2.

• **news** = Noticias USENET. Nivel de instalación = 7.

• **sys12** = Uso del sistema. Nivel de instalación = 12.

• **sys13** = Uso del sistema. Nivel de instalación = 13.

• **sys14** = Uso del sistema. Nivel de instalación = 14.

• **sys15** = Uso del sistema. Nivel de instalación = 15.

• **syslog** = El propio syslog. Nivel de instalación = 5.

• **user** = Proceso de usuario. Nivel de instalación = 1.

- **uucp** = sistema de copia de Unix a Unix. Nivel de instalación = 8.

Paso 3. Configure la utilidad syslog para el AP usando el siguiente comando:

(Cisco Controller) >config logging syslog facility AP

donde AP puede ser:

- **associate** = Registro del sistema asociado para AP.
- **disassociate** = Disociar syslog para AP.

Paso 4. Configure la utilidad syslog para un AP o todos los AP ingresando este comando:

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

donde **nivel de instalación** es uno de estos:

- **auth** = Sistema de autorización
- **cron** = instalación de cron/at
- **daemon** = demonios del sistema
- **kern** = Kernel
- **local0** = Uso local
- **local1** = uso local
- **local2** = Uso local
- **local3** = Uso local

- **local4** = Uso local
- **local5** = Uso local
- **local6** = uso local
- **local7** = Uso local
- **lpr** = Sistema de impresora de línea
- **mail** = Sistema de correo
- **news** = Noticias USENET
- **sys10** = Uso del sistema
- **sys11** = Uso del sistema
- **sys12** = Uso del sistema
- **sys13** = Uso del sistema
- **sys14** = Uso del sistema
- **sys9** = Uso del sistema
- **syslog** = Syslog en sí
- **user** = Proceso de usuario
- **uucp** = sistema de copia de Unix a Unix


Configuración de Syslog en puntos de acceso FlexConnect

La depuración basada en el cliente de FlexConnect permite habilitar la depuración específica del cliente para un AP o grupos de AP. También permite que la configuración del servidor syslog registre los mensajes de depuración.

Uso de la depuración basada en cliente de FlexConnect:

- Puede depurar el problema de conectividad del cliente del AP ingresando una dirección MAC particular de un cliente desde el WLC o la consola del AP.

- Puede depurar problemas de conectividad del cliente en el sitio de FlexConnect sin introducir comandos de depuración en varios AP o sin habilitar varias depuraciones. Un solo comando debug habilita los debugs.
- No necesita ingresar el comando debug en varios APs, dependiendo de dónde el cliente puede desplazarse. Al aplicar la depuración en el nivel de grupo de FlexConnect, todos los AP que forman parte del grupo de FlexConnect reciben esta solicitud de depuración.
- Los registros se recolectan centralmente en el servidor syslog proporcionando la dirección IP del servidor desde el WLC.
- Si configura un punto de acceso FlexConnect con un servidor syslog configurado en el punto de acceso, después de que el punto de acceso se recargue y la VLAN nativa distinta de 1, en el momento de la inicialización, pocos paquetes syslog del punto de acceso se etiquetan con el ID de VLAN 1. Este es un problema conocido.

 **Nota:** Las depuraciones del controlador AP no están habilitadas en el WLC. Si tiene acceso a la consola AP, se pueden habilitar las depuraciones del controlador.

Estos son los comandos de depuración en la CLI del WLC:

```
(Cisco Controller) >debug flexconnect client ap ap-name{add|delete}mac-addr1 mac-addr2 mac-addr3 mac-addr4
(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 mac-addr4
(Cisco Controller) >debug flexconnect client groupgroup-namesyslog{server-ip-address|disable}
(Cisco Controller) >show debug
```

Aquí se enumeran los comandos de depuración que se pueden ingresar en la consola AP. Estos comandos son aplicables para depurar la consola AP del cliente cuando está accesible. Si ingresa estos comandos en la consola AP, los comandos no se comunican al WLC.

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

Restricciones

- La configuración de AP no se guarda al reiniciarse.
 - La adición de un AP a un AP y la eliminación de un AP de un FlexConnect Group afecta el estado de depuración de FlexConnect del AP.
-
-



Nota: No es posible cambiar el puerto syslog que se está utilizando.

Para verificar la configuración de syslog en la CLI, ingrese el comando **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) >

Para ver la configuración global del servidor syslog para todos los puntos de acceso que se unen al controlador ingresando este comando: **show ap config global**.

Aparecerá información similar a la del siguiente texto:

AP global system logging host..... 10.0.0.1

Para mostrar la configuración del servidor de registro específico del AP para un AP, utilice el comando **show ap config generalap-name**.

Ejemplo:

<#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
[...]
```

Información Relacionada

- [Guía de configuración del controlador inalámbrico de Cisco, versión 8.8](#)
- [Soporte técnico y descargas de Cisco](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).